UNIVERSITÉ PARIS-EST – UNIVERSITÉ DE ROME III

LA CONSTRUCTION D'UN DROIT SPÉCIFIQUE À LA PROTECTION DES DONNÉES PERSONNELLES DANS L'UNION EUROPÉENNE

Madame Flavia Caloprisco

DIRECTEURS DE RECHERCHE

Édouard DUBOUT
Professeur à l'Université Paris II-Panthéon-Assas

Giandonato CAGGIANO
Professeur à l'Université de Rome III

SUFFRAGANTS

Mélanie CLEMENT FONTAINE
Professeur à l'Université de Versaille Saint-Quentin- en Yvelines (Rapporteur)

Delphine DERO-BUGNY
Professeur à l'Université Paris Descartes Paris V (Rapporteur)

Francesco MARTUCCI
Professeur à l'Université Paris II-Panthéon-Assas (Président)

Les universités de Paris-Est et de Rome III n'entendent donner aucune approbation ni improbation aux opinions émises dans les thèses ; ces opinions doivent être considérées comme propres à leurs auteurs.

Remerciements

Je souhaite exprimer ma profonde gratitude à mon directeur de thèse, le Professeur Édouard Dubout pour sa confiance et ses précieux conseils qui m'ont permis de mener à bien cette thèse.
Je suis ensuite très reconnaissante au Professeur Giandonato Caggiano d'avoir accepté de codiriger cette thèse et de m'avoir suivie de près ou de loin toutes ces années et pour son encouragement à m'engager dans cette voie. Je remercie par ailleurs l'Université de Rome III et de Paris-Est d'avoir permis la mise en place de cette cotutelle.

Enfin, mes remerciements vont à mes proches pour m'avoir soutenue et pour n'avoir jamais douté.

Résumé

La thèse procède à une analyse descriptive et évaluative du droit fondamental à la protection des données personnelles dans l'ordre juridique de l'Union européenne. Ce droit a été distingué des autres droits fondamentaux tels que le droit au respect de la vie privée. Afin d'en mesurer la portée, l'étude analyse les restrictions dont il peut faire l'objet lorsqu'il entre en conflit avec d'autres intérêts individuels également protégés ou avec des contraintes collectives relevant de l'intérêt général. En effet, la révolution numérique permet certes aux individus d'augmenter leur liberté, mais elle renforce aussi la capacité de l'État de contrôler l'individu. C'est pourquoi, la progressive constitutionnalisation du droit à la protection des données personnelles dans l'Union européenne entend améliorer la protection offerte à l'individu en constituant un moyen d'expression de l'identité et des valeurs de l'Union européenne. A cet égard, le rôle de la Cour de justice s'avère central et stratégique, non seulement à l'échelle européenne mais également à l'échelle mondiale. A travers des arrêts au retentissement international, elle s'efforce de garantir le juste équilibre des intérêts en jeu en évaluant la nécessité et la proportionnalité des mesures adoptées, assurant un effet extraterritorial au droit à la protection des données. La reconnaissance de la Charte des droits fondamentaux en tant que source du droit primaire a apporté une contribution décisive aux derniers développements de sa jurisprudence en matière de données à caractère personnel, et a donné une impulsion au processus d'autonomie du système de l'Union par rapport à celui de la Convention européenne des droits de l'homme.

Mots-clés Union européenne - Droits fondamentaux – Proportionnalité – Sécurité - Données personnelles - Identité européenne

Riassunto

La tesi svolge un'analisi descrittiva e valutativa del diritto fondamentale alla protezione dei dati personali. Questo diritto è stato distinto da altri diritti fondamentali come il diritto al rispetto della vita privata. Al fine di misurare l'incidenza di questo diritto, lo studio analizza le restrizioni che può subire e il suo bilanciamento con altri interessi individuali o generali ugualmente protetti. In effetti, la rivoluzione digitale da un lato consente alle persone di esercitare alcuni dei loro diritti e, dall'altro, consente allo stato di controllare l'individuo. La progressiva costituzionalizzazione del diritto alla protezione dei dati personali migliorerebbe la protezione offerta all'individuo.
Inoltre, il diritto fondamentale alla protezione dei dati personali costituirebbe un mezzo per esprimere l'identità e i valori dell'Unione europea.
Il ruolo della Corte di giustizia sembra essere centrale e strategico, non solo a livello europeo ma anche a livello globale, garantendo il giusto equilibrio degli interessi in gioco attraverso la valutazione della necessità e proporzionalità delle misure adottate. Il riconoscimento della Carta

dei diritti fondamentali come fonte di diritto primario ha dato un contributo decisivo agli ultimi sviluppi della sua giurisprudenza in materia di dati personali e un impulso decisivo al processo di autonomizzazione rispetto alla CEDU.

Parole chiave Unione europea - diritti fondamentali – proporzionalità – sicurezza - dati personali- identità europea

Abstract

The thesis carries out a descriptive and evaluative analysis of the fundamental right to the protection of personal data. This right has been distinguished from other fundamental rights such as the right to respect for private life. In order to measure the impact of this right, the study analyzes the restrictions that may be placed on it when it conflicts with other equally protected individual interests or with the general interest on the basis of the proportionality principle. In fact, the digital revolution on the one hand allows people to exercise some of their rights but, on the other hand, allows the governments to control the individual. The progressive "constitutionalisation" of the right to personal data protection would improve the protection offered to the individual.
Furthermore, the fundamental right to the protection of personal data would constitute a means of expressing the identity and values of the European Union.
In a context marked by the technologies of surveillance and exchange of personal data, the European Union has chosen a model that respects fundamental rights.
the role of the Court of Justice of the European Union appears to be central and strategic, not only at European level, but also globally, guaranteeing the right balance of interests by assessing the necessity and proportionality of the measures adopted. The recognition of the Charter of Fundamental Rights as a source of primary law has made a decisive contribution to the latest developments in its case-law in the matter and a decisive contribution to the process of autonomy with respect to the ECHR.

Keywords European Union - Fundamental rights- Proportionality – Security - European identity

ÉQUIPE MARCHÉS, INSTITUTIONS, LIBERTÉS (MIL)

Université Paris-Est Créteil (UPEC), Faculté de Droit

SOMMAIRE

INTRODUCTION GÉNÉRALE 17

I - L'ORIGINE DU DROIT A LA PROTECTION DES DONNÉES PERSONNELLES 25
II - LA CONSTITUTIONNALISATION DU DROIT FONDAMENTAL À LA PROTECTION DES DONNÉES PERSONNELLES.....46
III. L'ÉMERGENCE D'UN MODÈLE EUROPÉEN DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES 56

PARTIE I. UNE EXTENSION PROGRESSIVE DU CHAMP DE LA PROTECTION 72

TITRE I. LA MUTATION INTERNE DU STANDARD DE PROTECTION 76
CHAPITRE I. LE RÉGIME DE PROTECTION DANS LE MARCHÉ INTÉRIEUR 80
CHAPITRE II. LE RÉGIME DE PROTECTION DANS L'ELSJ 141
TITRE II. LA PROJECTION INTERNATIONALE DU STANDARD EUROPÉEN DE PROTECTION.....181
CHAPITRE I. L'EXTRATERRITORIALITÉ DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES DANS LES RELATIONS COMMERCIALES 183
CHAPITRE II. L'EXTRATERRITORIALITÉ DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CONTEXTE DE CRISE SÉCURITAIRE...221

PARTIE II. UNE ARTICULATION COMPLEXE DU RÉGIME DE PROTECTION 267

TITRE I. LA SYSTÉMATISATION D'UNE PROTECTION JURIDICTIONNELLE.....271
CHAPITRE I. UNE DOUBLE PROTECTION JURIDICTIONNELLE.....273
CHAPITRE II. L'AUTONOMISATION DU STANDARD DE PROTECTION 362
TITRE II. L'ADJONCTION D'UNE PROTECTION NON- JURIDICTIONNELLE.....397
CHAPITRE I. LA PROTECTION NON-JURIDICTIONNELLE AU SEIN DES ÉTATS MEMBRES 399
CHAPITRE II. LA PROTECTION NON-JURIDICTIONNELLE AU SEIN DE L'UNION EUROPÉENNE 444

BIBLIOGRAPHIE 480

TABLE DE JURISPRUDENCE 511

INDEX THÉMATIQUE.....518

TABLE DES MATIÈRES.....520

LISTE DES PRINCIPALES ABRÉVIATIONS

aff. jointes ..... Affaires jointes
Art ..... Article
Cass ..... Cour de Cassation
CDFUE ..... Charte des droits fondamentaux de l'Union européenne
CEDHou CourEDH ..... Cour européenne des droits de l'homme
CEDP ..... Contrôleur européen à la protection des données personnelles
ConventionEDH ..... Convention européenne des droits de l'homme
Chap ..... Chapitre
Chron ..... Chronique
CJUE ..... Cour de justice de l'Union européenne
CNIL ..... Commission nationale de l'informatique et des libertés
Coll ..... Collection
Contra ..... En sens contraire
Conv. EDH ..... Convention européenne des droits de l'homme
Dir ..... Sous la direction de
éd ..... Édition
ELSJ ..... Espace de liberté, de sécurité et de justice
G29 ..... Groupe de l'article 29
Gr. Ch ..... Cour européenne des droits de l'homme réunie en Grande chambre
GC ..... Cour de justice de l'Union européenne réunie en Grande Chambre
Ibid ..... Même auteur, même ouvrage, même endroit
Idem ..... Même auteur, même ouvrage
in ..... Dans
Infra ..... Plus bas
JAI ..... Justice et affaires intérieures
JOUE ..... Journal officiel de l'Union européenne
n° ..... Numéro
Op. cit. ..... *Opere citato*, ouvrage (pré)cité
p. ..... Page
Par ..... Paragraphe
pp ..... Pages
Pt ..... Point
PUF ..... Presses universitaires de France
RGPD ..... Règlement général sur la protection des données à caractère personnel
s ..... Suivants
Supra ..... Plus haut
TCE ..... Traité de la Communauté européenne
TFUE ..... Traité sur le fonctionnement de l'Union européenne

th ..... Thèse
TUE..... Traité sur l'Union européenne
UE ..... Union européenne
Vol ..... Volume
Voy..... Voye

ABRÉVIATIONS REVUES

CDE..... Cahiers de droit européen
CMLR ..... Common Market Law Review
EJLS ..... European Journal of Legal Studies
ELJ ..... European Law Journal
ELR ..... European Law Review
RDUE..... Revue du droit de l'Union européenne
RMCUE..... Revue du marché commun et de l'Union européenne
RTDE ..... Revue trimestrielle de droit européen
RTDH..... Revue trimestrielle des droits de l'homme

INTRODUCTION GÉNÉRALE

« Lorsque vous dites "le droit à la vie privée ne me préoccupe pas, parce que je n'ai rien à cacher", cela ne fait aucune différence avec le fait de dire "Je me moque du droit à la liberté d'expression parce que je n'ai rien à dire" ou "de la liberté de la presse parce que je n'ai rien à écrire" »[1].

Edward Snowden - Citizenfour *(2014)*

« Le roi prend note de toutes leurs intentions, Avec des moyens qu'ils ne peuvent même pas imaginer ».

William Shakespeare, Henry V *(1599)*

1 Cette retranscription du dialogue entre le journaliste Glenn Greenwald et Snowden est tirée du documentaire *Citizenfour* de Laura Poitras, sorti en 2014, qui filme la première rencontre entre Snowden et des journalistes dans sa chambre d'hôtel à Hong Kong. Cité par Romain Badouart dans *Le désenchantement de l'Internet*, FYP éditions, 2017, p. 10.

1 Les défis modernes. L'ère du numérique, ou l'ère des technologies de l'information, se caractérise par l'utilisation généralisée des ordinateurs, de l'Internet et des technologies numériques. Cela implique la collecte et le traitement de grandes quantités de données, y compris des données personnelles. La collecte et le traitement de données à caractère personnel dans une économie mondialisée se traduit par une augmentation du nombre de flux de données transfrontaliers. Un tel traitement peut apporter des avantages significatifs et visibles dans la vie quotidienne : les moteurs de recherche facilitent l'accès à des volumes considérables d'informations et de connaissances, les services de réseaux sociaux permettent aux gens de communiquer, d'exprimer des opinions et de mobiliser un soutien social, environnemental et politique. Les entreprises et les consommateurs bénéficient de techniques de commercialisation efficaces et efficientes qui stimulent l'économie. La technologie et le traitement des données personnelles sont également des outils indispensables pour les autorités étatiques dans leur lutte contre la criminalité et le terrorisme. De même, la collecte, le stockage et l'analyse de grandes quantités d'informations (le Big Data [2]) pour identifier des schémas et prédire les comportements, peuvent être une source de valeur significative pour la société, améliorant la productivité, la performance du secteur public et la participation de la société civile[3]. À l'instar de l'analyse des Big Data, l'intelligence artificielle (IA) et la prise de décision automatisée qu'elle génère nécessitent le traitement de grandes quantités de données. Ces données peuvent provenir de l'appareil lui-même ou de l'environnement. Le profilage[4], par exemple, est un processus qui peut s'appuyer sur une prise de décision automatisée en fonction de modèles ou de facteurs prédéterminés. Le profilage basé sur le Big Data implique la recherche de modèles reflétant les « caractéristiques d'un type de personnalité », par exemple lorsque les sociétés de shopping en ligne proposent des produits « que vous aimerez peut-être » sur la base des informations collectées dans le panier du client. Plus il y a de données, plus la mosaïque est claire[5]. Malgré ses multiples avantages, l'ère numérique pose également des problèmes en termes de confidentialité et de protection des données, car d'énormes quantités d'informations personnelles sont collectées et traitées de manière de plus en plus complexe et opaque. Les progrès technologiques ont conduit à la mise au point d'ensembles de données massifs qui peuvent être facilement recoupés et analysés pour rechercher des modèles ou pour l'adoption

---

2 Le terme « Big Data » peut faire référence à plusieurs concepts, en fonction du contexte. Il englobe généralement la capacité technologique croissante à collecter des processus et à extraire de nouvelles connaissances prédictives à partir d'un volume, d'une vitesse et d'une variété de données importants. Le concept de Big Data couvre donc à la fois les données elles-mêmes et l'analyse des données. Voy: Council of Europe, « Consultative Committee of Convention 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data », 23 January 2017, p. 2; European Commission, « Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions towards a thriving data economy» COM(2014) 442 final, Brussels, 2 July 2014, p. 4; International Telecommunications Union (2015), Recommendation Y.3600. « Big Data – Cloud computing based requirements and capabilities ».

3 Voy. Council of Europe, Consultative Committee of Convention 108, « Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data », T-PD(2017)01, Strasbourg, 23 January 2017.

[4] Voy. RGPD art. 4. 4) toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

5 S. RUSSEL, P. NORVIG, *Artificial Intelligence: A Modern Approach* (2nd ed.), 2003, Upper Saddle River, New Jersey: Prentice Hall, 2003, p. 27, 32–58, 968–972.

de décisions basées sur des algorithmes, qui peuvent fournir un aperçu sans précédent du comportement humain et de la vie privée[6]. Les principaux problèmes concernent, d'une part, le volume et la variété des données personnelles traitées et, d'autre part, le traitement et ses résultats. L'introduction d'algorithmes complexes et de logiciels permettant de transformer des données de masse en une ressource à des fins décisionnelles affecte les individus, notamment en cas de profilage. Le règlement (UE) 2016/679 du Parlement et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après RGPD), comprend des dispositions sur le droit de ne pas être soumis à la prise de décision automatisée, y compris le profilage, permettant à la personne de demander une intervention humaine et d'exprimer leur point de vue et de contester la décision[7]. Cela est nécessaire pour assurer un niveau de protection adéquat des données personnelles si, par exemple, aucune intervention humaine n'est possible ou si les algorithmes sont trop complexes et que la quantité de données impliquées est trop importante pour permettre aux individus de justifier certaines décisions et / ou des informations préalables pour obtenir leur consentement. Un exemple d'utilisation de l'IA et de la prise de décision automatisée se trouve dans les développements récents dans les demandes de prêts hypothécaires ou lors des processus de recrutement. Les demandes sont refusées en raison du fait que les demandeurs ne répondent pas à des paramètres ou à des facteurs prédéterminés. Le profilage et la publicité ciblée peuvent ne pas être un problème si les individus sont conscients qu'ils font l'objet de publicités sur mesure. Le profilage devient un problème lorsqu'il est utilisé pour manipuler des individus, c'est-à-dire pour rechercher des personnalités ou des groupes de personnes en vue d'une campagne politique. Par exemple, des groupes d'électeurs indécis peuvent être contactés via des messages politiques adaptés à leur « personnalité » et à leurs attitudes. Un autre problème pourrait être l'utilisation d'un tel profilage pour refuser l'accès à des biens et services à certaines personnes. Il existe d'autres enjeux pour la protection des données comme l'Internet des objets (IoT). Avec l'IoT, les appareils peuvent être connectés et interagir avec d'autres appareils via Internet. Cela permet aux objets et aux personnes d'être interconnectés via des réseaux de communication, de rendre compte de leur statut et / ou de l'état de leur milieu environnant. L'IoT peut être particulièrement bénéfique pour les soins de santé. Les entreprises ont déjà créé des appareils, des capteurs et des applications permettant de surveiller la santé d'un patient. En utilisant un bouton d'alarme portable et d'autres capteurs sans fil placés autour de la maison, il est possible de suivre la routine quotidienne des personnes âgées vivant seules et de générer des alertes si de graves perturbations sont détectées dans leur emploi du temps quotidien. Les détecteurs de chute, par exemple, sont largement utilisés par les personnes âgées. Ces capteurs peuvent détecter les chutes avec précision et en informer le médecin et / ou la famille de la personne concernée. Parallèlement, compte tenu de l'énorme quantité d'informations personnelles générées par les utilisateurs, l'expansion de l'IoT suscite une préoccupation croissante quant à la manière de protéger la vie privée et les données personnelles. Ces menaces peuvent inclure : un manque de garanties juridiques et procédurales entourant les processus pouvant entraîner l'exclusion des utilisateurs ; une protection

6 Voy. European Parliament (2017), « Resolution on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law enforcement » (P8_TA-PROV (2017) 0076, Strasbourg, 14 March 2017.

7 Voy. RGPD art. 22.

insuffisante des enfants et des jeunes contre les contenus ou comportements préjudiciables ; un manque de respect pour les droits des autres ; une insuffisance de paramètres par défaut respectueux de la vie privée ; un manque de transparence sur les finalités pour lesquelles les données personnelles sont collectées et traitées[8]. L'intelligence artificielle et la prise de décision automatisée soulèvent des questions quant à la responsabilité des violations affectant les données personnelles. Le règlement général sur la protection des données fournit un cadre juridique pour la responsabilité des acteurs du traitement : le responsable et le sous-traitant[9]. La question de la responsabilité dans le contexte de l'intelligence artificielle deviendra d'autant plus difficile lorsqu'une IA prendra une décision fondée sur le traitement des données qu'elle a elle-même développé. Ainsi lorsque l'IA et les algorithmes sont considérés comme des produits, cela soulève des problèmes entre la responsabilité personnelle, qui est encadrée par le RGPD, et la responsabilité du produit, qui n'est pas la même. Lorsque des données à caractère personnel ou des informations sur le comportement individuel sont collectées, traitées et évaluées de manière massive, leur exploitation peut conduire à des violations importantes des droits et libertés fondamentaux [10] . Ainsi les autorités étatiques peuvent entreprendre des activités de surveillance de masse en utilisant ces technologies. La surveillance de masse est un exemple de l'impact significatif que ces technologies peuvent avoir sur les droits des individus. En 2013, les révélations d'Edward Snowden sur le fonctionnement des programmes de surveillance Internet et téléphonique à grande échelle par l'Agence de sécurité américaine ont suscité des inquiétudes importantes quant aux dangers que les activités de surveillance représentent pour la vie privée, la démocratie et la liberté d'expression. La surveillance de masse peut porter atteinte à l'essence même du droit à la vie privée. En effet, elle peut avoir un effet négatif et dissuasif sur la démocratie, la créativité et l'innovation car la simple crainte que l'État ne cesse de suivre et d'analyser le comportement et les actions des citoyens peut les décourager à exprimer leurs points de vue et entraîner la méfiance et la prudence [11] . Le traitement des données personnelles est également un outil puissant dans les mains des entreprises. Aujourd'hui, il peut révéler des informations détaillées sur la santé ou la situation financière d'une personne, des informations utilisées par les entreprises pour prendre des décisions importantes pour les individus, telles que la prime d'assurance maladie à appliquer ou leur solvabilité. Les techniques de traitement des données peuvent également avoir un impact sur les processus démocratiques lorsqu'elles sont utilisées par des politiciens ou des entreprises pour influencer les élections par exemple, grâce au « ciblage » des communications

8 European Data Protection Supervisor, *Understanding the Internet of Things*, 2017, disponible à l'adresse. https://edps.europa.eu/data-protection/our-work/subjects/internet-things_en.

9 Voy. RGPD Art. 77–79 et 82.

10 DE HERT P., S. GUTWIRTH S, « Regulating Profiling in a Democratic Constitutional State », *in* M. HILDEBRANDT & S. GUTWIRTH (Eds), *Profiling the European Citizen. Cross Disciplinary Perspectives*, Dordrecht, Springer, 2008, pp. 271-291. Voy: EDPS « Meeting the Challenges of Big Data », *Opinion* 7/2015, 19 November 2015; EDPS (2016), « Coherent enforcement of fundamental rights in the age of Big Data », *Opinion* 8/2016, 23 September 2016; European Parliament (2016), « Resolution on fundamental rights implications of Big Data: privacy, data protection, non-discrimination, security and law enforcement », P8_TA(2017)0076, Strasbourg, 14 March 2017; Council of Europe, Consultative Committee of Convention 108, « Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data », T-PD(2017)01, Strasbourg, 23 January 2017.

11 Voy.EDPS, *Meeting the challenges of Big Data*, Opinion 7/2015, Brussels, 19 November 2015.

des électeurs[12]. En d'autres termes, alors que la vie privée était initialement perçue comme un droit à la protection des individus contre une ingérence injustifiée des autorités publiques, à l'ère moderne, elle pourrait également être menacée par les pouvoirs des acteurs privés. Cela soulève des questions sur l'utilisation de la technologie et de l'analyse prédictive dans les décisions qui affectent la vie quotidienne des individus, et renforce la nécessité de s'assurer que tout traitement de données à caractère personnel respecte les exigences des droits fondamentaux. Ainsi la protection des données est intrinsèquement liée aux changements technologiques, sociaux et politiques. Une liste complète des défis futurs serait donc impossible à concevoir. La thèse se propose donc d'analyser et d'évaluer le modèle de protection offert par l'Union européenne.

2 Le droit à la protection des données personnelles comme moyen d'expression de l'identité de l'Union européenne. L'identité est un élément indispensable à la constitution d'un « univers mental partagé », d'une « coalition des cultures » qu'est une civilisation[13] . L'identité révèle ainsi une « conscience de l'identique et donc un sentiment d'appartenance à la collectivité ou au groupe »[14]. L'émergence de l'identité de l'Union est elle-même le fruit d'un processus progressif. Initialement la « peur du retour de la guerre ou la volonté de paix », la « peur du déclin ou le souhait de reconstruire une influence européenne, le rejet des totalitarismes ont accéléré le mouvement de politisation d'identité se manifestant par l'affermissement du projet d'unification européenne » [15] . Dans les années qui suivent la Première Guerre mondiale on assiste à la formation d'une identité communautaire (dont le substrat est essentiellement économique). Cependant, la construction fonctionnaliste de l'Union européenne a conduit les droits fondamentaux à constituer le cœur même de ce système de valeurs[16]. Ainsi l'article 2 TUE dispose que « l'Union est fondée sur les valeurs de respect de la dignité humaine, de liberté, de démocratie, d'égalité, de l'État de droit, ainsi que de respect des droits de l'homme, y compris des droits des personnes appartenant à des minorités. Ces valeurs sont communes aux États membres dans une société caractérisée par le pluralisme, la non-discrimination, la tolérance, la justice, la solidarité et l'égalité entre les femmes et les hommes ». L'article 3 § 5 souligne que « dans ses relations avec le reste du monde, l'Union affirme et promeut ses valeurs et ses intérêts et contribue à la protection de ses citoyens ». Le traité, enrichi de la Charte, proclame des droits dont le respect est garanti au moyen de mécanismes particuliers ou dans le cadre de la jurisprudence. La Cour de justice a effectivement initié un mouvement de subjectivisation et de fondamentalisation de l'ordre juridique se traduisant par un renforcement constant des exigences en matière de protection des droits de

12 L'un des derniers scandales a été le scandale Cambridge Analytica http://www.liberation.fr/planete/2018/05/03/scandale-des-donnees-cambridge-analytica-ferme-boutique_1647406.

13 Y. BEN ACHOUR, *Le rôle des civilisations dans le système international, droit et relations internationales*, Bruylant, 2003, p.15.

14 R. FRANCK, *Conclusions,* Relations internationales, 2009/4, nº 140, p. 113.

15 R. FFRANCK, op. cit., p. 116.

16 Voy. MONTESQUIEUcité par V. CONSTANTINESCO, « La confrontation entre identité constitutionnelle européenne et identités constitutionnelles nationales, convergences ou contradictions ? Contrepoint ou hiérarchie ? », in *L'Union européenne, Union de droit, Union des droits, Mélanges en l'honneur de Philippe Manin*, Pedone, 2010, p. 79.

l'homme[17] . D'ailleurs le contrôle de la validité d'un acte de l'Union au regard des droits fondamentaux est l'expression d'une garantie constitutionnelle découlant du traité en tant que système juridique autonome et prévalent [18] . Les obligations résultant d'un « accord international » ne peuvent en aucune circonstance affecter les « principes constitutionnels du traité CE, au nombre desquels figure le principe selon lequel tous les actes communautaires doivent respecter les droits fondamentaux »[19]. Or, la question des relations qu'entretiennent identité et espace est tout aussi importante car la frontière délimite les souverainetés. L'Union européenne et en particulier la Cour de justice à travers des arrêts historiques en matière de données personnelles a affirmé sa souveraineté au-delà de ses frontières avec un effet extraterritorial. L'Union européenne a su exporter ses normes relatives à la protection des données personnelles notamment dans le domaine sécuritaire[20]. Dans un contexte marqué par les technologies de surveillance et d'échange de données à caractère personnel, l'Union européenne a choisi un modèle respectant les droits fondamentaux[21]. Le rôle de la Cour de justice n'a jamais été aussi important. Elle s'érige comme l'ultime recours face à cette fuite en avant sécuritaire et comme gardienne de l'identité et des valeurs européennes. Avant de préciser le cadre juridique en la matière et d'évaluer son efficacité, il convient de parcourir l'origine du droit à la protection des données personnelles (I) puis d'analyser son caractère de droit fondamental (II) qui s'inscrit dans le processus identitaire de l'Union européenne (III).

I - L'ORIGINE DU DROIT A LA PROTECTION DES DONNÉES PERSONNELLES

3 Des explications d'ordre sociale, économique et politique. Le processus de mondialisation, l'évolution incessante des technologies, l'intrusion d'Internet dans la vie privée et les problèmes de sécurité nationale et d'ordre public ne sont que quelques-uns des nombreux facteurs qui ont

---

17 J. RIDEAU, *Les droits fondamentaux dans l'Union européenne, dans le sillage de la Constitution européenne*, Bruylant, 2009, p. 489.

18 CJUE, Digital Rights Ireland et Seitlinger e.a. affaires jointes C-293/12 et C-594/12, 8 avril 2014.

19 CJUE, Maximillian Schrems / Data Protection Commissioner, C-362/14, 6 octobre 2015.

20 M. FOUCAULT, *Surveiller et punir: naissance de la prison,* Paris, Gallimard, 1975 ; A. MATTELART, *La globalisation de la surveillance. Aux origines de l'ordre sécuritaire, Paris,* La Découverte 2008 ; V. MITSILAGAS e V. MITSILEGAS, J. MONAR, W. REESW, *The European Union and Internal Security. Guardian of the People?*, Basingtoke, Palgrave Macmillan, 2003, p. 6-41.

21 COMMISSION EUROPEENNE (2010b), « Mettre en place un espace de liberté, de sécurité et de justice au service des citoyens européens. Plan d'action mettant en œuvre le programme de Stockholm », Bruxelles, Commission européenne. COMMISSION EUROPEENNE (2011b), « Proposition de Directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière », Bruxelles, Commission européenne. COMMISSION EUROPEENNE (2012), « Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données », Bruxelles, Commission européenne.

placé le droit à la protection des données personnelles au centre du débat politique, social et juridique des dernières décennies. Devant le constat des risques liés à la multiplication de l'utilisation des données personnelles[22], les États ont institué une protection afin de préserver les valeurs sur lesquelles ils reposent. Toutefois, cette protection est apparue insuffisante et a conduit à la juridicisation d'un droit fondamental à la protection des données personnelles au sein de l'Union européenne. D'un point de vue sociopolitique, la demande accrue de sécurité et la montée de l'individualisme expliquent l'utilisation des données personnelles. En effet, d'une part, le progrès technologique a permis de répondre à la demande de sécurité en créant de nouveaux moyens de renseignements et d'autre part les acteurs privés ont adopté un modèle commercial fondé sur la valorisation des données personnelles[23]. Le traitement des données par les autorités publiques afin de lutter contre le terrorisme et la criminalité organisée en Europe est parfois décrit à travers la notion de « sécurité humaine » : la sécurité ne consiste plus en la défense des intérêts vitaux de l'État mais se définit comme le droit pour l'individu d'être protégé contre tous types de risques [24] . Ainsi les technologies de sécurité se sont progressivement étendues au point de parler aujourd'hui de « société de surveillance »[25]. Les révélations d'Edward Snowden[26] ont, à cet égard, mis en exergue l'ampleur de la collecte et de l'exploitation des communications électroniques par les États-Unis et le Royaume-Uni. D'autre part, l'individualisme [27] apparu aux XVII[e] et XVIII[e] siècles avec la construction de l'État moderne a placé l'individu au centre de l'organisation sociale et politique. Ainsi les nouvelles technologies offrent aux individus des espaces inédits de liberté et des moyens exceptionnels pour épanouir leur personnalité. En effet, les nouvelles technologies constituent un moyen pour l'individu de révéler des informations sur lui-même. Internet favorise, à travers les blogs et les

22 Sur l'histoire des pratiques d'identification des personnes v. G. NOIRIEL (dir.), *L'identification. Genèse d'un travail d'État*, Ed. Belin, coll. Socio-Histoires, p. 272; P. KAYSER, *La protection de la vie privée par le droit. Protection du secret de la vie privée*, Economica- Presses universitaire d'Aix-Marseille 3e, éd., 1999, p.605, spèc. p. 215.

23 R. TINIERE, « Article 8 protection des données à caractère personnel », in F. PICOD, S. VAN DROOGHENBROEK, *Commentaire article par article de la CDFUE*, Bruylant, 2018 p. 186.

24 Pour un historique de la doctrine de « sécurité humaine » Voy. F. GROS, *Désastre humanitaire et sécurité humaine. Le troisième âge de la sécurité*, *Esprit*, 2008, n° 343, p. 51 et s; F. GROS, M. CASTILLO, A. GARAPON, *De la sécurité nationale à la sécurité humaine*, *Raisons politiques*, 2008, n° 32, p. 5et s.

25 A. MATTELARD, *La globalisation de la surveillance : Aux origines de l'ordre sécuritaire*, La découverte Poche, coll. Essai n° 290, 2008, p.266.

26 L'interview apparue sur *The Guardian* est disponible à l'adresse suivante : https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.

27 A. LALANDE, *Vocabulaire technique et critique de la philosophie*, PUF, coll. Quadrige Dico Poche, 2010, p. 1323. sp. p. 499. Selon André Lalande, l'individualisme renvoie dans son sens générique à « toute tendance qui voit dans l'individu ou dans l'individuel soit la forme la plus essentielle de réalité, soit le plus haut degré de valeur».

réseaux sociaux[28], une banalisation croissante de « l'exposition de soi »[29]. De plus, l'individu recherche des informations sur lui-même, par exemple à travers des applications il est possible pour l'individu de mesurer sa performance lors d'un exercice physique par des capteurs de vitesse ou de rythme cardiaque, performance qu'il pourra mettre ensuite en ligne sur des réseaux sociaux, tels que Facebook. Le contexte sociopolitique a contribué à la demande de protection de l'utilisation des données personnelles au point de parler de « schizophrénie »[30]. En effet, d'un côté, le citoyen demeure attaché aux principes du respect de ses données personnelles et de sa vie privée, de l'autre, il est prêt à sacrifier ses droits sur l'autel de la popularité et de l'audience sur les réseaux sociaux. Ainsi la multiplication [31] de l'utilisation des données personnelles a conduit à l'accentuation des risques pesant sur l'individu. Là encore, ces risques ne sont pas nouveaux mais ont été exacerbés par cette même multiplication. L'origine[32] et l'évolution du droit fondamental à la protection des données à caractère personnel ne sont pas pacifiques[33] . Toutefois il est indiscutable que son origine est étroitement liée aux notions d'intimité et de vie privée[34]. Certains signalent la deuxième moitié des années soixante-dix comme l'étape fondatrice, d'autres situent l'embryon de cette discipline le 31 janvier 1968, avec la Recommandation 509 du Conseil de l'Europe[35]. Indépendamment de la date d'origine, de nombreux exemples démontrent le lien avec la notion d'intimité et de vie privée : le *Privacy Act*, adopté aux États-Unis en 1974, exprime la dépendance entre les deux figures[36]; dans le

28 L'ampleur du phénomène se mesure par rapport au nombre de personnes inscrites et à la masse d'informations que ces personnes mettent en ligne. Ainsi un utilisateur de Facebook serait en moyenne relié à 120 amis et un profil-type sur Facebook contiendrait en moyenne « 40 informations à caractère personnel, parmi lesquelles figurent nom, date de naissance, sexe, opinions politiques et religieuses, préférences sexuelles, livres et films préférés, parcours scolaire, universitaire et professionnel, le tout accompagné de photographies et parfois même de vidéos ». Voy. Y.DETRAIGNE, A.-M. ESCOFFIER, *Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, 2009, p. 31-32.

29 Y. DETRAIGNE, A.-M. ESCOFFIER, préc., spéc. p. 31-32.

30 C. RICHAUD, *Données personnelles : la schizophrénie citoyenne*, consulté le 20 août 2018 sur le site de la revue *Pouvoirs*. Disponible à l'adresse: http://www.revue-pouvoirs.fr/Donnees-personnelles-la.html.

31 EDPS opinion 8/2016 on coherent enforcement of fundamental rights in the age of big data, 23 sept. 2016.

32 La plupart de la doctrine situent l'origine de cette discipline le 31 janvier 1968, avec la Recommandation 509 du Conseil de l'Europe : Recommandation 509 (1968) « Droits de l'homme et réalisations scientifiques et technologiques modernes », qui met en évidence les dangers que supposent pour la vie privée les dernières réalisations scientifiques et technologiques.

33 Pour une vue d'ensemble sur la protection des données en Europe, voir le *Manuel de droit européen en matière de protection des données*, élaboré par l'Agence des droits fondamentaux de l'Union Européenne et le Conseil de l'Europe, en association avec le greffe de la Cour Européenne des droits de l'homme, 2014.

34 Par exemple aux États-Unis a été adoptée le 31 décembre 1974, la *Privacy Act* ayant pour objectif la sauvegarde de la vie privée des individus face à l'usage frauduleux de fichiers fédéraux. La relation entre vie privée et données personnelles est explicitement reconnue par le Congrès états-unien, qui, dans l'exposé des motifs de la loi, constate que la vie privée des individus est directement affectée par la collecte, maintenance, utilisation et diffusion d'informations personnelles par les agences fédérales. Dans le continent européen, la protection des données personnelles se cristallise dans la Convention 108 du Conseil de l'Europe et l'art. 8 de la Convention européenne des droits de l'homme (CEDH) sur la vie privée.

35 Recommandation 509 (1968) « Droits de l'homme et réalisations scientifiques et technologiques modernes », qui met en évidence les dangers que supposent pour la vie privée les dernières réalisations scientifiques ettechnologiques.

36 Adoptée le 31 décembre 1974, le *Privacy Act* a pour objectif la sauvegarde de la vie privée des individus face à l'usage frauduleux de fichiers fédéraux. La relation entre vie privée et données personnelles est explicitement reconnue par le Congrès états-unien, qui, dans l'exposé des motifs de la loi, constate que la vie privée des individus est directement affectée par la collecte, maintenance, utilisation et diffusion d'informations personnelles par les agences fédérales.

continent européen, la protection des données personnelles se cristallise dans la Convention 108 du Conseil de l'Europe (ci-après Convention 108) et l'art. 8 de la Convention Européenne des droits de l'homme concernant la protection de la vie privée (ci-après CEDH)[37]. En ce qui concerne l'Union européenne, une importante partie de ses États membres n'a pas consacré au niveau constitutionnel un droit fondamental à la protection des données personnelles [38]. Sa reconnaissance se produit, de manière générale, à partir du droit à l'intimité ou à la vie privée. L'absence d'autonomie du droit à la protection des données personnelles vis-à-vis du droit à la vie privée qui caractérise les premières législations, reflète le stade de développement technique et économique des États membres. En effet, à l'époque de la rédaction des premières constitutions européennes, après la Seconde Guerre mondiale, la protection des données personnelles ne trouve pas de matérialisation en raison de la faible importance attachée à l'informatique[39]. Ainsi l'étude de l'origine du droit à la protection de la vie privée est nécessaire pour comprendre l'autonomisation du droit à la protection des données personnelles et la cristallisation d'un droit spécifique dans la Charte de droits fondamentaux de l'Union européenne. En effet, la protection de la vie privée est un concept ancien qui n'a jamais cessé d'évoluer dans le temps (A). Le droit à la protection des données personnelles est étroitement lié au droit à la vie privée dont il tire son origine, mais il apparaît comme un droit distinct né des préoccupations récentes, à partir du développement d'Internet (B).

A. Le rattachement au droit au respect de la vie privée

4 La vie privée, un concept ancien. Selon la pensée grecque, la capacité des hommes à s'organiser d'une manière politique est différente et en contraste frappant avec les relations naturelles qui ont leur centre dans l'*oikia*, la maison et la famille qui y réside. Comme l'écrit Arendt, la montée de la *polis*, la cité-état, « signifiait que l'homme recevait une sorte de seconde

---

37 L'article 8 de la CEDH assure le respect de la vie privée et familiale. Cette prévision légale a été utilisée par la Cour européenne des droits de l'homme (affaires Amann c. Suisse, Rotaru c. Roumanie et S. et Marper c. Royaume-Uni, entre autres) pour inclure dans son champ d'application la tutelle des données à caractère personnel.

38 Dans une grande partie des textes constitutionnels européens, la protection des données personnelles n'est qu'un reflet du droit à la vie privée. C'est le cas, entre autres, de la France (où le droit à la vie privée trouve sa raison d'être dans l'art. 4 de la Déclaration des droits de l'homme et du citoyen de 1789, bien que son expression littérale figure à l'art. 9 du Code Civil), la Belgique (art. 22 de la Constitution belge de 1831), l'Espagne (art. 18 de la Constitution espagnole de 1978) et le Luxembourg (art. 11.3 de la Constitution luxembourgeoise). Par contre, la Constitution grecque de 1975 dédie son art. 9 A à la protection des données personnelles et attribue à une autorité indépendante la garantie de son efficacité. La Constitution portugaise de 1976 va un peu plus loin en prévoyant, à son art. 35, le droit à la protection des données personnelles et en établissant une série de principes constitutionnels qui doivent être respectés par les pouvoirs publics lorsqu'une mesure dans ce domaine est envisagée.

39 C'est à partir des années soixante-dix que les États de l'Europe occidentale commencent à dicter leurs premières lois sur la protection des données personnelles : l'Allemagne, en 1977, avec la *Bundesdatenschutzgesetz*, la France, en 1978, avec la Loi n° 8-17 relative à l'informatique, aux fichiers et aux libertés ou l'Autriche, aussi en 1978, avec la *Datenschutzgesetz*, entre autres. Parallèlement, en 1981 est adoptée au sein du Conseil de l'Europe la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, texte qui sera repris comme source d'inspiration pour rédiger la Directive 95/46/CE.

vie, son *politikos bios* »[40]. Pour les Grecs de l'Antiquité, participer à la vie politique et donc publique était un devoir et la vie privée constituait une privation de la vie publique[41]. La sphère politique a été supplantée dans la modernité par la sphère sociale. Le travail et la productivité ont occupé le centre de la scène publique. L'*homo laborans* a remplacé l'individu qui excelle dans les discours et dans le courage de l'action, modèles et idéaux du citoyen grec. L'histoire nous apprend également que l'homme a découvert et développé les concepts de confidentialité et de secret. Les messages militaires étaient cryptés comme les messages d'amour. La protection des données a commencé à prendre forme dès l'Antiquité si l'on pense au fameux chiffrement de César, avec lequel il cryptait les ordres à ses généraux ; ou encore au carré de Polybe, système cryptographique inventé par le célèbre historien grec vers 150 avant J.-C. à l'origine du premier procédé de chiffrement par substitution[42]. Au Moyen Âge, le concept de vie privée était assez aléatoire. Les gens vivaient pratiquement en communauté, il pouvait s'agir de maisons, de quartiers ou de villages. Tout le monde savait tout sur tout le monde. À cette époque il y avait peu d'intérêt pour l'homme comme individu, il y avait des spectacles publics, que l'on pouvait voir dans les rues et sur les places, comme la punition publique des criminels. Les gens dormaient dans le même lit et partageaient les repas et la maison [43] . Toutefois, l'émergence de l'individualisme allait favoriser la reconnaissance d'une sphère privée à protéger tant de l'État que des autres individus. Dans l'époque moderne, bien avant la création et la diffusion d'ordinateurs permettant la collecte et la transmission des informations de manière très rapide, le droit à la vie privée coïncidait avec le droit d'être laissé seul, en paix, non perturbé, de jouir ainsi d'une sphère privée et intime. Cette prérogative dont chacun pouvait se prévaloir vis-à-vis de l'État a été théorisée pour la première fois dans le « *right to be left alone* »[44]. L'ombre de Big Brother[45] se profilait et le risque de voir l'État surveiller les individus et porter atteinte à leurs droits et libertés a débouché sur l'adoption de législations protectrices. Ainsi le concept de vie privée d'un point de vue juridique prend corps au XIX[e] siècle dans les pays industrialisés. Depuis, le droit à la vie privée a été reconnu comme droit de l'homme, et a pris sa place dans des traités internationaux et les constitutions de nombreux États[46]. Dans cette phase, les premières législations reconnaissaient le droit à la vie privée[47]. Cette conception, fille

40 H. ARENDT, *Vita Activa*, Milano, 2000.

41 H. ARENDT, *Vita Activa*, Milano, 2000: « Dans la sensibilité ancienne, l'aspect de privation de la vie privée, était considéré comme prédominant; cela signifiait littéralement un état de privation qui pourrait toucher des facultés supérieures et plus humaines. (...) On ne pense plus à la privation quand on parle de la vie privée, et cela est en partie dû à l'énorme enrichissement de la vie privée provoqué par l'individualisme moderne. La vie privée moderne a comme fonction celle de la protection de l'intimité, conçue non comme le contraire de la sphère politique mais de la sphère sociale ».

42 Les systèmes de chiffrement sont décrits par Polybe dans son ouvrage *Histoires*, livre X, chap. 7, par 45.6 et s.

43 M. IASELLI e S. GORLA, *Storia della Privacy*, Lex et Arts, 2015, p. 10 et s.

44 Les origines modernes de la vie privée, remontent traditionnellement à deux juristes américains, Samuel WARREN et Louis BRANDEIS, qui ont publié un essai intitulé *The Right to Privacy. L'implicite rendu explicite*. Pour aller plus loin Voy. S. COGLIO, *Transforming Privacy: A Tran- spersonal Philosophy of Rights*, ed. Praeger, Westport, 1998, pp. 187-202.

45 G. ORWELL, *Big Brother*,*1984*, Gallimard, 1950.

46 Voy. L'article 12 de la Déclaration Universelle et l'article 17 du pacte relatif aux droits civils et politiques.

47 L. BURGORGUE-LARSEN, *L'appréhension constitutionnelle de la vie privée en Europe*, in F. Sudre (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 111, spéc. p. 99-100.

d'un contexte historique et culturel d'origine américaine[48], a trouvé sa pleine reconnaissance dans le cadre juridique européen et a dominé jusqu'aux besoins d'une société technologiquement avancée en demande d'une redéfinition. Le droit à la vie privée a donc acquis un nouveau sens, qu'il ne pouvait pas avoir aux siècles précédents : cela comprend maintenant le droit, reconnu aux citoyens, d'exercer également un contrôle sur l'utilisation de leurs propres données personnelles. Le droit à la vie privée, en raison de la nouvelle dimension acquise, n'est plus compris dans un sens purement négatif, comme une faculté d'empêcher l'intrusion d'étrangers dans la vie privée, de refuser la diffusion d'informations personnelles, de renoncer à toute participation à la vie sociale. Il l'est dans un sens positif, comme une affirmation de la liberté et de la dignité de la personne, et comme la capacité de limiter le pouvoir ordinateur, en vérifiant les moyens et les fins. La conception européenne de vie privée comme droit fondamental au sein de l'Union européenne, tire très probablement son origine de raisons à caractère historique. Si l'on considère, en effet, que les États-Unis n'ont jamais expérimenté la dictature comme forme de gouvernement, il n'y a pas de doutes sur le fait qu'en Europe, face aux régimes nazi et fasciste, il y a eu l'exigence de garantir une protection de la sphère privée contre toute intrusion. La manipulation des données personnelles « sensibles » pour des fins politiques (si l'on pense à la race, au credo religieux, à l'affiliation syndicale comme à l'orientation sexuelle) a été utilisée comme une pratique généralisée, pour la réalisation d'une politique répressive ou raciste de la part des régimes autoritaires en Europe. Il suffit de rappeler, dans le cas de l'Italie, l'émanation des lois raciales[49]. Toutefois, il convient de constater que cette notion n'est pas précisée par le droit. Il s'agit donc d'une construction progressive prétorienne, qui s'est fixée au gré des jugements et qui englobe aussi bien le droit à l'intimité que le droit au secret des correspondances écrites, téléphoniques et électroniques et le droit à l'image. Non seulement la jurisprudence ne permet pas de dégager une définition globale de la vie privée, mais il en ressort que le respect qui lui est dû n'est pas absolu : la liberté d'expression ou l'intérêt public peuvent éventuellement justifier des atteintes à ce droit.

5 L'apport de la jurisprudence et de la doctrine. Un examen des législations passées et présentes en matière de protection des données montre que la protection des données à caractère personnel est un droit récent et en phase avec les évolutions de la société. Sa consécration dans la Charte des droits fondamentaux est le résultat du mouvement d'émancipation du droit à la vie privée[50] , consacré par l'article 8 de la ConventionEDH de 1950. D'ailleurs, les États européens n'ont pas tous consacré dans leur constitution un droit à la protection des données personnelles. Ce sont principalement les constitutions récentes, adoptées à partir des années

48 Le contexte de référence est le dix-neuvième siècle, marqué sur le plan social d'un fort désir d'intimité familiale, conjugale et personnelle. Comme le souligne M. PERROT, « Modi di abitare », in P. Ariès. G.Duby (édité par), *La vita privata*, Roma-Basi, 2001, vol. IV, p. 245 : « la plus grande intolérance aux contraintes imposées par la promiscuité ou par le voisinage, et le rejet croissant de la structure panoptique dans les bâtiments collectifs - prisons, hôpitaux, casernes, ou par les contrôles effectués sur des individus ».

49 R.D.L. 15 novembre 1938, n. 1779 « Integrazione e coordinamento in testo unico delle norme già emanate per la difesa della razza nella scuola italiana », *R.D.L.* 7 settembre 1938, n. 1381 recante "Provvedimenti nei confronti degli ebrei stranieri », *R.D.L.* 29 Giugno 1939, n. 1054 recante « Disciplina dell'esercizio delle professioni da parte dei cittadini di razza ebraica ».

50 Voir aussi dans les instruments internationaux la Déclaration universelle des droits de l'homme reconnaissant le droit à la vie privée dans son art. 12 et l'art. 1er de la Convention sur les droits civil et politique.

1970, qui traduisent ces préoccupations [51] . En droit français la protection des données personnelles n'a fait l'objet d'aucune consécration constitutionnelle[52] mais, lorsque la question s'est posée, l'assimilation à la protection de la vie privée a été le plus souvent la solution préconisée[53]. En Italie, le débat sur le thème de la vie privée n'a commencé qu'après les années 1950 lorsque, proches de la réforme du code civil, certains juristes italiens ont commencé à s'intéresser à la « vie privée », en la situant dans le contexte plus général des droits individuels[54]. A partir de ce moment le « droit à la *privacy* » a développé un vaste débat doctrinal. L'affaire « Soraya »[55] est considérée comme la principale affaire en la matière où le droit à la vie privée a été pleinement reconnu par la jurisprudence italienne. Les juges de la Cour de cassation ont identifié un fondement implicite du droit à la *privacy*, identifié « dans cet ensemble de normes ordinaires et constitutionnelles qui, en protégeant des aspects particuliers de la personne, dans le système de l'ordre substantiel, ne peuvent que se référer aussi à la sphère privée de celui-ci »[56]. Les textes internationaux et européens de protection des droits fondamentaux à portée générale reconnaissent souvent un droit au respect de la vie privée[57] mais ils ne disent rien sur le droit à la protection des données personnelles. Ainsi les jurisprudences européennes ont dégagé un droit à la protection des données personnelles sur le fondement du droit au respect de la vie privée. Le principe d'interprétation défini par la Cour européenne, selon lequel la Convention est « un instrument vivant à interpréter à la lumière des conditions de vie actuelle »[58], trouve un domaine d'application privilégié avec le droit au respect de la vie privée et familiale. Celui-ci est le fruit d'un dialogue continu des jurisprudences qui se sont appuyées sur le droit au respect de la vie privée. La reconnaissance de nouveaux droits fondamentaux par

---

51 Voy. par ex. la Constitution espagnole du 27 décembre 1978 (art. 18 § 4) et la Constitution portugaise du 2 avril 1976 (art. 35).

52 Le Comité de réflexion sur le préambule de la Constitution n'a pas estimé nécessaire de procéder à une telle inscription car ce droit est déjà reconnu par les jurisprudences européennes et la jurisprudence constitutionnelle française v. Comité de réflexion sur le préambule de la constitution, *Redécouvrir le Préambule de la Constitution, Rapport au Président de la République*, 2008, sp. p. 94-96. Sur ce même constat de la reconnaissance de droit par les jurisprudences européennes et la jurisprudence constitutionnelle française v. Conseil d'État , Étude annuelle 2014. *Le numérique et les droits fondamentaux* , p. 70 et s.

53 En effet, le Conseil constitutionnel, grâce à une interprétation extensive de la notion de liberté individuelle, a dégagé une conception indirecte de protection des données personnelles. Voy les décisions DC 83-164 de 1983, DC 84-184 de 1984, DC 90-281 de 1990, DC 93-316 de 1993, DC 95-352 de 1995, DC 96-377 de 1996 et DC 97-389 de 1997.A défaut d'une « charte du numérique », les députés ont voté dans la nuit de mercredi à jeudi 19 juillet 2018 l'inscription de la « *protection* » des données personnelles dans la Constitution. La loi fixera les règles concernant la protection des données à caractère personnel, prévoit cet amendement des rapporteurs et du groupe LREM au projet de révision constitutionnelle. Une semaine auparavant l'Assemblée avait rejeté au terme d'un vif débat l'inscription dans la Constitution d'une « charte du numérique », souhaitée par des parlementaires de tous bords mais critiquée par gouvernement et rapporteurs qui avaient estimé le travail « inabouti ». Cette charte, rédigée par un groupe de travail transpartisan Assemblée-Sénat, listait droits et libertés à l'ère du numérique. Voir l'article publié dans le journal *Le Monde* disponible à l'adresse : https://www.lemonde.fr/pixels/article/2018/07/19/l-assemblee-inscrit-la-protection-des-donnees-personnelles-dans-la-constitution_5333463_4408996.html

54 A. DE CUPIS, *I diritti della personalità*, Milano, 1942, p112.

55 Voy. Corte di Cassazione 27 maggio 1975 n. 2129.

56 Voy. Cass., 27 mai 1975, n. 2129.

57 Voy. art. 12 de la Déclaration universelle des droits de l'homme, art. 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, art. 17 du Pacte des Nations Unies relatif aux droits civils et politiques, article 16 de la Convention de New York sur les droits de l'enfant.

58 CEDH, Tyrer c. Royaume-Uni, 25 avril 1978, §31.

la jurisprudence soulève en effet la question de la légitimité du juge et de son pouvoir créateur. C'est pourquoi, lorsque la CourEDH reconnaît un nouveau droit, elle ne le consacre pas *ex nihilo* mais le déduit d'un autre droit expressément reconnu, assurant ainsi une « protection par ricochet »[59]. Ainsi les textes internationaux et européens de protection des droits fondamentaux qui entendent protéger la vie privée ne la définissent pas et ils ne reconnaissent pas expressément un droit à la protection des données personnelles[60]. S'il est facile de dire que les données personnelles, bien qu'ayant aujourd'hui une autonomie propre, peuvent faire partie de la vie privée, il est plus difficile de savoir ce qu'est la vie privée. D'ailleurs les jurisprudences européennes n'ont pas davantage cherché à définir la notion de vie privée, la CourEDH affirme ainsi, dans l'affaire *Nietmietz c. Allemagne*[61], qu'elle « ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de vie privée » en jugeant que la protection de l'article 8 ne couvre pas seulement la sphère intime des relations personnelles, mais aussi le droit pour l'individu de nouer et développer des relations avec ses semblables. Dans l'affaire *Pretty c. Royaume-Uni*[62], la CourEDH affirme que « la notion de vie privée est une notion large, non susceptible d'une définition exhaustive ». Pour les juges de Strasbourg, la vie privée est un concept qui ne se prête pas à une définition exhaustive. Ce concept est notamment plus large que celui de droit à l'intimité (*privacy* dans les pays de *Common Law*) et concerne une sphère au sein de laquelle toute personne peut librement développer sa personnalité et s'épanouir. Il est devenu manifeste qu'il fallait garantir aux citoyens une protection renforcée contre les tiers (en particulier l'État). Ainsi en 1992, la CourEDH a déclaré : « Il serait toutefois trop restrictif de limiter le concept de vie privée à un "cercle intime" où chacun peut mener sa vie personnelle à sa guise et d'écarter entièrement le monde extérieur à ce cercle. Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables »[63]. De sorte que la vie privée inclut nécessairement le droit de développer des relations avec d'autres personnes et avec le monde extérieur. Pendant longtemps, il n'existait, dans l'environnement juridique européen, aucune réglementation en matière de protection des données. C'est avec la Convention européenne des droits de l'homme que l'on a essayé de combler cette lacune au niveau européenne. Toutefois l'article 8 CEDH, ne fait pas référence explicitement à la protection des données personnelles. Cependant, l'interprétation « évolutive » et « dynamique » opérée par la Cour de Strasbourg, qui prend en compte l'évolution de la société et notamment l'émergence des nouvelles technologies, l'a conduite à inclure le droit à la protection des données personnelles dans le champ d'application de l'article 8 de la Convention, comme les obligations positives à la charge de l'État pour garantir le respect effectif de ce droit. Toutefois ce droit a fait bientôt l'objet d'une protection

---

59 F. SUDRE, *Droit européen et international des droits de l'homme*, 2016, p. 690. La protection par ricochet permet aux organes de la CEDH d'étendre la protection de certains droits garantis par la CEDH à d'autres droits non protégés par exemple en matière de protection de l'environnement, de protection des étrangers, de protection des détenus. Certains droits comme le droit à la vie, l'interdiction des traitements inhumains et dégradants ou le droit au respect de la vie privée constituent les vecteurs principaux de ces protections indirectes v. sur ce mécanisme pour la protection des étrangers.

60 F. SUDRE, Op. Citée. p. 690.

61 CEDH, Nietmiez c. Allemagne, 16 décembre 1992, req.n° 13710/88, §29.

62 CEDH, Pretty c. Royaume-Uni, 29 avril 2002, req.n°2346/02, §61.

63 CEDH, Niemietz c. Allemagne, 16 décembre 1992§ 31.

distincte. Définir la vie privée n'est pas évident. Un certain nombre de professeurs de droit, philosophes, sociologues et psychologues ont essayé d'en trouver une définition satisfaisante[64]. La doctrine a développé des théories pour définir la vie privée. Toutefois aucune d'entre elles ne semble efficace. Avant de passer à l'analyse du droit à la protection des données personnelles il convient de se pencher sur la notion de vie privée dans laquelle le droit à la protection des données personnelles trouve son origine selon l'approche classique et alternative.

6 L'approche classique. Selon l'approche classique, la notion de vie privée pourrait découler de sa définition négative, c'est-à-dire comme ce qui n'est pas public[65]. Les origines de cette approche remontent à la Grèce ancienne où la vie privée était considérée comme un manque de participation à la *polis.* Cette théorie a été reprise par le philosophe républicain Rousseau, lequel considérait que les préoccupations privées étaient une menace pour le bon fonctionnement du gouvernement[66]. Récemment Hannah Arendt a considéré que la vie privée est « l'état d'être privé de quelque chose »[67].Toutefois cette approche n'est pas efficace dans la pratique car il y a des situations où la démarcation privé/public n'est pas nette. Ainsi la CourEDH dans l'affaire *Perry c. Royaume-Uni* souligne que : « Il existe donc une zone d'interaction entre l'individu et autrui qui, même dans un contexte public, peut relever de la vie privée »[68].
Selon d'autres auteurs, le critère spatial pourrait délimiter la vie privée. Pour ces derniers, est privé tout ce qui se passe au domicile. Cette approche dévoile toutefois ses limites car il y a bien des actes accomplis dans des endroits publics qui relèvent du for intérieur et intéressent la liberté de conscience[69]. À défaut de ces critères conceptuels, d'autres auteurs ont développé une approche descriptive se fondant sur une énumération de l'ensemble des éléments composant la vie privée. Feraient alors partie de la notion de vie privée les informations concernant les opinions, les croyances religieuses, politiques, la vie sexuelle [70] . Cette définition montre également ses limites car les éléments proposés dans la liste varient selon un auteur à l'autre et il faudrait s'interroger sans cesse au cas par cas pour déterminer si tel élément fait ou non partie de la vie privée. Il faudrait donc trouver un critère qui permet de prendre en compte la relativité du contenu de la notion et ainsi de rendre cohérentes les intégrations ou les exclusions de certains éléments de son champ d'application[71].

---

64 A. MOORE, *Privacy Rights: Moral and legal foundations*, University Park PA, The Pennsylvania State University Press, 2010, p. 237.

65 Voy. R. LINDON, *La presse et la vie privée,* J.C.P. éd. G 1965, I, 1887, n°1 et R. BADINTER, *Le droit au respect de la vie privée*, J.C.P. éd. G 1968, I, n° 2136.

66 JJ. ROUSSEAU, *Du contrat social* (1762), in Œuvres complètes de Jean-Jacques Rousseau, Paris Gallimard (Pleiade), 1964.

67 H. ARENDT, *The Human condition,* Chicago University of Chicago Press, 1998, p.38.

68 CEDH, Perry c. Royaume-Uni, 17 juillet 2003, req. n° 63737/00, §36.

69 Voy. Cass.crim., 28 février 1874.

70 Voy. R. LINDON, *Les droits de la personnalité*, Dictionnaire juridique, 1983 p. 261 et M. DUPUIS, *Protection de la vie privée*, Lamy Droit des personnes, sous la direction de F. DEKEUER-DEFOSSEZ, 2013, p.39.

71 J. EYNARD, *Les données personnelles, quelle définition pour un régime de protection efficace*?, Michalon 2013, p. 57.

7 L'approche alternative. Les tentatives de définir la notion de vie privée se sont heurtées au caractère changeant de son contenu et à sa relativité dans le temps et dans l'espace. Sur la base du fait que la notion de vie privée est un concept relatif dans le temps et dans l'espace, une approche alternative a été dégagée qui consiste à ne plus appréhender la vie privée comme une notion statique[72] mais comme une notion dynamique qui évolue avec la société. Cette approche est une tentative de définir la vie privée tout en intégrant sa relativité à trois égards : premièrement, la vie privée relève de la relativité temporelle, ce qui fait partie de la vie privée à un moment historique donné n'en fait pas forcément partie à une autre époque ; ainsi par exemple en droit français le patrimoine était conçu à l'origine comme une émanation de la personnalité et donc protégé au titre de la vie privée. Deuxièmement, la notion de vie privée dépend de la relativité de la personne concernée, ainsi la CourEDH a décidé que « les questions patrimoniales concernant une personne menant une vie publique (…) ne relèvent pas du domaine de la vie privée »[73]. En dernier lieu, s'ajoute une relativité de contenu : la notion de vie privée doit tenir compte de la relativité subjective, tenant compte du caractère sensible de l'information.

B. L'autonomisation du droit à la protection des données personnelles

8 L'absence d'un droit autonome dans les textes internationaux. Le droit à la protection des données personnelles n'apparaît ni dans la Déclaration universelle des droits de l'homme de 1948, ni dans la Convention européenne des droits de l'homme de 1950, ni dans les Pactes internationaux des Nations-Unies relatifs aux droits civils et politiques et aux droits économiques, sociaux et culturels de 1966. C'est avec l'évolution technologique que plusieurs textes internationaux et européen ont établi un ensemble de règles relatives à l'utilisation des données personnelles mais sans leur consacrer un droit[74]. La protection des données à caractère personnel a été reconnue pour la première fois comme un droit distinct dans la Convention du Conseil d'Europe (Convention 108), qui a aussi constitué une importante source d'inspiration pour la directive 95/46/CE. Toutefois, les références au droit à la vie privée à l'article 1er de la Convention 108, ainsi que dans le préambule et à l'article 1er de la directive 95/46/CE attestent que le droit à la protection des données est étroitement lié au droit à la vie privée. L'absence d'une protection spécifique dans les textes internationaux n'a pas empêché les jurisprudences constitutionnelles des États membres de l'Union européenne de dégager le droit à la protection des données personnelles à partir du droit au respect de la vie privée [75] . En France, si la déclaration des droits de l'homme de 1789 reconnaît un droit à la sûreté, celui-ci s'entend essentiellement comme une protection de l'individu contre les abus du pouvoir. Il faut attendre

72 J. RAVANAS, *Jouissance des droits civils, protection de la vie privée. Délimitation de la protection,* Cl. Civ.art. 9, fac.1, 1989, n.13.

73 CEDH, Fressoz et Roire c. France, 21 janvier 1999, req.n° 29183/95.

74 L. COUDRAY, *La protection des données personnelles dans l'Union européenne*, Editions universitaires européennes, Editions universitaires européennes, Saarbruck, 2010, p. 32-58.

75 M-C. PONTHOREAU, « La reconnaissance des droits non écrits par les Cours constitutionnelles italienne et française. Essai sur le pouvoir créateur du juge constitutionnel», *Revue internationale de droit comparé*, 1995, p. 47 et s.

1970 pour que soit inséré dans l'article 9 du Code civil le principe selon lequel « chacun a droit au respect de sa vie privée ». L'article de Philippe Boucher paru le 21 mars 1974 dans *Le Monde*, « Safari ou la chasse aux Français », alertait l'opinion publique sur ces évolutions techniques et sur un projet qui, à partir du numéro de sécurité sociale et par une seule interrogation du fichier informatique, devait permettre à l'administration française de disposer de l'accès à l'ensemble des informations enregistrées sur une seule et même personne (sécurité sociale, fiscalité, police). Certes, le projet a été abandonné par le gouvernement français pour être remplacé par une législation protectrice, la loi informatique et libertés, qui, pour veiller à son application, a créé en France la première autorité administrative indépendante, la commission nationale de l'informatique et des libertés (CNIL). On soulignera que c'est en 1999 durant la discussion de la loi sur la couverture maladie universelle que le conseil constitutionnel a rattaché le droit à la vie privée à l'article 2 de la déclaration de 1789 (« la liberté proclamée par cet article 2 implique le respect de la vie privée »), lui donnant ainsi une portée constitutionnelle. Par conséquent le droit à la protection de la vie privée est récent et sa place dans la hiérarchie des normes reste fragile[76]. Seulement avec le temps on construira par le biais de la jurisprudence un nouveau droit constitutionnel à l'intimité. Ceci s'est principalement produit à travers la protection de diverses catégories. Ainsi, en Italie, personne ne met en question aujourd'hui l'existence d'un droit constitutionnel à la « *riservatezza* ». Ce droit a été construit par la juridiction ordinaire[77], mais la Cour constitutionnelle a garanti une telle protection dans deux arrêts de 1973. Toutefois, l'Italie a été l'avant-dernier pays européen, suivi seulement de la Grèce, à se doter d'une loi sur la protection de la vie privée (loi du 31 décembre 1996). En dépit du retard du législateur italien, il doit être précisé que la loi de 1996, faisant suite à la Directive communautaire relative à la protection des données personnelles, introduit un concept moderne de vie privée, qui ne se limite pas simplement à un « *right to be let alone* », selon la célèbre conception de la fin du XIXe siècle, mais qui se réfère plutôt à la protection de la personne humaine. Le concept de vie privée, entendu comme l'interdiction d'accéder à des informations personnelles, se transforme en un contrôle des renseignements relatifs à la personne.

9 Des raisons de caractère historique. La nécessité d'élaborer une législation spécifique en matière de protection des données tient à des raisons de caractère historique. Ce besoin commence à se faire sentir dès le début des années 1970 lorsque les États commencent à mettre en place des bases de données et des processus de traitement centralisés[78]. S'il est vrai que la Convention européenne des droits de l'homme et des libertés fondamentales, adoptée en 1950 par le Conseil de l'Europe, ne fait pas référence au droit à la protection des données personnelles, cette notion est bien qualifiée de droit fondamental par la Charte des droits fondamentaux de l'Union européenne dans son article 8. La première expression du détachement du droit à la

---

76 J-L. HALPERIN, *L'essor de la "privacy" et l'usage des concepts juridiques*, Droit et Société, 2005, p. 61.

77 Voy. Par exemple, Cass. 20.4.1963 n°990 ; Foro Italiano 1963.877.

78 En Allemagne, la *Bundesdatenschutzgesetz*, entrée en vigueur en 1977, succédait à la première loi nationale adoptée par la Chancellerie d'État du Land de Hesse. Il s'agit également de la première loi au monde en matière de protection des données personnelles. *Voy*. G. GONZALEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the* EU, Springer International Publishing, 2014 p. 56. En France la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.

protection des données personnelles du droit au respect à la vie privée au sein de l'Union européenne s'est faite par le traité d'Amsterdam. Ainsi l'article 286 du TCE révisé par le traité d'Amsterdam disposait que « les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes communautaires ». Toutefois, l'inscription de la protection des données personnelles au sein des textes du droit primaire, n'était pas formulée sous la forme d'un droit, et était encore limitée par la structure en piliers de l'Union européenne[79]. D'ailleurs, cela explique pourquoi la Cour de justice dans cette phase se réfère au principe général de droit sur le respect de la vie privée plutôt que sur l'art. 286 du TCE [80] . Ainsi la directive 95/46 ne valait que dans l'ancien premier pilier, expression de l'intégration plus poussée. La protection offerte par l'article 8 de la Charte [81] des droits fondamentaux est le point d'arrivée d'un parcours entrepris avec l'adoption de la Convention 108 du Conseil de l'Europe en 1981[82] qui a inspiré la jurisprudence de la CEDH et de la Cour de justice. Ainsi, bien avant l'adoption de textes normatifs prévoyant la reconnaissance du droit fondamental à la protection des données, le juge a assuré la défense *en concreto* des droits fondamentaux de la personne[83]. L'impact juridique du nouveau statut conféré à la Charte des droits fondamentaux de l'Union permet une consolidation des droits fondamentaux tels qu'ils résultent de différentes sources, parmi lesquelles la CEDH, les traditions constitutionnelles nationales et les obligations internationales des États membres, les Chartes sociales de l'Union et du Conseil de l'Europe, ainsi que la jurisprudence de la Cour de justice et de la CEDH[84]. La Charte résulte d'une cristallisation des droits fondamentaux existants dans les sources précitées.

---

79 En effet cette consécration ne valait que pour l'ancien premier pilier.

80 C'est d'abord dans le cadre du premier pilier que la Cour de justice a été saisie d'affaires relatives à l'utilisation des données personnelles et pour lesquelles elle a choisi de se fonder sur ce principe général du droit communautaire v. CJCE, 20 mai 2003, Rechnungshof c. Österreichischer Rundfunk et autres, aff. C-465/00, C- 138/01, C-139/01, Rec. I-4989 ; CJCE, 6 novembre 2003, Bodil Lindqvist, aff. C-101/01, Rec. I-12971. Toutefois, ce droit fondé sur les principes généraux du droit communautaire était également susceptible de concerner les deux autres piliers. Celui-ci aurait ainsi pu être appliqué dans l'affaire relative au transfert des données PNR si la Cour n'avait pas annulé les actes contestés pour défaut de base légale v. CJCE, G. Ch., 30 mai 2006, Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes, aff. C-317/04 et C-318/04, Rec. I-04721.

81 Voy. Les explications relatives à la charte des droits fondamentaux disponible à l'adresse : https://www.cvce.eu/content/publication/2010/6/9/11b81cf7-22fc-4463-873f-1db65a733a8c/publishable_fr.pdf
L'art. 8 a été fondé sur l'article 286 du traité instituant la Communauté européenne et sur la directive 95/46/CE du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (JO L 281 du 23.11.1995, p. 31), ainsi que sur l'article 8 de la CEDH et sur la Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel du 28 janvier 1981, ratifiée par tous les États membres. L'article 286 du traité CE est désormais remplacé par l'article 16 du traité sur le fonctionnement de l'Union européenne et l'article 39 du traité sur l'Union européenne. Il convient de noter également le règlement (CE) no 45/2001 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données (JO L 8 du 12.1.2001, p. 1). La directive et le règlement précités contiennent des conditions et limitations applicables à l'exercice du droit à la protection des données à caractère personnel.

82 Voy. Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel.

83 CJCE, *National Panasonic c. Commission* 1979, dans cette affaire la Cour déclare que la protection des données personnelles constitue un aspect implicite du plus étendu droit au respect de la vie privée, Voy. §18 et 19 de la décision.

84 G. ARESTIS, « Fundamental rights in the EU: three years after Lisbon, the Luxembourg perspective », *College of Europe, Research Papers in Law* 2/2013, p. 1-13.

On peut qualifier de « nouveaux » non pas les droits modernes et innovants auxquels la Charte se réfère occasionnellement (par exemple le droit à la protection des données à caractère personnel, le droit à un haut niveau de protection de l'environnement, etc.) mais plutôt le fait que ces droits, qui ne sont sans doute pas de nouveaux droits puisqu'ils bénéficient déjà d'une protection en vertu de divers instruments juridiques, n'avaient jusqu'ici jamais été considérés comme des droits autonomes. Toutefois cela ne les transforme pas en droits individuels directement opposables, ce qui signifie que les individus n'ont pas gagné de nouvelles « options » pour contester la légalité des actes pris par les institutions européennes ou les États membres. De manière similaire, le changement de statut de la Charte n'a pas conféré à l'Union de nouveaux pouvoirs. Les juridictions européennes, en revanche, doivent tenir compte du nouveau « statut » conféré aux droits énoncés par la Charte. Par ailleurs, lorsque les juridictions européennes doivent contrôler la légalité de mesures prises par les institutions européennes ou de mesures nationales relevant du champ d'application du droit européen, elles doivent annuler toute législation de l'Union contraire et le juge national devra écarter les dispositions nationales incompatibles.

10 La consécration d'un droit autonome dans le droit primaire de l'Union européenne. Le résultat de ce long processus est la proclamation à Nice de la Charte des droits fondamentaux avec la consécration de l'art.8 relatif à la protection des données personnelles comme un droit distinct de l'art.7 relatif à la vie privée[85]. La protection de données à caractère personnel peut donc être appréhendée comme un droit fondamental. Cela signifie que le droit à la protection des données apporte forcément quelque chose en plus au droit à la vie privée[86]. Ainsi l'art. 8 de la Charte reconnaît dans son premier paragraphe l'existence du droit à la protection des données personnelles : « toute personne a droit à la protection des données à caractère personnel la concernant ». Le deuxième paragraphe concerne le contenu du droit à la protection des données personnelles avec la liste des exigences du traitement des données : « ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification ». Le troisième paragraphe concerne sa mise en œuvre par une autorité de contrôle indépendante. Le droit à la protection des données personnelles et le droit au respect de la vie privée sont deux droits distincts. D'une part, le concept de vie privée est beaucoup plus large que celui de données personnelles, d'autre part il peut y avoir des données personnelles qui ne sont pas privées comme observé par la Cour de justice dans l'affaire *Bavarian Laeger*[87]. Cela a été précisé par la Cour de justice dans l'affaire *Client Earth :* « les concepts de données personnelles et de

85 La Charte signée à Nice le 7 décembre 2000, réaffirme, dans le respect des compétences et des tâches de l'UE, ainsi que du principe de subsidiarité, les droits qui résultent notamment des traditions constitutionnelles et des obligations internationales communes aux pays de l'UE, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, des chartes sociales adoptées par l'UE et le Conseil de l'Europe, ainsi que de la jurisprudence de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme. En donnant visibilité et clarté aux droits fondamentaux, la charte instaure une sécurité juridique au sein de l'UE.

86 O. LYNSKEY, *Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order*, International and Comparative Law Quarterly, 2014, Vol. 63, No. 3, p. 569–597.

87 Voy. T-194/04 Bavarian Lager, 8 novembre 2007, §118-119.

données relatives à la vie privée ne doivent pas être confondus »[88]. Lorsque la Charte a été reconnue comme ayant la même valeur juridique que les traités, on a assisté à l'accomplissement au niveau de l'Union du processus de constitutionnalisation. Plus particulièrement, le droit à la protection des données personnelles y trouve son autonomisation par rapport à d'autres situations subjectives comme le droit à la vie privée[89]. Sont considérées comme données personnelles, toutes les informations identifiant directement ou indirectement une personne physique et non pas les informations qui pourraient affecter la vie privée d'un individu. Cela montre que le droit à la protection des données personnelles et le droit à la vie privée sont distincts. De plus, le droit à la protection des données personnelles sert d'autres droits fondamentaux et valeurs tels que la transparence, l'*accountability* et le traitement licite. D'ailleurs la sécurité des informations et la qualité sont des valeurs garanties par la mise en œuvre d'un traitement licite des données personnelles. La protection des données personnelles vise aussi à protéger la dignité inscrite à l'art. 1 de la Charte et à l' art. 2 du TUE. En effet, l'exercice des libertés individuelles comme la liberté d'expression, d'associations, etc. serait inhibé si l'individu croit que le traitement des données et ses finalités ne respectent pas les principes légaux de collecte. Cela aurait en effet un impact sur le droit à l'autodétermination. De plus, le droit à la protection des données personnelles garantit aussi l'absence d'une discrimination liée à un traitement inégal des individus fondé sur des caractéristiques collectées à travers des techniques de profilage. La question que l'on pourrait se poser ici est de savoir si le droit à la protection des données personnelles peut rester « seul ». Afin d'y répondre il semble que le droit fondamental à la protection des données personnelles doit constituer une notion autonome par rapport à la législation de droit secondaire, il doit pouvoir résister dans la mise en balance avec d'autres droits fondamentaux et il doit fonctionner tant négativement que positivement (il doit pouvoir limiter le pouvoir et le réguler). Concernant la première condition, les explications de la Charte se réfèrent à la directive 95/46 et à la Convention 108. Toutefois, le contenu de l'art. 8 de la Charte reste autonome par rapport aux principes mis en place dans la législation secondaire. Concernant la deuxième condition, le droit à la protection des données n'est pas un droit absolu, il peut subir des restrictions. Toutefois ces limitations sont strictement encadrées et il se peut que ce droit « résiste » vis-à-vis d'autres droits dans un contrôle à posteriori par le juge. Enfin, la troisième condition semble respectée lorsque l'on regarde l'« essence » du droit à la protection des données personnelles. Ainsi dans l'affaire *Digital Rights*, la Cour de justice estime que l'essence de ce droit a été respectée puisque des normes de sécurité avaient été prises en compte pour protéger les données personnelles. Elle estime alors que ce n'est pas la communication des données qui a été saisie mais seulement celle des métadonnées. Il semble alors que ce droit peut opérer positivement dans la régulation (par exemple à travers les mesures de sécurité prises pour garantir la confidentialité des données) et négativement dans l'interdiction d'accès au contenu des communications. Il est intéressant de souligner que ce droit faisait déjà l'objet d'une protection spécifique dans certains ordres

88 Voy. CJUE, Client Earth C-615/13, 16 juillet 2015, §32.

89 A. DI MAJO, « Il trattamento dei dati personali tra diritto sostanziale e modelli di tutela », in *Studi in onore di Pietro Rescigno II* ; « Diritto privato, 1 », in *Persone, famiglia, successioni e proprietà*, Milano, 1998, p. 263, spéc.p. 271.

constitutionnels des États membres[90]. Suite à cette autonomisation du droit à la protection des données personnelles, les expressions comme « vie privée » ou « *privacy* » doivent être employées avec attention[91]. La véritable consécration d'un droit autonome à la protection des données personnelles remonte au Traité de Lisbonne. Ainsi l'article 16 du Traité sur le fonctionnement de l'Union européenne affirme que le champ d'application de ce droit n'est désormais plus limité par la structure en piliers de l'Union européenne. Par conséquent, ce droit s'applique quels que soient les secteurs concernés. De plus, l'article 6 paragraphe 1 du Traité sur le fonctionnement de l'Union européenne a conféré une valeur juridique équivalente au droit primaire à la Charte des droits fondamentaux de l'Union européenne qui reconnaît en son article 8 un droit à la protection des données personnelles distinct de l'article 7 concernant la vie privée. L'association entre droit à la vie privée et droit à la protection des données personnelles a donc été rejetée par la Charte des droits fondamentaux de l'Union européenne qui a reconnu cette dernière comme un droit autonome. Or, si la Charte « a été conçue comme devant constituer une codification de l'acquis existant de l'Union européenne, plutôt que comme la proclamation de droits nouveaux »[92], la distinction entre le droit au respect de la vie privée et le droit à la protection des données personnelles est bien nouvelle. Ainsi deux approches différentes qui expliquent le phénomène de l'autonomisation du droit à la protection des données personnelles ont vu le jour : l'approche des séparatistes et l'approche des instrumentalistes.

11 L'approche des séparatistes. Parmi les séparatistes la contribution la plus exhaustive a été apportée par Paul de Hert et Serge Gutwirth[93]. Selon cette approche, la fonction du droit à la protection des données et celle du droit à la vie privée sont différentes. D'une part, le droit à la vie privée tend à la non interférence, à protéger les individus contre l'utilisation illégitime du pouvoir, tandis que le droit à la protection des données tend à réguler et non à prohiber le flux d'informations la concernant dans un esprit de transparence[94]. Le concept de « vie privée » a été largement interprété dans la jurisprudence et par la doctrine [95] , comme couvrant des situations intimes, des informations sensibles ou confidentielles, des informations pouvant nuire à la perception du public contre un individu, voire des aspects de la vie professionnelle et du comportement public. Cependant, l'évaluation de l'existence ou non d'une ingérence dans

---

90 Voy. l'art. 35, Constituição da República Portuguesa, l'art. 18, comma 4, Constitución española du 27 décembre 1978 et l'art. 10 della Costitution Olandaise du 17 février 1983, les constitutions des Länder allemands. N'oublions pas que la Grèce dans sa révision constitutionnelle de 2001 a inséré un article sur la protection des données (art. 9A).

91 J. EYNARD, *Les données personnelles. Quelle définition pour un régime de protection efficace* ? Paris 2013, p. 53.

92 O. DE SCHUTTER, *Les droits fondamentaux dans l'Union européenne,* JDE, 2008, n° 148, p. 126 et s.

93 P. DE HERT et S GUTWIRTH, « Privacy, data protection and law enforcement. Opacity of the Individual and transparency of power », in E. CLAES et al (eds), *Privacy and the criminal law*, Antwerpen, Intersentia, 2006, p. 61-81.

94 Voy. J. KOKOTT and C. SBOTTA, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », International Data Privacy Law, 2013, p. 222.

95 B. BEIGNER, *Vie privée et vie publique*, Archives de philosophie du droit, 1997, p. 170.

la « vie privée » dépend du contexte et des faits de chaque cas. Par exemple, lorsqu'un employeur enregistre des informations relatives aux noms et à la rémunération des employés, le simple enregistrement de ces informations ne peut être considéré comme une ingérence dans la vie privée. Une telle ingérence pourrait toutefois être invoquée si, par exemple, l'employeur transmettait les informations personnelles des employés à des tiers. Les employeurs doivent dans tous les cas se conformer aux règles de protection des données car l'enregistrement des informations des employés constitue un traitement de données.

En revanche, dans certaines circonstances, le risque d'atteinte à la vie privée du fait d'un traitement de données à caractère personnel est incontestable. Tel est le cas par exemple dans l'hypothèse de collecte d'empreintes digitales[96].

Il a été souligné[97] que le droit au respect de la vie privée et familiale est avant tout le reflet d'une préoccupation individualiste. À l'inverse, la protection des données définit des règles et des mécanismes de traitement des données et donne à chacun la possibilité d'agir et de maîtriser son patrimoine informationnel. Le premier droit est statique et négatif tandis que le second est dynamique. De plus, dans le cas des données personnelles, le contrôle n'est pas laissé aux seuls sujets mais aussi confié à une autorité indépendante. Par ailleurs, la référence au droit à la vie privée est moins explicite dans le RGPD.

À la différence de la solution retenue dans la directive 95/46, le droit à la vie privée ne fait pas l'objet d'une réception distincte des autres droits et libertés fondamentaux[98]. En particulier, l'objectif du règlement (UE) n° 2016/679 n'est plus la protection « *des droits et libertés fondamentaux et notamment de la vie privée* », mais la protection « *des libertés et droits fondamentaux des personnes physiques et en par- ticulier leur droit à la protection des données à caractère personnel* »[99]. Cela montre le processus d'autonomisation du droit fondamental à la protection des données personnelles par rapport au droit à la vie privée[100]. En effet, le droit à la protection des données personnelles doit être distingué de la liberté négative de ne pas subir d'interférences dans sa propre vie privée, ici le droit est constitué par la liberté positive d'exercer un contrôle sur le flux de ses propres renseignements. Pour cette raison il est fréquent

96 CJUE, n° C-291/12, Michael Schwarz c/ Stadt Bochum, 17 octobre 2013; CJUE 16 avril 2015, affaires jointes C-446/12 à C 449/12.

97 S. RODOTA, *Nouvelles technologies et droits de l'homme : faits, interprétations, perspectives, Mouvements*, vol. 62, p. 55-70.

98 M.CLEMENT FONTAINE, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *LEGICOM* 2017/2 (N° 59), p. 61-68, spéc.p. 64.

99 Règlement (UE) n° 2016/679 notamment voir le considérant 2 et l'article 1 paragraphe 2.

100 R. PARDOLESI, *Dalla riservatezza alla protezione dei dato personali: una storia di evoluzione e di discontinuita*, Vol. I e II, Milano, Passim, 2003 p. 143 ; Pour un cadre avant l'adoption de la directive 95/46 voy. : GIAMPICCOLO, *La tutela giuridica della persona umana e il c.d. diritto alla riservatezza*, in *Riv. trim. dir. proc. civ*., 1958, p. 458 et ss.; DE CUPIS, *I diritti della personalita*, t. 2, in *Tratt. Cicu-Messineo*, Milano, 1961, p. 15 ss.; PUGLIESE, « Il preteso diritto alla riservatezza e le indiscrezioni cinematografiche », in *Foro it*., 1954, p. 116 ss.; P. RESCIGNO, « Il diritto di essere lasciati soli », in *Synteleia Vincenzo Arangio Ruiz*, I, Napoli, 1964, p. 494 ss.; M. GIORGIANNI, *La tutela della riservatezza* , in *Riv. trim. dir. proc. civ*., 1970, p. 13 ss.; A. CATAUDELLA, *La tutela della vita privata*, Milano, Passim 1972, G.B. FERRI, *Persona e privacy*, in *ID., Persona e formalismo ridico*. Saggi di diritto civile, Rimini, 1987, p. 241 ss.; G. GIACOBBE, *Riservatezza* (diritto alla), in *Enc. dir*., XL, Milano, 1989, p. 1243 ss.

que le droit à la protection des données personnelles soit entendu comme droit à « l'autodétermination informative »[101].

Au contraire, l'approche des instrumentalistes voit dans la protection des données une évolution du droit à la vie privée liée au développement des technologies[102]. D'ailleurs la Cour de justice semble justifier la plus-value de l'article 8 de la Charte consacré à la protection des données personnelles par rapport à celui de l'article 8 de la CEDH consacrant la protection de la vie privée. Ainsi dans l'arrêt *Tele2 Sverige*, il a indiqué que la protection des droits fondamentaux repose sur la seule Charte dont les droits correspondants devraient être interprétés conformément au droit de la Convention EDH mais peuvent se voir reconnaître une protection plus étendue et que l'article 8 de la Charte concerne un droit fondamental distinct de celui consacré à l'article 7 de celle-ci et qui n'a pas d'équivalent dans la CEDH[103].

12 L'approche des instrumentalistes. Parmi les instrumentalistes, Antoniette Rouvroy et Yves Poullet estiment que le droit à la protection des données est instrumental au droit fondamental à la vie privée [104] . Finalement, seuls les séparatistes reconnaissent une valeur ajoutée au droit à la protection des données personnelles. Cela ne veut pas dire que les deux droits ne sont pas étroitement liés[105], et la vie privée est une notion qui peut enclore les données personnelles. Le droit à la protection des données personnelles s'est affranchi du droit au respect de la vie privée. Néanmoins les deux droits sont étroitement liés, ils s'efforcent de protéger des valeurs similaires, c'est-à-dire l'autonomie et la dignité humaine des individus en leur accordant une sphère personnelle dans laquelle ils peuvent librement développer leur personnalité, exprimer leur liberté de religion, et leur liberté d'expression[106]. Néanmoins, les deux droits sont différents dans leur formulation et dans leur portée. Le droit au respect de la vie privée consiste en une interdiction générale de l'ingérence, sous réserve de certains critères. Le droit fondamental à la protection des données personnelles comme formulé dans l'article 8 de la Charte des droits fondamentaux, affirme non seulement le droit à la protection des données personnelles, mais énonce également les valeurs fondamentales associées à ce droit. Il dispose

---

101 D. GUTMANN, *Le sentiment d'identité. Etude de droit des personnes et de la famille*, Paris, 2000, spec.p. 9.; L.L. CHRISTIANIS, « Dimensions philosophique et religieuses des approches juridique de l'identité », in J. POUSSON-PETIT, *L'identité de la personne humaine. Etude de droit français et de droit comparé*, Bruxelles, 2002, p. 63 ss.

102 M. TZANOU, *The fundamental right to data protection, normative value in ther context of counter-terrorism surveillance*, Hart Publishing 2017, p. 35.

103 CJUE, Tele2 Sverige, aff. Jointes C-203/15 et C-698/1, §130.

104 A. ROUVOROY et Y. POULLET, « The right to informational self-determination and the values of self-developpement : reassessing the importance of privacy for democracy ? », in S. GURWIRTH and others (eds), *Reinventing Data protection ?*, New York, Springer, 2009, p.45.

105 CJUE, 9 novembre 2010, Volker un Markus Schecke GbR et a. c/ Land Hessen, C-92/09; C-93/09, La Cour considère en effet que le droit fondamental à la protection des données à caractère personnel « *est étroitement lié au droit au respect de la vie privée* »[31]. Plus encore, selon la Cour, « *la protection des données à carac- tère personnel, résultant de l'obligation explicite prévue à l'article 8 de la Charte, revêt une impor- tance particulière pour le droit au respect de la vie privée* ».

106 P. HUSTINX, EDPS,Speeches& Articles, «*EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation* , July 2013, disponible à l'adresse/ https://edps.europa.eu/data-protection/our-work/publications/speeches-articles/eu-data-protection-law-review-directive_en

que le traitement des données à caractère personnel doit être loyal et fondé sur le consentement de la personne concernée ou sur une base légitime. Les individus doivent avoir le droit d'accéder à leurs données personnelles et de les faire rectifier. De plus, le respect de ce droit doit être soumis au contrôle d'une autorité indépendante. Le droit à la protection des données personnelles intervient lorsque des données personnelles sont traitées. Toute opération de traitement de données personnelles fait l'objet d'une protection appropriée. La protection des données concerne toutes sortes de données à caractère personnel et de traitement de données, quelle que soit la relation et l'impact sur la vie privée. Ce droit est donc plus large que le droit au respect de la vie privée. Par exemple, il n'est pas nécessaire de démontrer une atteinte à la vie privée pour que les règles de protection des données soient appliquées. Au contraire, le droit à la vie privée concerne des situations où un intérêt privé, ou la «vie privée» d'un individu, a été compromis.

Suivant ce raisonnement, la Cour a invalidé, la directive 2006/24/CE relative à la conservation des données électroniques[107]. Elle a, par ailleurs, affirmé dans le célèbre arrêt Google Spain[108], que les dispositions relatives au traitement des données personnelles devaient s'interpréter au regard de l'article 1er, paragraphe 1, de la directive du 24 octobre 1995, aux termes duquel : « *Les États membres assurent, conformément à la présente directive, la protection des libertés et droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel* ». Depuis, elle précise « à titre préliminaire » dans ses décisions que « *les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptibles de porter atteinte aux libertés fondamentales et, en particulier, au droit à la vie privée, doivent nécessairement être interprétées à la lumière des droits fondamentaux qui, selon une jurisprudence constante de la Cour, font partie intégrante des principes généraux du droit dont celle-ci assure le respect et qui sont désormais inscrits dans la Charte* »[109].

Si l'on peut douter de l'existence d'une plus-value tangible de l'article 8 de la Charte par rapport à l'article 8 de la Convention EDH, il n'en demeure pas moins que la Charte bénéficie en matière de protection des données personnelles d'un avantage considérable. Le régime juridique de ce droit étant principalement défini au niveau de l'Union européenne et ayant vocation à se développer, jouant un rôle de premier plan dans la protection des individus contre les excès de la société de l'information.

13 La dimension internationale de la réglementation en matière de données personnelles.

La première caractéristique de la réglementation juridique de l'utilisation des données personnelles consiste dans sa dimension internationale avec l'essor des nouvelles technologies de l'information et de la communication.

---

107 CJUE, 8 avril 2014, Digital Rights Ireland Ltd., C-293/12.

108 CJUE, 13 mai 2014, Google Spain SL et Google Inc. contre Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, n° C-131/12.

109 M.CLEMENT FONTAINE, « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *LEGICOM* 2017/2 (N° 59), p. 61-68, spéc.p. 65.

Dans l'ordre juridique international, les premières réglementations ont été élaborées simultanément aux premières législations nationales à partir des années 1970 [110] . Ces réglementations sont de nature très variable. Certaines n'ont pas de force contraignante sous réserve de leur prise en compte par le juge dans l'interprétation des règles juridiques, alors que d'autres sont inscrites dans des traités et s'imposent aux États et même parfois dans les rapports entre particuliers. Certaines ont vocation universelle, alors que d'autres ont une vocation régionale. La question de l'utilisation des données personnelles a donné lieu à l'adoption de textes non contraignants à vocation universelle. Ces textes ont été adoptés dans le cadre des Nations-Unies[111], de l'OCDE[112], de l'Organisation mondiale du Commerce et de l'Organisation Internationale du Travail. Des principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel ont été adoptés en 1990 par l'Assemblée générale des Nations Unies[113]. Ces principes directeurs viennent compléter les textes à portée générale que constituent la Déclaration universelle des droits de l'homme et les pactes internationaux relatifs, d'une part, aux droits civils et politiques et, d'autre part, aux droits économiques et sociaux. Des textes spécifiques sont également intervenus : l'accord établissant l'Organisation mondiale du commerce en 1994 prévoit dans son article XIV des règles relatives à la protection des données personnelles. De même, le Bureau international du travail a adopté un recueil de directives pratiques relatives à la protection des données personnelles des travailleurs. Depuis 2013, les Nations unies ont adopté deux résolutions sur le droit à la vie privée à l'ère numérique [114] en réponse au développement de nouvelles technologies et aux révélations sur la surveillance de masse entreprises dans certains États (les révélations d'Edward Snowden). Ils condamnent fermement la surveillance de masse et soulignent l'impact que cette surveillance peut avoir sur les droits fondamentaux à la vie privée

---

110 En France si la déclaration des droits de l'homme de 1789 reconnaît un droit à la sûreté, celui- ci s'entend essentiellement comme une protection de l'individu contre les abus du pouvoir. Il faut attendre 1970 pour que soit inséré dans l'article 9 du Code civil le principe que « chacun a droit au respect de sa vie privée ». Les années 1970 sont marquées en France par une prise de conscience collective liée aux conséquences potentiellement néfastes du développement de l'informatique, en particulier dans les administrations.

111 Le droit à la protection de la sphère privée d'un individu contre toute intrusion de tiers, en particulier de l'État, a été énoncé pour la première fois dans un acte juridique international à l'article 12 de la Déclaration universelle des droits de l'homme de 1948 de l'Organisation des Nations unies sur le respect de la vie privée et familiale : « Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou telles atteintes ».

112 Des lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel ont été élaboré en 1980. Les lignes directrices, qui revêtent la forme d'une recommandation du conseil de l'OCDE, ont été élaborées par un groupe d'experts gouvernementaux placé sous la présidence de M. M.D. Kirby, Président de la Commission australienne de la réforme législative. Cette recommandation a été adoptée et a pris effet le 23 septembre 1980. Les lignes directrices sont accompagnées d'un exposé des motifs destiné à fournir des éléments d'information sur les débats et les raisonnements qui sous-tendent leur énoncé. Le Conseil de l'OCDE a amendé ses lignes directrices en matière de vie privée le 11 juillet 2013 après discussion des propositions de modification suggérées par un groupe international d'experts, présidé par la Commissaire à la vie privée du Canada et auquel ont participé les autorités nationales de protection des données personnelles, dont la CNIL. Cette révision a notamment permis de renforcer la responsabilisation des entreprises mais aussi de préconiser la mise en place d'autorités de protection des données personnelles.

113 Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel adoptés par la résolution n° 45/95 du 14 décembre 1990 par l'Assemblée générale des Nations unies.

114 Voy. UN, General Assembly, *Resolution on the right to privacy in the digital age*, A/RES/68/167, New York, 18 December 2013 ; and UN, General Assembly, « Revised draft resolution on the right to privacy in the digital age », A/C.3/69/L.26/Rev.1, New York, 19 November 2014.

et à la liberté d'expression, et sur le fonctionnement d'une société dynamique et démocratique. Bien que ces textes internationaux ne soient pas juridiquement contraignants, ils ont déclenché un important débat politique international de haut niveau sur la vie privée, les nouvelles technologies et la surveillance. Ils ont également conduit à la création d'un rapporteur spécial sur le droit à la vie privée, chargé de promouvoir et de protéger ce droit. Les tâches spécifiques du rapporteur comprennent la collecte d'informations sur les pratiques et expériences nationales en matière de vie privée et les défis découlant des nouvelles technologies, l'échange et la promotion des meilleures pratiques, et l'identification des obstacles potentiels. Alors que les résolutions antérieures portaient sur les effets négatifs de la surveillance de masse et la responsabilité des États de restreindre les pouvoirs des services de renseignement, des résolutions plus récentes reflètent une évolution majeure du débat sur la vie privée aux Nations Unies[115]. Ainsi, au-delà de la responsabilité des autorités étatiques, les résolutions plus récentes, soulignent la responsabilité du secteur privé dans le respect des droits humains et appellent les entreprises à informer les utilisateurs sur la collecte, l'utilisation, le partage et la conservation des données personnelles et à établir des politiques de traitement transparentes. Cette réglementation juridique complexe, qui revêt une forte dimension internationale, a permis l'élaboration d'un cadre juridique au niveau régional et au sein de l'Union européenne.

14 La dimension régionale de la réglementation en matière de données personnelles. À l'échelle régionale, en particulier en Europe, plusieurs textes se sont succédés à partir de l'art. 8 de la Convention européenne des droits de l'homme qui a joué un rôle pionnier[116]. À partir de l'article 8 de la Convention, les textes se sont inspirés les uns des autres : la Convention n°108 sur la protection des personnes à l'égard du traitement automatisé des données personnelles du 28 janvier 1981[117], élaborée dans le cadre du Conseil d'Europe, a inspiré la plupart des législation nationales et même la directive 95/46/CE qui a été la norme de base au niveau européen [118] . C'est donc seulement une dizaine d'années plus tard qu'un texte contraignant relatif aux données personnelles a été adopté au sein de l'Union européenne[119]. En effet la libre circulation des marchandises, des capitaux, des services et des personnes au sein du marché intérieur imposait la libre circulation des données, impossible à réaliser si les États

115 Voy. UN, General Assembly, « Revised draft resolution on the right to privacy in the digital age », A/C.3/71/L.39/ Rev.1, New York, 16 November 2016; UN, Human Rights Council, « The right to privacy in the digital age », A/HRC/34/L.7/Rev.1, 22 March 2017.

116 F. SUDRE, *La "construction" par le juge européen du droit au respect de la vie privée,* in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 32.

117 Ouverte à la signature et à la ratification par les États membres du Conseil de l'Europe mais aussi par les États tiers, cette Convention, qui ne comprend pas dans son titre l'adjectif européen, se veut universelle. Cependant, elle reste encore essentiellement régionale. Si elle est dépourvue en principe d'effet direct dans les droits nationaux et ne peut être invoquée par les particuliers devant la Cour européenne, les juges français lui ont reconnu un effet direct et la Cour européenne l'a prise en compte dans l'interprétation des dispositions de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Cette convention a été complétée d'un protocole additionnel sur les autorités de protection des données personnelles et les flux transfrontières de données personnelles, entré en vigueur en 2001.

118 La directive a été adoptée en 1995, date à laquelle plusieurs États membres avaient déjà adopté des lois nationales sur la protection des données.

119 Directive 95/46 CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

membres ne pouvaient se fier à un niveau uniformément élevé de protection des données. Entre temps le droit à la protection des données personnelles a été consacré par la Charte des droits fondamentaux de l'Union européenne[120]. Ainsi, des réglementations nationales avaient déjà été élaborées par les États dès le début des années 1970 en Europe et en Amérique du nord. En 1974, le Land de Hesse adopta la première législation spécifique qui posa les bases de la législation allemande adopté en janvier 1977, la Suède élabora aussi une législation spécifique. S'ensuivit le *Privacy Act* aux États-Unis, n'ayant cependant qu'un champ d'application limité aux seuls fichiers détenus par les administrations fédérales. En France, le danger fut perçu en 1974 lors de la publication de l'article « Safari ou la chasse aux Français » dans le journal *Le Monde*, dont l'objet était de permettre le rapprochement de l'ensemble des fichiers administratifs grâce au numéro national d'identification. Le débat public a abouti à la mise en place d'une Commission informatique et libertés et, sur la base de ses propositions, une loi « informatique et libertés » fut rédigée[121]. Cette prise de conscience s'est inscrite dans le contexte d'une évolution technologique fondamentale : c'est-à-dire le passage du fichier papier au fichier informatisé[122]. Si dans les années 1970, les enjeux de la protection des données visaient à encadrer les ambitions de l'administration et des services de police, désormais c'est la valeur commerciale des données personnelles qui aiguise l'appétit de nombreux opérateurs économiques. Ainsi tous les États membres de l'UE ont ratifié la convention 108. En 1999, des amendements à la convention 108 ont été proposés pour permettre à l'UE de devenir partie mais n'est jamais entrée en vigueur[123]. En 2001, un protocole additionnel à la convention 108 a été adopté. Il a introduit des dispositions sur les flux transfrontières de données vers les non-parties, les pays dits tiers, et sur la création obligatoire d'autorités nationales de contrôle de la protection des données[124]. Face à l'accentuation des risques liés à la multiplication de

---

120 Art. 8, JOCE C364 du 18 décembre 2000. Bien que signée en 2000, la Charte n'a acquis valeur contraignante qu'avec l'entrée en vigueur du traité de Lisbonne modifiant le traité sur l'Union européenne et le traité instituant la Communauté européenne, signé à Lisbonne le 13 décembre 2007 et entré en vigueur le 1er décembre 2009, JOUE C306 du 17 décembre 2007.

121 Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, JO du 7 janvier 1978.

122 L'article de Philippe Boucher paru le 21 mars 1974 dans le monde « Safari ou la chasse aux Français », alertait l'opinion publique sur ces évolutions techniques et sur un projet qui, à partir du numéro de sécurité sociale et par une seule interrogation du fichier informatique, devait permettre à l'administration française de disposer de l'accès à l'ensemble des informations enregistrées sur une seule et même personne (sécurité sociale, fiscalité, police). Le projet de loi fut abandonné par le gouvernement français pour être remplacé par une législation protectrice, la loi « informatique et libertés », qui, pour veiller à son application, créa en France la première autorité administrative indépendante, la commission nationale de l'informatique et des libertés (CNIL).

123 Council of Europe, « Amendments to the Convention for the protection of individuals with regard to automatic processing of Personal Data » (ETS No. 108) adopted by the Committee of Ministers, in Strasbourg, on 15 June 1999.

124 Council of Europe, « Additional Protocol to the Convention for the protection of individuals with regard to automatic processing of personal data, regarding supervisory authorities and transborder data flows », CETS No. 181, 2001. With the modernisation of Convention 108, this Protocol is no longer applied as its provisions have been updated and integrated into the Modernised Convention 108. La convention 108 est ouverte à l'adhésion des parties non contractantes du Conseil de l'Europe. Le potentiel de la Convention en tant que norme universelle, ainsi que son caractère ouvert, servent de base à la promotion de la protection des données au niveau mondial. À ce jour, 51 pays font parties à la Convention 108. Ils comprennent tous les États membres du Conseil de l'Europe (47 pays); l'Uruguay, premier pays non européen à avoir adhéré en août 2013; et Maurice, le Sénégal et la Tunisie, qui ont adhéré en 2016 et 2017. La Convention a récemment subi un processus de modernisation. Une consultation publique menée en 2011 a confirmé les deux principaux objectifs de ce travail: renforcer la protection de la vie privée dans le domaine numérique et renforcer le mécanisme de suivi de la convention. Le processus de modernisation s'est concentré sur ces objectifs et s'est achevé avec l'adoption d'un protocole modifiant la Convention 108 (Protocole STCE n ° 223). Les travaux ont été menés parallèlement à d'autres réformes des instruments internationaux de protection des données et parallèlement à la réforme des règles de protection des données de l'UE, lancée en 2012.

l'utilisation des données personnelles, le droit à la protection des données personnelles a progressivement été dégagé de cette réglementation juridique internationale et régionale pour devenir un droit fondamental à part entière au sein de l'Union européenne inscrit désormais dans le droit primaire au titre de l'article 8 de la Charte des droits fondamentaux et de l'article 16 du TFUE.

II - LA CONSTITUTIONNALISATION DU DROIT FONDAMENTAL À LA PROTECTION DES DONNÉES PERSONNELLES

15 Un droit fondamental. Le droit à la protection des données personnelles relève désormais de la nébuleuse des droits fondamentaux. La notion de droits fondamentaux demeure complexe à appréhender puisqu'elle peut se définir selon l'approche formelle ou substantielle. Sur le plan formel, les droits fondamentaux sont ceux qui sont inscrits dans un texte constitutionnel ou un texte international dont l'objet est de dresser la liste des droits fondamentaux. Selon cette approche, les droits fondamentaux sont les droits et libertés qui s'imposent aux pouvoirs législatif, exécutif et juridictionnel parce qu'ils sont protégés dans les normes supra législatives, notamment constitutionnelles mais aussi conventionnelles. C'est la source supra législative d'un droit ou d'une liberté qui lui confère son caractère fondamental. Cette approche est souvent complétée par des garanties procédurales de protection devant un organe juridictionnel de contrôle habilité à garantir leur respect[125]. Selon d'autres, la *fondamentalité* n'est pas liée à la norme qui la supporte, mais à l'importance reconnue à ce droit par la société et, juridiquement, par l'autorité qui l'édicte »[126]. Au contraire, selon l'approche substantielle (ou matérielle), un droit est fondamental en fonction de son essence, c'est-à-dire en considérant que la fondamentalité résulte de l'importance substantielle qui est reconnue à ce droit conformément à une vision naturaliste du droit. Ainsi les droits fondamentaux sont « des droits assez essentiels pour fonder et déterminer, plus ou moins directement, les grandes structures de l'ordre juridique tout entier en ses catégories, dans lequel et par lesquels ils cherchent à se donner ainsi les moyens multiples de leurs garanties et de leur réalisation »[127]. Les droits fondamentaux seraient ainsi ceux qui bénéficient d'une protection de la norme suprême mais également ceux qui se rapportent à l'humain. Les droits fondamentaux seraient en réalité pour d'autres une « positivisation » des droits de l'homme qui seraient d'essence plus philosophique que juridique[128]. Ces deux approches, formelle et substantielle, s'avèrent complémentaires. Ainsi les droits fondamentaux au sens matériel sont souvent consacrés dans les normes de valeur

---

125 L. FAVOREU (dir.), *Droit des libertés fondamentales*, 6 éd., Dalloz, coll. Précis, 2012, 720 p. 61.

126 B. MATHIEU, M. VERPEAUX, *Contentieux constitutionnel des droits fondamentaux*, LGDJ, coll. Manuel, 2002, p. 808 spéc.p. 10-11.

127 E. PICARD, « L'émergence des droits fondamentaux en France, in Les droits fondamentaux – une nouvelle catégorie juridique ? » *A.J.D.A.*, 1998, n° spécial, p. 8.

128 J. MOULY, *Les droits sociaux à l'épreuve des droits de l'homme,* Dr. Soc., 2002, p. 799.

supra législative. Pour autant, toutes les normes de valeur supra législative ne correspondent pas à un intérêt primordial pour leur bénéficiaire. C'est pourquoi, les droits fondamentaux seront envisagés comme une combinaison des deux approches, comme des droits et libertés liés à la personne en tant que telle et consacrés au sommet de la hiérarchie des normes de valeur supra législative [129] . Les droits fondamentaux seraient donc ceux qui bénéficient d'une protection de la norme suprême mais également ceux qui se rapportent à l'humain. D'ailleurs les droits fondamentaux ont une nature de droits subjectifs. Les droits subjectifs traduisent un rapport juridique reconnu et garanti par le droit objectif entre deux sujets de droit[130]. Il s'agit « des prérogatives individuelles reconnues et sanctionnées par le droit objectif qui permettent à leur titulaire de faire, d'exiger, ou d'interdire quelque chose dans leur propre intérêt ou, parfois, dans l'intérêt d'autrui »[131] . Cependant, la protection des droits fondamentaux par l'Union européenne n'est pas inhérente à la construction de son ordre juridique. En effet, l'article 6 du Traité sur l'Union européenne définissait clairement le cadre dans lequel devait opérer le juge communautaire et les droits fondamentaux trouvaient leur origine tant dans la Convention européenne des droits de l'homme que dans les traditions constitutionnelles communes aux États membres. D'ailleurs la réception de ces droits dans l'ordre juridique communautaire s'effectuait par le canal des principes généraux du droit. Les pères fondateurs de la Communauté européenne privilégièrent une intégration par secteurs dans le domaine économique estimant que la solidarité de fait engendrerait la construction d'une Europe politique. Comme déclaré par Schuman, « l'Europe ne se fera pas d'un coup, ni dans une construction d'ensemble : elle se fera par des réalisations concrètes créant d'abord des solidarités de fait. »[132] C'est la volonté de rendre le projet d'un « marché unique »[133] viable qui a permis la reconnaissance et la protection de certains droits fondamentaux. Ainsi, les notions de droits et libertés fondamentales[134] ne se concrétisait qu'à travers la volonté d'instituer

---

129 E. DREYER, « Du caractère fondamental de certains droits », *RRJ*, 2006, n° 2, p. 551 et s., §§ 9-23.

130 B. TEYSSIÉ, *Droit des personnes*, *LexisNexis* 2014, n° 68, p.668.

131 G. CORNU (dir.), *Vocabulaire juridique*, 10ème éd., PUF, coll. Quadrige, 2014, 1099 p., sp. p. 37.

132 Voy. la Déclaration de Robert Schuman, du 9 mai 1950, site Internet de l'Union européenne.

133 Entre la France, l'Allemagne, la Belgique, les Pays-Bas, l'Italie et le Luxembourg. Voir l'art. 2 du Traité de Rome qui affirmait que « la Communauté a pour mission, par l'établissement d'un marché commun et par le rapprochement progressif des politiques des États membres, de promouvoir un développement harmonieux des activités économiques dans l'ensemble de la Communauté, une expansion continue et équilibrée, une stabilité accrue, un relèvement accéléré du niveau de vie et des relations plus étroites entre les États qu'elle réunit ».

134 Voir B. MATHIEU et M. VERPEAUX précité p.17. Ils estiment que les notions de droits fondamentaux, et libertés fondamentales ne sont pas synonymes : « il existe des libertés qui ne sont pas des droits, par exemple la faculté de se suicider, ou celle de recourir à un avortement, des libertés qui sont des droits ce qui est le cas le plus général pour les libertés fondamentales, comme la liberté d'aller et venir, ou le droit de grève, et des droits qui ne sont pas des libertés, comme le droit à la santé ».

durablement la liberté de circulation des personnes[135], des marchandises[136], des services[137] et des capitaux[138]. L'approche consistant à ne pas développer une politique de protection des droits fondamentaux trouvait une justification dans l'existence parallèle d'une organisation européenne dotée d'un instrument juridique spécifique : la Convention européenne des droits de l'homme[139]. Le Conseil de l'Europe et les Communautés européennes ont donc été instituées selon des exigences différentes et des fonctionnements différents. Cependant, les ordres juridiques qui en découlent se veulent complémentaires mais il convient de remarquer que ces derniers ont été constitués comme étant indépendants ce qui explique en retour l'absence initiale relative des droits fondamentaux dans le droit communautaire. Au contraire du Conseil de l'Europe, la CEE, instituée avec le Traité de Rome du 1957, n'avait pas pour vocation de protéger les droits fondamentaux. C'est avec l'affaire *Stauder* en 1969[140] que la Cour de justice a affirmé le principe selon lequel les droits fondamentaux font partie du droit communautaire en tant que principes généraux dont elle assure le respect[141]. La portée de cette jurisprudence a été précisée dans l'affaire internationale *Handelgesellshaft* de 1970 où la Cour a précisé que pour dégager ces principes protecteurs des droits fondamentaux elle recourait à deux sources d'inspiration : d'une part, les traditions constitutionnelles communes aux États membre[142], et d'autre part, les accords internationaux de protection des droits de l'homme[143]. Parmi tous les traités internationaux dont la Cour a déclaré s'inspirer, le plus important est la Convention européenne des droits de l'homme qu'elle cite pour la première fois en 1975[144], et en de

---

135 Voy. Article 39 T.C.E.

136 Voy. Articles 23 et 24 T.C.E.

137 Voy. Article 49 T.C.E.

138 Voy. Article 56 T.C.E.

139 Pour une étude complète Voy. P.H- IMBERT, *Convention européenne des droits de l'homme de 1950 et ses protocoles*, *Jurisclasseur Libertés*, Fascicule 80.

140 Arrêt de la Cour du 12 novembre 1969. - Erich Stauder contre Ville d'Ulm - Sozialamt. - Demande de décision préjudicielle: Verwaltungsgericht Stuttgart - Allemagne. - Affaire 29-69.
Il s'agit de règles non écrites appliquées par le juge. Les principes généraux ont une valeur supérieure aux normes du droit dérivé et aussi aux accords internationaux conclus par l'Union. Leur respect s'impose non seulement aux institutions et organes de l'Union mais aussi aux États membres lorsqu'ils procèdent à l'exécution du droit de l'Union. Les traités originaux des Communautés européennes ne contenaient pas de référence aux droits de l'homme ou à leur protection. À mesure que la Cour de justice des Communautés européennes de l'époque était saisie d'affaires invoquant des violations des droits de l'homme dans des domaines relevant de la compétence du droit de l'UE, celle-ci a développé une nouvelle approche. Pour offrir une protection aux individus, elle a intégré les droits fondamentaux dans les principes généraux du droit européen. Selon la CJUE, ces principes généraux reflètent le contenu de la protection des droits de l'homme prévue par les constitutions nationales et les traités sur les droits de l'homme en particulière la CEDH. La CJUE a déclaré qu'elle garantirait la conformité du droit de l'UE à ces principes. En reconnaissant que ses politiques pouvaient avoir un impact sur les droits de l'homme et dans le souci de veiller à ce que les citoyens se sentent protégés de l'UE, en 2000 a été proclamé la Charte des droits fondamentaux de l'Union européenne. La Charte avait une portée politique mais avec l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, elle a acquis force obligatoire.

142 CJCE 17 dec. 1970, aff. 11/70.

143 CJCE aff. Nold, 14 mai 1974, aff. 4/73, dans cet arrêt la Cour a en effet affirmé qu' «Il faut tenir compte des éléments des traités internationaux relatifs à la protection des droits de l'homme dont les États membres ont été signataires dans l'application du droit de l'Union ».

144 CJCE, Rutili c. Ministre de l'Intérieur, aff. C- 36/75, 1975.

nombreux cas suivants. Il est possible de remarquer que les droits fondamentaux ont été à l'origine d'un dialogue stratégique de la Cour de justice et de la Cour européenne des droits de l'homme. Il s'agit « des interactions judiciaires et normatives, spontanées et imposées, directes et indirectes entre systèmes juridiques »[145]. Ces interactions conduisent par conséquent à un pluralisme juridique et donc à l'imbrication directe et indirecte des ordres juridiques[146]. Si l'Union européenne constitue un ordre juridique spécifique, elle s'inscrit néanmoins dans un schéma complexe. Ainsi elle établit une protection des droits fondamentaux en parallèle à la Convention européenne des droits de l'homme et à celle des États. Le domaine des droits fondamentaux constitue l'élément central de l'insertion réciproque entre systèmes. De plus, l'apport du Traité de Lisbonne impliquant l'adhésion de l'Union européenne à la Convention européenne des droits de l'homme souligne une perméabilité des ordres juridiques qui se traduit par l'utilisation des normes européennes par les juges européens. D'ailleurs les articles 52§2[147] et 53[148] de la Charte établissent clairement un lien entre l'Union européenne et la Convention européenne des droits de l'homme en permettant la communicabilité des normes. Cette influence des ordres juridiques a été possible dans un premier temps grâce aux principes généraux du droit comme source d'inspiration pour la Cour de justice et dans un second temps avec la Charte des droits fondamentaux, en témoignent le processus de circularité des droits au sein de l'Europe. Cette circularité des droits fondamentaux a d'ailleurs une base juridique dans l'article 52§3 de la Charte qui prévoit une interprétation et une portée correspondantes à celles de la Convention européenne (A). Malgré l'absence d'une politique originelle de protection des droits fondamentaux dans les traités originaires de l'Union européenne, le juge communautaire a su introduire la notion de droits fondamentaux dont le droit à la protection des données fait partie (B).

A. Une protection étroitement liée au droit de la Convention

16 De la valeur politique à la valeur juridique de la Charte des droits fondamentaux. D'après les explications relatives à la Charte, les fondements juridiques de l'article 8 sont doubles : d'une part il repose sur l'acquis du Conseil de l'Europe[149], de l'autre sur l'acquis communautaire [150] . L'apport des principes généraux de droit et en particulier de la ConventionEDH est tel qu'ils se voient aujourd'hui inscrits dans le droit primaire de l'Union

---

145 M. DELMAS-MARTY, *Le pluralisme ordonné et les interactions entre ensembles juridiques*, Dalloz, 2006, p. 951-957

146 Ibid. p. 952.

147 « Les droits reconnus par la présente Charte qui trouvent leur fondement dans les Traités communautaires ou dans le Traité sur l'Union européenne s'exercent dans les conditions et limites définies par ceux-ci».

148 « Aucune disposition de la présente Charte ne doit être interprétée comme limitant ou portant atteinte aux droits de l'homme et libertés fondamentales reconnus, dans leur champ d'application respectif, par le droit de l'Union, le droit international et les conventions internationales auxquelles sont parties l'Union, la Communauté ou tous les États membres, et notamment la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi que par les constitutions des États membres. ».

149 Convention n°108 du Conseil de l'Europe.

150 Document CHARTE 4473/1/00 du 19 octobre 2000.

européenne. Jusqu'à la reconnaissance de la valeur contraignante de la Charte des droits fondamentaux, les principes généraux ont été l'unique source de la protection des droits fondamentaux. La consécration des droits fondamentaux repose en effet sur la précédente constitutionnalisation des principes généraux du droit dans le droit primaire [151] . D'ailleurs, l'absence initiale de valeur juridique contraignante attachée à la Charte des droits fondamentaux, du fait de l'impossible entrée en vigueur du Traité établissant une Constitution pour l'Europe, n'a pas empêché les juges de l'Union européenne[152] et les avocats généraux de l'utiliser en tant que source du droit. L'affaire décisive concernant l'utilisation de la Charte des droits fondamentaux par la Cour de justice s'est effectuée dans l'arrêt *Parlement c. Conseil* du 27 juin 2006. La Cour a estimé que « cette Charte ne constitue pas un instrument juridique contraignant », elle note néanmoins que « le législateur communautaire a cependant entendu en reconnaître l'importance en affirmant, au deuxième considérant de la directive 2003/86 CE, que cette dernière respecte les principes qui sont reconnus non seulement par l'article 8 de la Convention européenne des droits de l'homme, mais également par la Charte »[153]. De plus, l'Avocat général A. TIZZANO opère une première référence significative à la Charte en énonçant que « dans un litige portant sur la nature et la portée d'un droit fondamental, il est impossible d'ignorer les énonciations pertinentes de la Charte ni surtout son évidente vocation à servir, lorsque ses dispositions le permettent, de paramètre de référence substantiel pour tous les acteurs – États membres, institutions, personnes physiques et morales – de la scène communautaire » [154] . De même, l'Avocat général Ph. LÉGER affirme que la « Charte a indéniablement placé les droits qui en font l'objet au plus haut niveau des valeurs communes aux États membres. (...) Comme le laisse supposer la solennité de sa forme et de la procédure qui a conduit à son adoption, la Charte devrait constituer un instrument privilégié servant à l'identification des droits fondamentaux »[155]. Il est possible d'affirmer que la « force politique » de la Charte des droits fondamentaux est devenue une « force juridique » depuis l'entrée en vigueur du Traité de Lisbonne [156] Le respect des droits fondamentaux est devenu tel dans l'Union européenne que « ce ne sont plus les droits de l'homme qui doivent être examinés au

---

151 L'article F, paragraphe 2, du Traité de Maastricht précise en effet que « (l') Union respecte les droits fondamentaux, tels qu'ils sont garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950, et tels qu'ils résultent des traditions constitutionnelles communes aux États membres, en tant que principes généraux du droit communautaire ». Selon F. Picod, cette disposition constitue un « hommage à la Cour de justice » en ce qu'elle a « expressément consacré la jurisprudence de la Cour de justice relative aux droits fondamentaux, sans pour autant ériger ces derniers au rang de principes ayant une valeur équivalente à celle du droit originaire, ou, pour renforcer l'analogie avec une constitution, de principes constitutionnels » Voir PICOD (F.), « Droit de l'Union européenne des droits de l'homme et des libertés fondamentales », *Jurisclasseur libertés*, fascicule 120, pt. 180.

152 L. BURGORGUE-LARSEN, « La force de l'évocation ou le fabuleux destin de la Charte des droits fondamentaux de l'Union européenne », in *Mélanges en l'honneur de Pierre Pactet*, Paris, Dalloz, 2003, p. 77 ; J. P. JACQUÉ, *La protection juridictionnelle des droits fondamentaux dans l'Union européenne* , *A.J.D.A.*, 2002, p. 476.

153 CJCE, 27 juin 2006, aff. C-540/03, Parlement c/ Conseil.

154 A. TIZZANO, conclusions sous CJCE, 26 juin 2001, aff. C-173/99, « BECTU », pt. 28.

155 Voy. Ph. LÉGER, conclusions sous CJCE, 6 décembre. 2001, aff. C-359/99 P, « Hautala », Rec., I, p. 9565.

156 P. MAGNETTE, « Prendre la Charte au sérieux. La force politique d'un texte juridique non contraignant », in J-Y. CARLIER et O. DE SCHUTTER, (sous la dir.), La Charte des droits fondamentaux de l'Union européenne. Son apport à la protection des droits de l'homme en Europe : hommage à Silvio Marcus-Helmons, spéc. p. 97-104.

travers du prisme communautaire mais l'action communautaire au travers du prisme des droits de l'homme »[157]. Le mécanisme d'interprétation conforme des dispositions de la Charte au droit de la Convention EDH est assuré par l'article 52§ 3 de la Charte. Toutefois, l'article 8 de la Charte n'est pas identifié comme un droit « correspondant » à la ConventionEDH par les explications de la Charte. Afin d'assurer la cohérence de la protection, la Cour de justice dans l'affaire *Osterreichisher Rundfunk* a souligné le lien étroit avec le droit à la vie privée reconnu à l'article 7 de la Charte qui doit être interprété conformément au droit de la Convention. La Charte des droits fondamentaux représente l'aboutissement textuel et jurisprudentiel de la prise en compte de la protection des droits de l'homme dans l'Union européenne. À cet égard, l'inscription des droits fondamentaux dans le droit primaire de l'Union européenne a été définie comme une « modification du patrimoine génétique communautaire » [158] . Cette évolution constitutionnelle du droit de l'Union européenne synthétise et consacre l'œuvre prétorienne de la Cour de justice. En effet la Charte s'inspire de la Convention européenne des droits de l'homme, de la Charte sociale européenne et d'autres conventions relatives aux droits de l'homme, sur les traditions constitutionnelles communes aux États membres, ainsi que sur la jurisprudence de la CourEDH[159]. Ce texte contribue à renforcer la construction constitutionnelle de l'Union européenne. Ainsi grâce à la Charte, l'Union européenne s'est vue attribuer des obligations et compétences liées au respect et à la protection des droits fondamentaux. Cela a étendu le champ normatif de l'Union européenne à un domaine de compétences traditionnellement régi par les normes constitutionnelles des États membres. Ainsi la consécration de la Charte des droits fondamentaux en tant que source de droit primaire est venue moduler la portée des principes généraux du droit en tant que source formelle des droits fondamentaux. Elle a constitué depuis son entrée en vigueur la principale source formelle des droits fondamentaux. La proclamation des principes généraux dans les textes de droit primaire de l'Union européenne pose aujourd'hui la question de leur avenir vis-à-vis de leur « obsolescence »[160] sur le plan formel. En effet, par l'entrée en vigueur du Traité de Lisbonne, l'ensemble des compétences de l'Union européenne est assujetti au respect de la Charte et donc au respect des droits fondamentaux. La Charte des droits fondamentaux de l'Union européenne constituerait une « modernisation »[161] de la Convention européenne des droits de l'homme

---

157 F. SUDRE, « Le renforcement de la protection des droits de l'homme au sein de l'Union européenne », in J. RIDEAU, (sous la dir.), *De la Communauté de droit à l'Union de droit*, L.G.D.J, 2000, pp. 217 et 218.

158 R. TINIÈRE, L'office du juge communautaire des droits fondamentaux, précité, p. 407.

159 D'ailleurs, le 5e alinéa du Préambule de la Charte rappelle l'importance des principes généraux de droit et stipule que « la présente Charte réaffirme, dans le respect des compétences et des tâches de la Communauté et de l'Union, ainsi que du principe de subsidiarité, les droits qui résultent notamment des traditions constitutionnelles et des obligations internationales communes aux États membres, du Traité sur l'Union européenne et des Traités communautaires, de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, des Chartes sociales adoptées par la Communauté et par le Conseil de l'Europe, ainsi que de la jurisprudence de la Cour de justice des Communautés européennes et de la Cour européenne des droits de l'homme ».

160 F. SUDRE, « Le renforcement de la protection des droits de l'homme au sein de l'Union européenne », J. in RIDEAU préec.

161 J. DUTHEIL DE LA ROCHÈRE, « Charte des Droits Fondamentaux, quel apport à la protection des droits ? », in *Mélanges en l'honneur de Benoit Jeanneau, Les mutations contemporaines du droit public*, Paris, Dalloz, 2002, p. 97.

puisqu'elle formule de nouveaux droits[162] même si celle-ci demeure un « instrument vivant à interpréter »[163]. Le droit à la protection des données personnelles est un droit qui illustre la modernité de la Charte des droits fondamentaux par rapport à d'autres instruments internationaux[164] de protection des droits de l'homme ne consacrant pas explicitement ce droit. Ainsi la Charte constitue désormais le texte central de la protection des droits fondamentaux par la Cour de justice [165] malgré une référence à la Convention européenne des droits de l'homme [166] . La formalisation d'une Charte de droits essentiellement inspirés du droit conventionnel permet également de combler l'incapacité de l'Union européenne à adhérer à la Convention européenne des droits de l'homme[167]. La future adhésion de l'Union européenne à la Convention européenne des droits de l'homme [168] confirme d'ailleurs l'attachement de l'Union européenne aux droits fondamentaux et la volonté d'une protection accrue et parallèle. Désormais, l'Union européenne et les États membres doivent respecter les droits fondamentaux dans l'exécution des tâ ches prévues par les traités. Ces obligations ont été progressivement encadrées par la jurisprudence de Cour de justice qui a comblé les lacunes des traités originaires, assurant ainsi simultanément l'autonomie et la cohérence de l'ordre juridique de l'Union dans ses relations avec les ordres constitutionnels nationaux[169].

17 Le champ d'application de la Charte des droits fondamentaux. Depuis l'entrée en vigueur du Traité de Lisbonne, la Charte des droits fondamentaux a acquis la mê me valeur

---

162 J. DUTHEIL DE LA ROCHÈRE, « La charte des droits fondamentaux de l'Union européenne », *JurisClasseur Libertés*, Fascicule 140, pts. 49 et s.

163 Selon la jurisprudence constante de la Cour, la Convention européenne des droits de l'homme est « un instrument vivant à interpréter à la lumière des conditions de vie actuelles » (C.E.D.H., 25 avril 1978, « Tyrer c/ Royaume-Uni », série A no 26, § 31).

164 Le droit à la protection des données personnelles n'apparaît ni dans la Déclaration universelle des droits de l'homme de 1948, ni dans la Convention européenne des droits de l'homme de 1950, ni dans les Pactes internationaux des Nations-Unies relatifs aux droits civils et politiques et aux droits économiques, sociaux et culturels de 1966

165 Signée et proclamée par les présidents du Parlement européen, du Conseil et de la Commission lors du Conseil européen de Nice le 7 décembre 2000, la Charte résulte d'un processus original et concrétise le fruit d'une convergence entre la jurisprudence de la Cour de justice et les traités constitutifs de l'Union européenne. Grâce à l'art. 6§2 du Traité sur l'Uni on européenne, la Charte s'adresse aux institutions et organes de l'Union européenne tant dans le champ de son droit que des deuxième et troisième piliers. De même, la Charte s'adresse aux États membres lorsque ces derniers mettent en œuvre le droit l'Union.

166 H. DUMONT et S. VAN DROOGHENBROECK, « La contribution de la Charte à la constitutionnalisation du droit de l'Union européenne », in J.Y. CARLIER et O. DE SCHUTTER, (sous la dir.), *La Charte des droits fondamentaux de l'Union européenne. Son apport à la protection des droits de l'homme en Europe : hommage à Silvio Marcus-Helmons*, Bruxelles, Bruylant, 2002, 304 p, spéc. pp. 61-96.

167 CJCE, 28 mars 1996, Avis 2/94, « Adhésion de la Communauté européenne à la Convention de sauvegarde des droits de l'homme et des libertés fondamentales », Rec., I, p.1759, pt. 23.

168 Résultant de l'obligation instituée par le Traité de Lisbonne. Voir Traité sur l'Union européenne, article 6§2 : « L'Union adhère à la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. ».

169 S. PEERS, T. HERVEY, J.KENNER, A. WARD (eds), *The EU Charter of Fundamental Rights*, Hart Publishing, 2014.

juridique[170]. Même si certaines de ses dispositions développent les instruments déjà existants en matière de droits de l'homme, la Charte n'élargit pas la compétence de l'Union européenne. La Charte est applicable aux institutions selon le respect du principe de subsidiarité et en aucun cas elle ne peut étendre les compétences et les tâches que les traités leur confèrent. Elle est également applicable aux pays de l'Union européenne lorsqu'ils mettent en œuvre la législation de l'UE [171] . Concernant sa mise en œuvre, elle est contraignante pour les institutions communautaires lorsque celles-ci adoptent de nouvelles mesures, et pour les États membres lors de la mise en œuvre de ces nouvelles mesures[172]. Ce critère délimite le champ d'application de la Charte et par conséquent le pouvoir interprétatif de la Cour de justice. Ainsi la Cour de justice a estimé que « les droits fondamentaux garantis dans l'ordre juridique de l'UE s'appliquent dans toutes les situations qui relèvent du droit de l'Union mais non en dehors de celles-ci » [173]. La Charte constitue ainsi le point de référence pour la Cour de justice et pour le législateur de l'Union, lorsque la législation communautaire donne une « expression particulière aux droits fondamentaux », notamment dans les politiques communautaires de lutte contre les discriminations, ou concernant le droit d'asile, la protection des données, la transparence, la bonne administration, et les droits procéduraux dans le cadre des poursuites civiles et pénales[174]. D'après l'article 52 de la Charte, toute limitation des droits fondamentaux doit être prévue par la loi, respecter le contenu essentiel de ces droits ainsi que le principe de proportionnalité. Dans le cas contraire, la législation de l'Union doit être considérée comme nulle. Une fois analysée l'inclusion des droits fondamentaux dans l'ordre juridique de l'Union européenne et les mécanismes de cohérence avec la protection offerte par la CEDH, il est

---

170 K. Ł. BOJARSKI, D. SCHINDLAUER, K. WLADASCH, *The European Charter of Fundamental Rights as a Living Instrument*, Rome-Warsaw-Vienna, 2014; G. PALMISANO (a cura di), *Making the Charter of Fundamental Rights a Living Instrument*, Leiden, 2014; J.A. LAENARTS, F. GUTIÉRRE, « The place of the Charter in the EU constitutional edifice », in S. PEERS, T. HERVEY, J. KENNER, A. WARD, *The EU Charter of fundamental Rights*, Oxford and Portland (OR) 2014, 1559 ss. ; S. DE VRIES, U. BERNITZ, S. WEATHERIL, (eds), *The EU Charter of Fundamental Rights as a Binding Instrument: Five Years Old*, Oxford, 2015; P. MORI, « Autonomia e primato della Carta dei diritti fondamentali dell'Unione europea », in G. NESI, P. GARGIULO (a cura di), L. FERRERI BRAVO, *Il diritto internazionale come professione*, Trento, 2015, p.169 et s.; L.S. ROSSI, « Stesso valore giuridico dei Trattati? Rango, primato ed effetti diretti della Carta dei diritti fondamentali dell'Unione europea », in E. FALLETTI, V. PICCONE (a cura di), *Il filo delle tutele nel dedalo d'Europa*, Napoli, 2016, p. 73 et s.; A. SPADARO, M. CONDINANZI, O. POLLICINO (a cura di), *La Carta dei diritti dell'Unione Europea e le altre Carte (ascendenze culturali e mutue implicazioni)*, Torino, 2016.

171 L'article 51 dispose: «Les dispositions de la présente Charte s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. En conséquence, ils respectent les droits, observent les principes et en promeuvent l'application, conformément à leurs compétences respectives. La présente Charte ne crée aucune compétence ni aucune tâche nouvelles pour la Communauté et pour l'Union et ne modifie pas les compétences et tâches définies par les traités».

172 Voir art. 51 de la Charte: 1. Les dispositions de la présente Charte s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. En conséquence, ils respectent les droits, observent les principes et en promeuvent l'application, conformément à leurs compétences respectives. 2. La présente Charte ne crée aucune compétence ni aucune tâche nouvelles pour la Communauté et pour l'Union et ne modifie pas les compétences et tâches définies par les traités.

173 CJUE, C-617/10, Åklagaren/Hans Åkerberg Fransson, 26 février 2013, §105. Voir sur cet aspet R. Baratta, Il telos dell'interpretazione conforme all'acquis dell'Unione, in Rivista di diritto internazionale, 2015, p. 28 ss., a p. 41 ss.

174 De plus, les droits fondamentaux peuvent également représenter un enjeu dans la législation communautaire concernant d'autres domaines de la compétence de l'Union, comme le transport, la concurrence, les douanes et la surveillance des frontières. Comme ces politiques peuvent avoir des conséquences sur les droits des citoyens et des personnes, par exemple, la dignité humaine, la vie privée, le droit d'être entendu et la liberté de circulation, le droit de l'Union devrait également tenir compte de ces situations.

possible de se pencher sur le régime du droit fondamental à la protection des données personnelles.

B. Le dialogue entre la Cour de justice et la CourEDH

18 L'affranchissement de la Cour de justice. La ConventionEDH a su pénétrer de manière significative dans les actes contraignants de droit secondaire de l'Union qui se réfèrent souvent à la CEDH. Ainsi le respect de la Convention est devenu une condition essentielle à l'application du droit issu de l'Union européenne. Le rappel et l'application de la Convention européenne des droits de l'homme du droit issu de l'Union européenne démontre d'une part, la volonté de pallier les carences de cette dernière en matière de droits fondamentaux et, d'autre part, le dépassement des frontières traditionnelles des ordres juridiques. L'action initiale de la Cour de justice, à travers l'utilisation des principes généraux de droit en faveur des droits fondamentaux, se voit enrichie par la multiplication des références textuelles tant aux droits fondamentaux qu'au droit de la Convention européenne des droits de l'homme. Toutefois, la volonté de la Cour de justice de garantir la protection des droits fondamentaux demeure limitée pour un certain temps puisque la Cour ne dispose pas d'un titre de compétence lui permettant de tirer toutes les conséquences d'une protection globale des droits fondamentaux. Parmi les principes généraux de droit, la Convention européenne des droits de l'homme tend à devenir une source d'inspiration privilégiée pour la Cour de justice. Il est possible de parler de véritables « glissements progressifs »[175] entre l'utilisation des traditions constitutionnelles communes aux États membres et le texte du Conseil de l'Europe[176]. De même, il a été souligné le passage d'une « source d'inspiration » des droits fondamentaux à une « source de la légalité » du droit de l'Union européenne[177]. Il en ressort une dynamique de « convergence pour un droit commun européen des droits de l'homme »[178]. D'ailleurs, on peut constater que les États européens n'ont pas tous consacré dans leur constitution un droit à la protection des données personnelles. Ce sont principalement les constitutions récentes, adoptées à partir des années 1970, qui traduisent ces préoccupations[179]. De ce fait l'Union européenne a dû s'appuyer pour longtemps sur la

175 F. MANCINI et V. DI BUCCI, *Le développement des droits fondamentaux en tant que partie du droit communautaire*, précité, p. 38.

176 Ainsi face à la difficulté de se référer au droit comparé, aux traditions constitutionnelles communes et la transposition délicate de certains principes de droit international, la Cour de justice a introduit la Convention européenne des droits de l'homme afin de l'établir en tant que source à part entière des principes généraux dudroit.

177 G. COHEN JONATHAN, « La Cour des Communautés européennes et les droits de l'homme », *Revue du Marché Commun*, 1978, p. 90 et s.

178 F. SUDRE, « A propos du « dialogue des juges » et du contrôle de conventionalité », in *Etudes en l'Honneur de Jean-Claude GAUTRON*, Paris, Pedone, 2004, p. 208.

179 Par ex. la Constitution espagnole du 27 décembre 1978 (art. 18 § 4) et la Constitution portugaise du 2 avril 1976 (art. 35). Voy sur cet aspect : M.-T. MEULDERS-KLEIN, « L'irrésistible ascension de la vie privée au sein des droits de l'homme », in F. Sudre *(dir.), Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 305 s ; L. BURGORGUE-LARSEN, *L'appréhension constitutionnelle de la vie privée en Europe*, in F. SUDRE (dir.), *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Bruylant, 2005, p. 69 et s.

ConventionEDH. Cette harmonie est soulignée par la Cour de justice, selon laquelle, la Convention européenne doit être utilisée comme une norme de référence dans la mise en œuvre du droit communautaire en matière de droits fondamentaux. Ainsi la Convention est devenue une source de légalité de l'Union européenne. D'ailleurs la Cour de justice se réfère directement à la CEDH et plus encore à la jurisprudence de la CourEDH, ainsi la Convention européenne des droits de l'homme a été « absorbée »[180] comme source de légalité communautaire. Dans une première phase, la Cour de justice n'hésite pas à apprécier directement le droit communautaire au droit conventionnel par l'utilisation d'une référence à la Convention européenne des droits de l'homme. Ainsi dans l'affaire *Osterreichischer Rundfunk*[181], la Cour de justice a opéré directement l'appréciation de l'article 8 de la Convention aux dispositions de la directive 95/46 sans qu'il ne soit fait référence aux principes généraux de droit. Ainsi la Cour de justice a estimé que les dérogations opérées par le droit communautaire à l'exercice du droit à la vie privée, notamment la collecte de données nominatives relatives aux revenus professionnels d'un individu, n'entrainaient pas une violation de l'article 8 de la Convention européenne des droits de l'homme. L'ingérence prévue par la directive en question se voyait ainsi déclarée compatible avec les exigences de la Convention européenne des droits, telle qu'interprétée par la Cour européenne de Strasbourg. Dans l'affaire *Lindqvist* [182] , la ConventionEDH et la jurisprudence de la CourEDH figurent encore comme normes de référence de la Cour de justice. Dans l'arrêt *Commission c. Allemagne*[183] , concernant la question de l'indépendance des autorités nationales de contrôle en matière de protection des données, la Cour de justice souligne que le double objectif de la directive 95/46 (à savoir, la libre circulation des données et la protection des données) est susceptible de porter atteinte au droit à la vie privée tel que reconnu à l'article 8 de la ConventionEDH. Dans les affaires *Volker und Markus Schecke* et *Eifert*, concernant la publication sur Internet de données personnelles de bénéficiaires d'aides de fonds agricoles, la Cour de justice procède à l'interprétation de l'article 8 de la Charte mais à la lumière de l'article 8 de la CEDH et sous l'angle de la jurisprudence correspondante. Toutefois, la situation a changé lorsque l'Union s'est dotée d'une Charte des droits fondamentaux [184] . Ainsi dans l'affaire *Scarlet Extended* [185] , le juge de Luxembourg abandonne toute référence à la CEDH ce qui illustre la « volonté d'autonomisation du droit communautaire par rapport à l'article 8 de la CEDH et à la jurisprudence s'y rapportant »[186]. De récents arrêts en matière de protection des données personnelles sont la parfaite illustration du passage d'une conception fonctionnelle à une conception

---

180 F. SUDRE, *Le renforcement de la protection des droits de l'homme au sein de l'Union européenne*, précité, p. 219.

181 CJCE., 20 mai 2003, aff. jointes C-465/00, C-138/01 et C-139/01, « Osterreichischer Rundfunk et a. », Rec., I, p. 4989, pt. 71.

182 CJCE, *Bodil Lindqvist*, aff. C-110/01, 6 novembre 2003.

183 CJUE, *Commission c. Allemagne*, aff. C-518/07, 9 mars 2010.

185 CJUE, aff. C-70/10, 24 novembre 2011.

186 Commentaire de F. KAUFF-GAZIN, Europe, n°1à, octobre 2010, comm. 299.

constitutionnelle[187] des droits fondamentaux[188]. À partir de l'arrêt *Digital Rights Ireland* le raisonnement de la Cour de justice utilise la Charte des droits fondamentaux comme grille d'analyse pour mener à bien son contrôle. Dans l'arrêt *Google Spain* la progressive autonomisation semble aboutie. Ici, le juge fonde son raisonnement sur la Charte et sur sa jurisprudence et exporte son modèle de protection vers le fournisseur de services Internet Google situés aux États-Unis.

III. L'ÉMERGENCE D'UN MODÈLE EUROPÉEN DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES

A. Le cadre législatif au sein de l'Union européenne

19 Le cadre juridique dans le droit primaire. D'après les explications relatives à la Charte des droits fondamentaux, les fondements juridiques de l'article 8 sont doubles. Cet article repose en effet sur un acquis issu du droit du Conseil de l'Europe et sur le successif acquis communautaire. En effet les traités originaux des Communautés européennes ne contenaient aucune référence aux droits de l'homme ou à leur protection, étant donné que la Communauté économique européenne était initialement envisagée comme une organisation régionale axée sur l'intégration économique et la création d'un marché commun. Un principe fondamental qui sous-tend la création et le développement des Communautés européennes et qui est également valable aujourd'hui est le principe de l'attribution. Selon ce principe, l'Union européenne n'intervient que dans les limites des compétences qui lui sont conférées par les États membres, telles que reflétées dans les traités de l'Union. Contrairement au Conseil de l'Europe, les traités de l'UE n'incluent aucune compétence explicite en matière de droits fondamentaux. Pour accorder la protection aux individus, la Cour de justice a introduit les droits fondamentaux dans les soi-disant principes généraux du droit européen. Selon la Cour de justice, ces principes généraux reflètent le contenu de la protection des droits de l'homme figurant dans les constitutions nationales et les traités relatifs aux droits de l'homme, en particulier la CEDH. La Cour de justice a déclaré qu'elle assurerait la conformité de la législation de l'Union avec ces principes. Reconnaissant que ses politiques ont un impact sur les droits de l'homme et s'efforçant de se rapprocher des citoyens de l'Union, l'Union a proclamé en 2000 la Charte des droits fondamentaux de l'Union européenne (ci-après « la Charte »). Les droits décrits dans la Charte sont divisés en six sections : dignité, libertés, égalité, solidarité, droits des citoyens et justice. À l'origine, il ne s'agissait que d'un document politique, la Charte devenant

[187] H. HIJMANS, The European Union as a constitutional guardian of internet privacy and data protection, PhD Thesis, University of Amsterdam 2016, http://hdl.handle.net/11245/ 2.169421, p. 389.

[188] F. SUDRE et R. TINIERE, *Droit communautaire des droits fondamentaux*, éd Nemesis, Bruxelles, 2012, p. 17.

juridiquement contraignante en tant que droit primaire de l'Union [189] lorsque le traité de Lisbonne est entré en vigueur le 1er décembre 2009. Les dispositions de la Charte lient également les États membres lorsqu'ils mettent en œuvre le droit de l'Union. La Charte garantit non seulement le respect de la vie privée et familiale (article 7), mais établit également le droit à la protection des données personnelles (article 8). La Charte élève explicitement le niveau de cette protection à celui d'un droit fondamental dans le droit de l'Union. Les institutions et organes de l'Union doivent garantir et respecter ce droit, tout comme les États membres lorsqu'ils mettent en œuvre le droit de l'Union (article 51 de la Charte). Formulé plusieurs années après la directive sur la protection des données, l'article 8 de la Charte doit être compris comme une loi préexistante sur la protection des données de l'Union. La Charte, par conséquent, mentionne non seulement explicitement un droit à la protection des données à l'article 8, paragraphe 1, mais renvoie également aux principes clés de protection des données énoncés à l'article 8, paragraphe 2. Enfin, l'article 8 (3) de la Charte exige qu'une autorité indépendante contrôle la mise en œuvre de ces principes. L'adoption du traité de Lisbonne est un jalon dans le développement du droit de la protection des données, non seulement pour faire de la Charte un document juridique contraignant au niveau du droit primaire, mais aussi pour garantir le droit aux données personnelles. Ce droit est spécifiquement prévu à l'article 16 du TFUE, dans la partie du traité consacrée aux principes généraux de l'Union. L'article 16 crée également une nouvelle base juridique, conférant à l'Union la compétence de légiférer en matière de protection des données dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, à la seule exception de la politique étrangère et de sécurité commune relevant de l'article 39 TUE. Cette évolution est importante car avant l'entrée en vigueur du Traité de Lisbonne, les règles européennes de protection des données notamment la directive 95/46 sur la protection des données reposaient initialement sur la base juridique du marché intérieur et sur la nécessité de rapprocher les législations nationales afin que la libre circulation des données au sein de l'Union ne soit pas inhibée[190]. L'article 16 du TFUE fournit désormais une base juridique indépendante pour une approche moderne et globale de la protection des données, qui couvre toutes les questions de la compétence de l'UE, ycompris la coopération policière et judiciaire en matière pénale. L'article 16 du TFUE affirme également que le respect des règles de protection des données adoptées en vertu de celui-ci doit être soumis au contrôle d'autorités de surveillance indépendantes. D'ailleurs la *constitutionnalisation* de la Charte, dérivant de sa proclamation comme droit primaire, est un évènement majeur pour la Cour de justice, qui dispose d'une norme propre de référence, lui permettant de jouer son rôle de gardien « constitutionnel » des droits fondamentaux. D'ailleurs l'article 16 a servi de base juridique à l'adoption de la réforme globale[191] des règles de protection des données en 2016, à savoir le règlement général sur la protection des données et la directive sur la protection des données pour les autorités policières et pénales. Cependant, les États n'ont visiblement pas souhaité se saisir de cette possibilité de s'affranchir des contraintes inhérentes au jeu des bases

189 Voy. article 6, paragraphe 1, du TUE.

190 M.-C. PONTHOREAU, « La directive 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *RFDA*, 1997, p. 125 et s.

191 Voy. le communiqué de presse disponible à l'adresse : http://europa.eu/rapid/press-release_IP-12-46_fr.htm?locale=FR.

juridiques et ont préféré maintenir deux instruments distincts fondés sur l'article 16TFUE. Ce choix permet aux États de mettre en place des standards de protections différencié en valorisant davantage les impératifs de sécurité publique. Ainsi l'interprétation de la Cour de justice vis-à-vis des dispositions de la directive 680/16 qui définissent un standard inférieur à celui offert par le règlement 679/16 sera crucial afin de préciser les règles issues du droit dérivé qui relèvent d'un droit fondamental.

20 Le Cadre juridique dans le droit secondaire. De 1995 à mai 2018, le principal instrument juridique de l'UE sur la protection des données était la directive 95/46 / CE du Parlement européen et du Conseil du 24 octobre 1995 concernant la protection des personnes à l'égard des données personnelles et la libre circulation[192]. La directive 95/46 dite « directive mère » a été adoptée en 1995, à une époque où plusieurs États membres avaient déjà adopté des lois nationales sur la protection des données[193], et est ressortie de la nécessité d'harmoniser ces lois afin d'assurer un niveau élevé de protection des données et la libre circulation des données à caractère personnel entre les différents États membres. En effet, la libre circulation des biens, des capitaux, des services et des personnes au sein du marché intérieur nécessitait la libre circulation des données, qui ne pouvait être réalisée que si les États membres pouvaient compter sur un niveau élevé de protection des données. Cette directive a établi un système de protection des données détaillé et complet dans l'UE. Cependant, conformément au système juridique de l'UE, les directives ne s'appliquent pas directement et doivent être transposées dans les législations nationales des États membres. Inévitablement, les États membres bénéficient d'une marge de manœuvre pour transposer les dispositions de la directive. Même si la directive visait à assurer une harmonisation complète (et un niveau de protection complet), dans la pratique, elle a été transposée différemment dans les États membres. Cela a abouti à la mise en place de diverses règles de protection des données dans l'Union européenne, avec des définitions interprétées différemment dans les législations nationales. Les niveaux d'application et la sévérité des sanctions variaient également d'un État membre à l'autre. Enfin, des changements importants ont été apportés à la technologie de l'information depuis la rédaction de la directive au milieu des années quatre-vingt-dix. Prises ensemble, ces raisons ont conduit à la réforme de la législation européenne en matière de protection des données. Toutefois elle a permis d'une part le développement de la jurisprudence de la Cour de justice en la matière et d'autre part le développement du droit dérivé de l'Union européenne. Cela a conduit à l'adoption du règlement 45/2001/CE étendant l'application des principes de la directive aux institutions et organes de l'Union, la directive 2002/58/CE dite directive vie privée et communications électroniques qui adapte les principes de la directive 95/46 au secteur des télécommunications, la directive 2006/24/CE relative à la conservation des données traitées en matière de communications électroniques et la décision 2008/977/JAI relative à la protection des données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Cependant depuis l'entrée en vigueur du traité de Lisbonne, l'Union a entrepris une refonte de sa législation

192 Voy. Directive du Parlement européen et du Conseil, du 24 octobre 1995, JOCE, n L281 du 23 novembre1995, p. 31.

193 Le Land allemand de Hesse a adopté en 1970 la première loi sur la protection des données au monde, qui ne s'appliquait qu'à cet État. La Suède a adopté le Datalagen en 1973; L'Allemagne a adopté le *Bundesdatenschutzgestez* en 1976; La France a adopté en 1977 la Loi relative à l'informatique, aux fichiers et aux libertés. Le Royaume-Uni a adopté en 1984 la loi sur la protection des données. Enfin, les Pays-Bas ont adopté le Wet *Persoonregistraties* en 1989.

en la matière. La réforme a conduit à l'adoption du règlement général sur la protection des données en avril 2016, remplaçant la directive 95/46 et la directive relative à la collecte et au traitement des données dans le domaine pénal[194] abrogeant la décision-cadre 2008/977/JAI. Les débats sur la nécessité de moderniser les règles de protection des données de l'UE ont débuté en 2009, lorsque la Commission a lancé une consultation publique sur le futur cadre juridique du droit fondamental à la protection des données à caractère personnel. La proposition de règlement a été publiée par la Commission en janvier 2012, marquant le début d'un long processus législatif de négociations entre le Parlement européen et le Conseil de l'UE. Après son adoption, le règlement général sur la protection des données (ci-après RGPD) prévoyait une période de transition de deux ans. Il est devenu pleinement applicable le 25 mai 2018, date à laquelle la directive sur la protection des données a été abrogée.

21 La directive *e-privacy*. L'établissement de règles spéciales de protection des données a également été jugé nécessaire dans le secteur des communications électroniques. Avec le développement d'Internet et de la téléphonie mobile, il était important de veiller à ce que les droits des utilisateurs à la vie privée et à la confidentialité soient respectés. La directive 2002/58 / CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans les communications électroniques[195] (directive sur la vie privée et les communications électroniques ou directive sur la vie privée) établit des règles sur la sécurité des données personnelles et la confidentialité des communications. Parmi les obligations, les opérateurs de services de communications électroniques doivent, entre autres, veiller à ce que l'accès aux données personnelles soit limité aux personnes autorisées et prendre des mesures pour éviter la destruction, la perte ou l'endommagement de ces données[196] · Si, en dépit des mesures de sécurité mises en œuvre, une violation de la sécurité se produit, les opérateurs doivent en informer l'autorité nationale compétente chargée de la mise en œuvre de la sécurité et l'application de la directive de ladite violation de données personnelles. Les opérateurs sont parfois tenus de notifier également les violations de données personnelles aux individus, notamment lorsque la violation est susceptible d'affecter leurs données personnelles ou leur vie privée[197]. La confidentialité des communications nécessite que l'écoute, le stockage ou tout type de surveillance ou d'interception des communications sur les métadonnées soient, en principe, interdit. La directive interdit également les communications non sollicitées (souvent appelées « *spam* »), sauf si les utilisateurs ont donné leur consentement, et contient des règles sur le stockage des « *cookies »* sur les ordinateurs et les appareils. Ces obligations négatives indiquent clairement que la confidentialité des communications est étroitement liée à la protection du droit au respect de la vie privée consacré à l'article 7 de la Charte et au droit à la

194 Directive 680/16 du Parlement européen et du Conseil du 27 avril 2016, relative à la protection des personnes physiques a l'égard du traitement des données a caractère personnel par les autorités compétentes a des fins de prévention et de détection des infractions pénales d'enquêtes et de poursuite en la matière ou d'exécution de sanctions pénales et à la libre circulation de ces donnes, JOUE, n L119 du 4 mai 2016, p.89.

195 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

196 Voy. art. 4 § 1.

197 Voy. art. 4 § 2.

protection des données personnelles consacré à l'article 8 de la Charte. En janvier 2017, la Commission a publié une proposition de règlement concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques, destinée à remplacer la directive sur la vie privée et les communications électroniques. La réforme vise à aligner les règles régissant les communications électroniques avec le nouveau régime de protection des données établi en vertu du règlement général sur la protection des données. Le nouveau règlement sera directement applicable dans toute l'Union ; tous les individus bénéficieront du même niveau de protection de leurs communications électroniques, tandis que les opérateurs et les entreprises de télécommunication bénéficieront de la clarté, de la sécurité juridique et de l'existence d'un ensemble unique de règles dans toute l'Union. Les règles proposées en matière de confidentialité des communications électroniques s'appliqueront également aux nouveaux acteurs fournissant des services de communication électronique qui ne sont pas couverts par la directive sur la vie privée et les communications électroniques. Avec une utilisation massive de services tels que Skype, WhatsApp, Facebook Messenger et Viber pour envoyer des messages ou appeler, les acteurs fournissant des services de communication électronique entreront désormais dans le champ d'application de la réglementation et devront respecter ses exigences en matière de protection des données, de confidentialité et de sécurité. Au moment de la publication de cette thèse, un processus législatif sur les règles de confidentialité électronique était toujours en cours.

22 Le règlement 45/2001. La directive 95/46 sur la protection des données ne s'appliquant qu'aux États membres de l'UE, un instrument juridique supplémentaire était nécessaire pour assurer la protection des données pour le traitement des données personnelles par les institutions et organes de l'UE. Le règlement (CE) n ° 45/2001 relatif à la protection des personnes à l'égard du traitement des données à caractère personnel par les institutions et organes de la Communauté et à la libre circulation de ces données (Règlement de l'Union sur la protection des données) assume cette tâche. Le règlement n° 45/2001 suit de près les principes du régime général de protection des données de l'UE et applique ces principes au traitement des données effectués par les institutions et organes de l'UE dans l'exercice de leurs fonctions. En outre, il établit une autorité de surveillance indépendante chargée de veiller à l'application de ces dispositions, le contrôleur européen de la protection des données (CEPD). Le CEPD est investi de pouvoirs de surveillance des traitements de données à caractère personnel mises en œuvre par les institutions et organes de l'Union. Il a aussi pour mission d'enquêter sur les plaintes pour violation présumée des règles de protection des données. Il conseille également les institutions et organes de l'Union sur toutes les questions relatives à la protection des données personnelles, allant des propositions de nouvelle législation à l'élaboration de règles internes relatives à l'informatique. En janvier 2017, la Commission européenne a présenté une proposition de nouvelle réglementation sur le traitement des données par les institutions de l'Union, qui abrogera le règlement actuel. Comme pour la réforme de la directive « vie privée et communications électroniques », la réforme du règlement n ° 45/2001 modernisera et alignera ses règles sur le nouveau régime de protection des données établi en vertu du règlement général sur la protection des données.

23 La refonte dans l'ex-premier pilier : le RGPD. L'adoption du règlement général sur la protection des données en 2016 (ci-après RGPD) a modernisé la législation de l'Union en matière de protection des données, la rendant ainsi apte à protéger les droits fondamentaux dans le contexte des défis économiques et sociaux de l'ère numérique. Le RGPD préserve et développe les principes et droits fondamentaux de la personne concernée dans la directive 95/46 sur la protection des données. Cependant, il a introduit de nouvelles obligations pour les entreprises et acteurs publics afin de mettre en œuvre la protection des données dès la conception et par défaut ; imposer la nomination dans certaines circonstances d'un délégué à la protection des données ; se conformer à un nouveau droit à la portabilité des données et respecter le principe de responsabilité. En vertu du droit de l'Union, les règlements sont directement applicables. Cela crée des règles cohérentes de protection des données dans l'ensemble de l'Union, établissant un environnement de sécurité juridique dont les opérateurs économiques et les particuliers en tant que « personnes concernées » peuvent bénéficier. Cependant, même si le règlement général sur la protection des données est directement applicable, les États membres sont tenus de mettre à jour leurs lois nationales sur la protection des données et de se conformer pleinement au règlement, tout en conservant une marge d'appréciation pour les dispositions spécifiques du considérant[198]. Concernant son application territoriale et matérielle, le règlement s'applique aux entreprises établies dans l'Union et également aux responsables et aux sous-traitants non établis dans l'Union lorsqu'ils offrent des biens ou des services aux personnes concernées dans l'Union ou surveillent leur comportement. Comme plusieurs entreprises technologiques d'outre-mer détiennent une partie importante du marché européen et traitent des millions de données de ressortissants européens, soumettre ces organisations aux règles de protection des données de l'Union est crucial pour assurer la protection des individus et garantir des conditions de concurrence équitables.

24 La refonte dans l'ex-troisième pilier : La directive 680/16. La directive sur la protection des données 95/46, désormais abrogée, se limitait à encadrer les activités relevant du marché intérieur et celles des autorités publiques autres que les forces de l'ordre. L'adoption d'instruments spéciaux était donc primordiale pour atteindre la clarté et l'équilibre nécessaires entre la protection des données et d'autres intérêts légitimes et pour relever les défis qui sont particulièrement pertinents dans des secteurs spécifiques. C'est le cas des règles régissant le traitement des données personnelles par les autorités répressives. Le premier instrument

[198] Voy. Considérant 10 du RGPD: Afin d'assurer un niveau cohérent et élevé de protection des personnes physiques et de lever les obstacles aux flux de données à caractère personnel au sein de l'Union, le niveau de protection des droits et des libertés des personnes physiques à l'égard du traitement de ces données devrait être équivalent dans tous les États membres. Il convient dès lors d'assurer une application cohérente et homogène des règles de protection des libertés et droits fondamentaux des personnes physiques à l'égard du traitement des données à caractère personnel dans l'ensemble de l'Union. En ce qui concerne le traitement de données à caractère personnel nécessaire au respect d'une obligation légale, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement, il y a lieu d'autoriser les États membres à maintenir ou à introduire des dispositions nationales destinées à préciser davantage l'application des règles du présent règlement. Parallèlement à la législation générale et horizontale relative à la protection des données mettant en œuvre la directive 95/46/CE, il existe, dans les États membres, plusieurs législations sectorielles spécifiques dans des domaines qui requièrent des dispositions plus précises. Le présent règlement laisse aussi aux États membres une marge de manœuvre pour préciser ses règles, y compris en ce qui concerne le traitement de catégories particulières de données à caractère personnel (ci-après dénommées «données sensibles»). À cet égard, le présent règlement n'exclut pas que le droit des États membres précise les circonstances des situations particulières de traitement y compris en fixant de manière plus précise les conditions dans lesquelles le traitement de données à caractère personnel est licite.

juridique de l'Union encadrant ce domaine a été la décision-cadre 2008/977 / JAI[199] du Conseil relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. Ses règles ne s'appliquaient qu'aux données policières et judiciaires échangées entre États membres. Le traitement national des données personnelles par les forces de l'ordre avait été exclu de son champ d'application. La Directive 2016/680[200] relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention, de la recherche, de la détection ou de la répression d'infractions pénales ou de l'exécution de sanctions pénales et la libre circulation de ces données, a remédié à cette situation. Adoptée en parallèle au RGPD, la directive 680/2016 a abrogé la décision-cadre 2008/977 / JAI et mis en place un système complet de protection des données à caractère personnel liées à la sécurité publique. Alors que le RGPD établit des règles générales pour protéger les personnes en ce qui concerne le traitement de leurs données personnelles et assurer la libre circulation de ces données au sein de l'Union, la directive établit des règles spécifiques pour la protection des données en matière pénale et coopération policière. Lorsqu'une autorité compétente traite des données à caractère personnel à des fins de prévention, d'enquête, de détection ou de poursuite d'infractions pénales, la directive 2016/680 s'applique. Lorsque les autorités compétentes traitent des données à caractère personnel à d'autres fins que celles mentionnées ci-dessus, le régime général prévu par le règlement général sur la protection des données s'applique. Contrairement à son prédécesseur (décision-cadre 2008/977 / JAI), le champ d'application de la directive 2016/680 s'étend au traitement national des données à caractère personnel par les autorités répressives et ne se limite pas aux échanges de données entre États membres[201]. En outre, la directive vise à établir un équilibre entre les droits des individus et les objectifs légitimes du traitement lié à la sécurité. À cette fin, la directive affirme le droit à la protection des données à caractère personnel et les principes de base devant régir le traitement de ces données, en suivant les règles et principes consacrés dans le RGPD. La directive prend également en compte et tente d'aborder de sérieux défis technologiques émergents qui peuvent avoir un impact particulièrement grave sur les individus, tels que l'utilisation de techniques de profilage par les autorités répressives. En principe, les décisions fondées uniquement sur le traitement automatisé, y compris le profilage, doivent être interdites[202]. En outre, elles ne doivent pas reposer sur des données sensibles. Ces principes sont soumis à certaines exceptions prévues par la directive. De plus, un tel traitement ne doit entraîner aucune discrimination[203]. La directive

199 Voy. La décision cadre 2008/977 / JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

200 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil.

201 Voy. C. DI FRANCESCO MAESA, *Balance between Security and Fundamental Rights Protection: An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR, ,* Eurojus, 2016, disponible à l'adresse/ http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/

202 Voy. l'art. 11 §1.

203 Voy. art. 11 §2 et 3.

contient également des règles pour assurer la responsabilité des autorités. Elles doivent désigner un délégué à la protection des données chargé de contrôler le respect des règles de protection des données, d'informer et de conseiller l'entité et les employés chargés du traitement de leurs obligations, et de coopérer avec l'autorité de contrôle. Ainsi, le traitement des données à caractère personnel dans le secteur de la police et de la justice pénale est désormais soumis au contrôle d'autorités de contrôle indépendantes. Et le régime juridique général de la protection des données et le régime spécial de protection des données pour les forces de l'ordre en matière pénale doivent tous deux respecter les exigences de la Charte des droits fondamentaux de l'Union.

25 Le rôle de la Cour de justice. La Cour de justice a compétence pour déterminer si un État membre a rempli ses obligations en vertu de la législation européenne sur la protection des données et pour interpréter la législation de l'Union européenne afin de garantir son application effective et uniforme dans tous les États membres. Depuis l'adoption de la directive sur la protection des données en 1995, une jurisprudence considérable s'est stratifiée, clarifiant la portée et la signification des principes de protection des données et du droit fondamental à la protection des données personnelles consacré par l'article 8 de la Charte. Même si la directive a été abrogée et qu'un nouvel instrument juridique, le RGPD est désormais en vigueur, cette jurisprudence préexistante reste pertinente et valable pour l'interprétation et l'application des principes de protection des données de l'Union, dans la mesure où les principes fondamentaux de la directive sur la protection des données ont été transposés dans le RGPD. S'appuyant sur l'article 8 de la Charte, la Cour de justice a rendu plusieurs arrêts historiques qui répondent aux questions que soulèvent l'intensification du recours aux données personnelles dans la société de l'information. Ainsi dans l'arrêt *Google Spain*[204], elle a consacré l'existence d'un droit au déréférencement [205] dans le droit de l'Union européenne. Ici la Cour de justice a en effet considéré que compte tenu de la place d'Internet dans la société moderne, l'ingérence dans la vie privée est potentiellement très grave et ne saurait être justifiée par l'intérêt économique de l'exploitant d'un moteur de recherche ou l'intérêt légitime des internautes à avoir accès à ces informations[206]. D'ailleurs l'apport de cette jurisprudence est tel que le droit à l'oubli a été codifié dans l'article 17 du RGPD. De plus, dans ce même arrêt la Cour de justice applique la directive 95/46 à l'entreprise Américaine Google Inc. au nom de l'effet utile du droit au « respect de la vie privée à l'égard du traitement de données à caractère personnel »[207], elle donne un effet extraterritorial à la législation de l'Union. Cette application a été retenue par le législateur et se trouve codifié par l'article 3 du RGPD.
La Cour de justice est intervenue également sur un autre trait marquant la société de l'information, c'est-à-dire le développement de la surveillance de masse dans le but de garantir la sécurité publique. Ainsi elle a déclaré la directive 2006/24 invalide dans l'affaire *Digital*

---

204 CJUE, *Google Spain*, aff. C-131/12, 13 mai 2014.

205 C'est-à-dire le droit pour un individu de demander à l'exploitant d'un moteur de recherche sur internet de supprimer de la liste de résultats affichés à la suite d'une recherche effectuée à partir de son nom des liens vers des pages web, publiées par des tiers et contenant des informations relatives à cette personne.

206 Voy. §80 de l'arrêt *Google Spain.*

207 Voy. §57-59 de l'arrêt *Google Spain.*

Rights Ireland[208], car disproportionnée[209] dans l'objectif légitime de lutte contre le terrorisme vis-à-vis de la protection des données personnelles.
De plus, la Cour de justice est intervenue à nouveau sur la question de la rétention des données se prononçant cette fois-ci sur les législations nationales adoptées en application de la directive 2006/24. Ainsi dans l'affaire *Tele2 Sverige*, elle a expliqué dans quelles conditions une règlementation permettant la conservation des données relatives au trafic et des données de localisation dans le but de lutter contre le terrorisme et la criminalité pouvaient être conformes au droit fondamental à la protection des données personnelles et à la vie privée[210]. Dans l'arrêt *Schrems*, la Cour de justice a invalidé la décision de la Commission européenne *« Safe Harbour* »[211] autorisant le transfert des données personnelles de l'Union vers les États-Unis à cause des graves carences de la protection des données personnelles. Ainsi la Commission a dû renégocier une nouvelle décision d'adéquation, l'accord « *Privacy Shield* » permettant ledit transfert. Dans son avis 1/ 15 sur le transfert des données des passagers « *PNR* ou *Passagers Name Record* » entre l'Union européenne et le Canada, la Cour de justice a indiqué un certain nombre de règles tenant au type de données collectées et à la durée du stockage.

B. Une approche inhérente à l'identité européenne

26 La spécificité de la régulation multiniveau. Le droit européen à la protection des données personnelles est un droit récent né avec le développement de l'informatique puis de l'Internet. Cela explique sans doute que l'interrégulation[212] dans le domaine de la protection des données personnelles ait été délaissée par la doctrine. En effet les phénomènes d'interrégulation ont été principalement étudiés dans le cadre des domaines traditionnels de la régulation, à savoir la

208 CJUE, Digital Rights Ireland, aff : jtes C-293/12 et C-594/12, 8 avril 2014, Voy § 108 et s.

209 Plus précisément, la directive définissait une obligation pour les fournisseurs de services de télécommunications et les fournisseurs d'accès internet de conserver l'ensemble des informations relatives aux communications et connexions de tous les utilisateurs pour une durée considérable comprise entre 6 et 24 mois.

210 Voy 109-111 de l'arrêt *Tele2Sverige*. Ainsi la règlementation nationale doit prévoir des règles claires et précises régissant la portée et l'application d'une telle mesure de conservation des données et offrir des garanties suffisantes permettant de protéger efficacement les personnes concernées contre des risques d'abus. Son ampleur doit également être précisément délimitée à ce qui est strictement nécessaire compte tenu de l'objectif poursuivi, s'agissant du public visé.

211 Voy. Décision d'exécution 2000/520/CE prise en application de l'article 25§6 de la directive 95/46.
212 La notion d'interrégulation caractérise en général les relations entre les autorités de régulation. L'interrégulation rend compte de la nécessité de dépasser la segmentation initiale de la régulation en raison de l'évolution de la complexité et de l'interdépendance des marchés. Il y a alors une dialectique entre interrégulation sectorielle et régulation intersectorielle. La première vise à faire le lien entre les régulations sectorielles tout en les maintenant. La seconde tend à prôner la fusion des autorités intervenant dans des secteurs connexes pour des raisons d'efficacité. Pour une analyse approfondie de ce concept, cf. H. DELZANGLES, « La notion d'interrégulation », in G. ECKERT et J.-Ph. KOVAR, *L'interrégulation*, L'Harmattan, coll. « Logiques juridiques », 2015.

concurrence, et les secteurs tels que les télécommunications, l'audiovisuel, les secteurs bancaire et financier[213].

Le modèle européen de la protection des données personnelles a été conçu dès l'origine comme une interrégulation multiniveau : à l'échelle des États et à l'échelle de l'Union européenne.

Tout d'abord, cette régulation multiniveau s'est construite par étapes des États vers l'Union. Certains États européens ont adopté des législations spécifiques[214] sur la protection des données personnelles dans les années 1970[215].

Deuxièmement, la directive n° 95/46, ayant pour objectif à la fois de faciliter les flux des données personnelles entre les États membres de l'Union européenne et vers des pays tiers, a généralisé à l'échelle communautaire l'institutionnalisation des autorités nationales de régulation. L'ambition de ce texte était de créer une régulation multiniveau avec des autorités de contrôle au sein de chaque État membre et à l'échelle européenne avec le groupe dit de l'article 29 (G29).

Enfin, une régulation de la protection des données pour les institutions et organes de l'Union a été mise en place par le règlement n° 45/2001/CE. Ce dernier institue le Contrôleur européen des données personnelles (CEPD) en tant qu'autorité de contrôle indépendante qui a pour mission de garantir le respect dudit règlement. La régulation verticale entre l'échelon national et celui de l'Union européenne est ainsi complétée par une régulation horizontale à l'échelle de l'Union européenne elle-même.

Cette régulation a été complétée par des régimes spécifiques liés au système de compétences des Communautés, puis de l'Union européenne[216] . La décision-cadre n° 2008/977 JAI du Conseil a été adoptée dans le cadre de la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale. En outre, il existe des régulations *sui generis* dans le cadre du domaine des migrations et du contrôle des frontières. Ces régulations sont liées à l'existence de bases de données sensibles telles que le Système d'information Schengen (SIS II), le Système d'information visa (VIS), Eurodac. L'Agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'Espace de liberté, de sécurité et de justice (EU-Lisa)[217] a été créée en 2012 afin d'assurer un haut niveau de protection des données autour de ces trois fichiers. Dans le domaine de la coopération judiciaire, la création d'Europol et d'Eurojust a aussi été accompagnée de deux autorités de contrôle communes. Depuis le traité de Lisbonne, la protection des données

213 Voy. O.TAMBOU, « L'émergence d'un modèle européen d'interrégulation en matière de protection des données personnelles » . *Liber Amicorum en l'honneur du professeur Joël Monéger*, Lexis Nexis, 2017, p.381-394.

214 Chacune de ces lois a introduit une autorité de contrôle, le *Datenschutzbeauftragter* dans le Land du Hesse, le *Bundesbeauftragter für den Datenschutz* pour la RFA, la *Datainspektionen* en Suède, et la Commission nationale de l'informatique et des libertés (CNIL) en France. Autrement dit, dès l'origine, l'existence d'une autorité de contrôle a constitué un élément essentiel.

215 Le Land de Hesse en Allemagne, la Suède, l'État fédéral allemand et la France ont ainsi été précurseurs en la matière. Voy. G. GONZALEZ FUSTER, *The emergence of Personal Data Protection as a fundamental Right of the EU,* Springer, 2014 spéc. p. 55 et s.

216 Voy. « Manuel européen de la protection des données », Agence des droits fondamentaux de l'Union européenne et Conseil de l'Europe, Office des publications de l'Union européenne, 2014, p. 161.

217 Voy. Règl. n° 1077/2011, portant création d'une agence européenne pour la gestion opérationnelle des systèmes d'information à grande échelle au sein de l'espace de liberté, de sécurité et de justice : JOUE n° L 286, p. 1.

personnelles repose sur des bases juridiques spécifiques. D'une part, l'article 8 de la Charte des droits fondamentaux consacre la protection des données personnelles comme un droit fondamental dissocié de celui du respect de la vie privée. D'autre part, l'article 16 du Traité sur le fonctionnement de l'Union européenne (ci-après TFUE) permet l'adoption de normes de droit dérivé afin de protéger ce droit fondamental. Dans ce contexte l'apport du traité de Lisbonne a permis au droit à la protection des données personnelles de reposer sur des bases juridiques spécifiques. D'une part l'article 16 TFUE constitue désormais la base juridique de droit commun du droit européen de la protection des données personnelles sur laquelle la réforme de la protection des données personnelles a vu le jour. Initiée en 2012, cette réforme globale repose sur deux textes : le règlement définissant le cadre général de l'Union européenne pour la protection des données (ci-après RGPD)[218], et la directive sur le traitement des données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et libre circulation des données (ci-après directive CJPP)[219]. D'autre part, l'article 8 de la Charte des droits fondamentaux consacre la protection des données personnelles comme un droit fondamental dissocié de celui du respect de la vie privée[220].

27 L'approche américaine. Ainsi l'émergence d'un modèle européen de protection des données personnelles peut s'apprécier grâce à l'analyse d'autres traditions juridiques comme celle née dans le droit nord-américain[221] . En effet, les États-Unis ont une conception très différente de la protection des données personnelles depuis l'« invention » du « *right to privacy* » par l'article de Warren et Brandeis en 1890[222]. Cette différence tient tout d'abord à l'organisation même du système de droit américain : au niveau fédéral, seules les atteintes portées par le Gouvernement à la vie privée des citoyens sont visées par le « *Privacy Act* ». Les autres atteintes à la vie privée et à la protection des données personnelles relèvent de la compétence propre de chaque État et de ses Tribunaux, comme l'a décidé la Cour Suprême dès 1965 [223] . À ces sources s'ajoute le caractère sectoriel des réglementations applicables, contrairement au droit européen qui regroupe les règles relatives à la protection des données européennes au sein d'un texte unique, le droit américain légifère par secteur d'activités. Cette diversité est expliquée par James Whitman[224] avec l'argumentation selon laquelle, la protection de la vie privée en Europe est rattachée à la « dignité » de la personne alors qu'elle révélerait

218 Voy. Règl. n° 2016/679, 27 avr. 2016 : JOUE n° L 199, p. 1.

219 Voy. Dir. n° 2016/680, 27 avr. 2016 : JOUE n° L 119, p. 89.

220 G. GONZALEZ FUSTER, *The emergence of Personal Data Protection as a fundamental Right of the EU*, Springer, 2014.

221 C. CASTETS-RENARD, *Quels liens établir avec les US et l'UE en matière de vie privée et de protection des données personnelles ?*, Dalloz IP/IT 2016, p. 115.

222 S. D. WARREN, L. D. BRANDEIS, *The Right to Privacy*, Harvard Law Review, 1890, 4, p. 193-220.

223 Griswold c/ Connecticut, 381 U.S. 479 (1965). Voy. E. ZOLLER, *Grands arrêts de la Cour suprême des États-Unis*, Paris, PUF, coll. « Droit fondamental », 2000, p. 694.

224 Voy. J. L. HALPPÉRIN, in *Nouveaux Cahiers du Conseil constitutionnel*, N° 48 (Dossier : Vie Privée), Juin 2015, p. 59-68.

de la « liberté » aux États-Unis[225].Toutefois, des signes de convergence apparaissent. Depuis l'invalidation de l'accord « *Safe Harbor »* et l'adoption du « *Privacy Shield* », les États-Unis semblent vouloir adopter une approche plus proche de la conception européenne. Ainsi l'administration Obama avait proposé des mesures visant à imposer des restrictions à l'utilisation des données issues des moteurs de recherche. Cependant l'administration Trump a porté un coup d'arrêt à ces initiatives avec l'adoption du *Cloud Act*[226]. Il semble que le chemin de la convergence reste long à parcourir.

Le but de cette introduction est de montrer la manière dont le droit à la protection des données personnelles s'est construit dans le droit de l'Union et de vérifier si le régime de protection est efficace, en soulignant le passage d'un droit attaché au marché intérieur et donc de nature politique et économique à un droit qui s'est constitutionnalisé grâce au rôle du Juge et à la constitutionnalisation de la Charte. En effet la libre circulation des marchandises, des capitaux, des services et des personnes au sein du marché intérieur imposait la libre circulation des données, impossible à réaliser si les États membres ne pouvaient pas se fier à un niveau uniformément élevé de protection des données.

***

28 Résumé de la problématique : La présente analyse veut évaluer la valeur ajoutée du droit à la protection des données personnelles comme droit autonome, ce qui implique d'étudier le droit fondamental à la protection des données de manière isolé. De plus, cette autonomisation du droit à la protection des données personnelles vis-à-vis du droit au respect de la vie privée a permis l'affranchissement du raisonnement de la Cour de justice de la jurisprudence de la CourEDH. Ainsi ce parcours d'autonomisation de la Cour de justice sera illustré à travers des affaires récentes. Il s'agit d'un droit qui connaît aujourd'hui un « fabuleux destin »[227] grâce au rôle de la Cour de justice en tant que cœur de la gouvernance européenne [228] . Le droit fondamental à la protection des données constituerait le vecteur privilégié pour étudier l'identité européenne « positive », c'est-à-dire celle qui permet de constituer une entité européenne de l'intérieur, de façon active et non simplement passivement du seul fait de la différence. Ainsi à travers le droit à la protection des données, l'Union européenne exporte ses valeurs et son standard de protection dans le monde. La première partie de la thèse est dédiée à l'examen du régime de protection original et spécifique offert par la législation de l'Union européenne dans sa dimension interne et externe, y compris un examen critique de la réforme lancée en janvier 2012 et aboutie en mai 2018. Une attention particulière sera portée à la dimension externe de

225 J. WHITMAN, « The Two Western Cultures of Privacy : Dignity v. Liberty », *The Yale Law Journal*, 113, 2004, p. 1151-1221.

226 Le Cloud Act (Clarifying Lawful Overseas Use of Data Act) est une loi votée par le Congrès américain afin de faciliter l'obtention pour l'administration américaine de données stockées ou transitant à l'étranger, via notamment les opérateurs et fournisseurs de services en ligne.

227 J. ZILLER, *Le fabuleux destin des Explications relatives à la Charte des droits fondamentaux de l'Union européenne*, in Jean-Paul Jaqué, *Chemins d'Europe. Mélanges,* Paris, Dalloz, 2010, p. 765-781.

228 S. SAURUGGER et F. TERPAN, *La Cour de justice au cœur de la gouvernance européenne*, *Pouvoirs*, n° 149, 2014, p. 59-75. En effet deux arrêts historiques ont été rendus, l'arrêt *Data Retention* qui a annulé la Directive 2006/24/ CE relative à la rétention des données et l'arrêt *Google Spain* qui a consacré le droit à l'oubli numérique.

la protection des données personnelles dans le droit de l'Union européenne et à une analyse des mécanismes à travers lesquels elle assure un niveau élevé de protection aux données personnelles qui sont transférées vers les pays tiers. La thèse se propose, donc, de souligner les résultats obtenus par une véritable « politique étrangère » de l'Union européenne en matière de droit à la protection des données personnelles. Une attention particulière sera portée aux relations entre États-Unis et Union européenne à la lumière du contentieux entre les deux rives de l'Atlantique. Dans les dernières années, en effet, le phénomène du transfert international des données personnelles n'a pas exclusivement été lié à des raisons de caractère commercial, il résulte de plus en plus des exigences de protection de la sûreté publique. En effet, le partage des données personnelles entre les autorités de police des différents pays est devenu un élément essentiel dans le cadre de la coopération dans la lutte contre le terrorisme et le crime international organisé. Comme il se verra, le droit de l'Union européenne doit constamment mettre en balance les impératifs de la sûreté publique avec le droit fondamental de l'individu à la protection des données personnelles. La deuxième partie de la thèse est dédiée à la mise en œuvre du droit à la protection des données personnelles tant par les juridictions européennes que par les instances quasi-juridictionnelles afin d'illustrer la conciliation entre le droit à la protection des données personnelles et d'autres droits fondamentaux. En effet, le cadre juridique de la protection des données personnelles résulte ainsi d'un ensemble de textes communautaires, dont le respect et l'interprétation sont assurés par des organes *ad hoc* qui viennent au soutien des juridictions de droit commun. Le droit fondamental à la protection des données personnelles sera le prisme pour observer la définition d'une identité européenne. Il faut alors se demander si le droit à la protection des données personnelles dans l'Union constitue un objectif en soi, appelant à bâtir un modèle européen reposant sur des valeurs communes et qui contribuerait à la construction d'une entité politique européenne, ou si l'harmonisation en la matière n'est qu'un instrument au service d'autres politiques[229].

229 Pour une réflexion sur la capacité de l'Union européenne à affirmer un projet européen humaniste inspiré par la protection des droits fondamentaux Voy. E. DUBOUT, *L'échec de la citoyenneté européenne ? Les mutations d'une citoyenneté complexe en période de crise identitaire*, *Jus Politicum*, juill. 2017, n° 18, Ebook, http://juspoliticum.com

PARTIE I. UNE EXTENSION PROGRESSIVE DU CHAMP DE LA PROTECTION

PARTIE II. UNE ARTICULATION COMPLEXE DES MODES DE PROTECTION

PARTIE I. UNE EXTENSION PROGRESSIVE DU CHAMP DE LA PROTECTION

29 Le cadre de protection. Le droit fondamental à la protection des données à caractère personnel est un droit qui, relativement à d'autres domaines, se caractérise par un fort niveau d'harmonisation, tant par le droit issu de la Convention européenne des droits de l'homme que par le droit de l'Union européenne. Par ailleurs, le régime de protection offert par le droit de l'Union est assuré par des sources de droit primaire et secondaire. Le cadre juridique de protection accordé aux données personnelles est spécifique à l'Union européenne et relève de son identité. Ainsi le législateur, conscient qu'avec la révolution numérique la protection des données et les règles touchant à la vie privée du citoyen ne peuvent plus s'arrêter aux frontières nationales et que l'espace économique européen a besoin d'un standard commun, est intervenu au fil du temps avec plusieurs instruments législatifs couvrant différents domaines, ce qui illustre la construction fonctionnaliste de l'Union européenne[230].

Bien que le droit à la vie privée dans son élément statique de droit « *to be let alone* » soit né en 1890 aux États-Unis[231], le droit à la protection des données personnelles conçu comme un droit dynamique à « l'autodétermination informationnelle » est né avec le développement d'Internet [232] . C'est pour faire face aux risques liés aux technologies et à l'utilisation des données personnelles qu'une réglementation spécifique a été élaborée au sein de l'Union européenne. La législation de l'Union européenne en matière de protection des données personnelles apparaît donc hétérogène avec des instruments distincts pour encadrer la protection des données personnelles dans le marché intérieur et dans l'Espace de Liberté Sécurité et Justice (ci-après ELSJ). Les données à caractère personnel sont un outil précieux non seulement pour les échanges économiques[233] mais également pour le renseignement dans la lutte contre la criminalité, comme le démontre la tentative, de la part des États-Unis, d'accéder aux données à caractère personnel entre les mains des GAFAM (Google, Amazon, Facebook, Apple, Microsoft) où qu'elles se trouvent à travers le « *Cloud Act* » [234] . La Commission européenne a d'ailleurs présenté le 17 avril 2018 dans un communiqué de presse[235] une proposition de règlement « *e-evidence* »[236] afin de rendre plus facile et plus rapide pour les autorités policières et judiciaires l'obtention de preuves électroniques situées dans le *cloud* et

230 S. PEYROU, « La protection des données à caractère personnel : un droit désormais constitutionnalisé et garanti par la CJUE », in R. TINIÈRE et C. VIAIL (dir.), *La protection des droits fondamentaux dans l'Union européenne*, Bruylant, 2013, p215.

231 S. WARREN, L. BRANDEIS, *The right to privacy*, in *Harvard law rewiev*, vol. 4, 1890, p. 193.

232 S. RODOTÀ, *Tecnologie e diritti*, Il Mulino,1995 p. 23.

233 Avec le développement exponentiel des technologies de l'information, d'Internet et du numérique le partage des données ne connaît plus de limites, ce qui génère une valeur économique mais également un danger pour la vie privée des personnes dont les données sont exploitées.

234 Le *Cloud Act* entre ainsi en contradiction avec les dispositions du RGPD (Règlement UE 2016/679), notamment les articles 44 et suivants et spécialement l'article 48 sur les « Transferts ou divulgations non autorisés par le droit de l'Union » qui dispose que « Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international […] »

235 Voy. le communiqué de presse IP/18/3343, disponible à l'adresse: http://europa.eu/rapid/press-release_IP-18-3343_fr.htm

236 Voy. la proposition de reglèment e-evidence COM (2018)225 final disponible à l'adresse: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A225%3AFIN

nécessaires afin d'enquêter, de poursuivre et de condamner des criminels et des terroristes[237]. La tension entre liberté et sécurité est au cœur de la construction du droit pénal européen[238]. Suite aux attentats du 11 septembre aux États-Unis, l'Union européenne a connu une accélération dans la construction de sa politique de sécurité externe. Dans ce contexte, des mesures et accords spécifiques pour l'échange des données et renseignements avec des États tiers ont été adoptés[239]. Cela a renforcé l'intégration de l'Union européenne au mépris de la subsidiarité[240]. Il est possible de parler de dimension interne du droit à la protection des données personnelles, encadrant les échanges liés au marché intérieur (Titre I), et de dimension externe liée à la politique étrangère de l'Union européenne (Titre II).

237 Pour aller plus loin voy. S. PEYROU, *Le projet de règlement « E-evidence » (preuves électroniques) présenté par la Commission européenne : un « Cloud Act » européen*, disponible à l'adresse : http://www.gdr-elsj.eu/2018/04/24/droits-fondamentaux/le-projet-de-reglement-e-evidence-preuves-electroniques-presente-par-la-commission-europeenne-un-cloud-act-europeen/.

238 C. MURPHY et D. ACOSTA ARCARAZO, « Rethinking Europe's Freedom, Security and Justice », *in* C. MURPHY et D. ACOSTA ARCARAZO (dir.), *EU Security and Justice Law: After Lisbon and Stockholm*, Hart, 2014, pp. 1-16, sp. p. 5.

239 Voy. Notamment la décision cadre 2008/977/JAI.

240 M. DELMAS-MARTY, « L'intrégration européenne entre pluralisme, souverainisme et universalisme », *RSC*, 2016, n°3, p. 447-454, sp. p. 447.

TITRE I. LA MUTATION INTERNE DU STANDARD DE PROTECTION

30 La *summa divisio.* Qualifiées de « nouveau pétrole de l'économie »[241], les données ont une valeur marchande qui a conduit certains à préconiser une fiscalité en partie assise sur le volume de données traitées par des entreprises ayant pour activité principale le suivi régulier et systématique des clients [242] . La complexité du sujet vient notamment de son caractère interdisciplinaire et de la complication croissante des technologies dans la société. Ainsi l'accélération des échanges de données personnelles dues à leur valeur marchande[243] sont une source de risque pour les droits et libertés des personnes physiques ainsi que pour la concurrence. La naissance de nouveaux modèles économiques, s'appuyant en grande partie sur l'exploitation et le commerce des données, a rendu nécessaire une plus grande harmonisation législative au sein de l'Union européenne, afin de permettre l'émergence d'un véritable marché unique numérique [244] . Le législateur de l'Union européenne, conscient que des régimes nationaux différents à l'égard de la protection des données personnelles pouvaient entraver les échanges et le fonctionnement du marché intérieur, a élaboré au début des années 1990, un cadre juridique hétérogène initié par la directive 95/46[245]. D'autres textes sont venus compléter le dispositif. Au nombre de ceux-ci figurent certains instruments relevant de l'ancien premier pilier, tels que la directive 2002/58/CE[246] sur la vie privée et les communications électroniques,

---

241 P.N COLLIN, Rapport au ministre de l'Économie et des Finances, au ministre du Redressement productif, au ministre délégué chargé du budget et à la ministre chargée des petites et moyennes entreprises, de l'innovation et de l'économie numérique, janv. 2013, p. 49 (ci-après Rapport Collin).

242 Voy. Le Rapport COLLIN préec. p. 121 et s.

243 La collecte, le traitement et l'utilisation commerciale des données sont souvent considérés comme des problématiques relevant plus de la protection des données que du droit de la concurrence. Des cas récents témoignent cependant du fait que les autorités de concurrence ont commencé à envisager la possession et l'utilisation des données du point de vue de la concurrence, même si, en fin de compte, aucune préoccupation n'a été retenue dans les affaires concernées. Par exemple, dans l'affaire *Facebook/ Whatsapp*, la Commission européenne a autorisé l'opération de rapprochement, en considérant que les données additionnelles auxquelles l'opération donne accès à Facebook laisseront subsister sur le marché un grand nombre de données utilisateurs qui ne seront pas soumises au contrôle exclusif de Facebook. Sur ce point voir Comm. UE, déc. 3 oct. 2014, aff. COMP/M.7217, pt 189. Voy. par ex. Commission européenne, « Google/Doubleclick », COMP/M. 4731,en date du 11.03.2008, www.ec.europa.eu/competition/mergers/cases/decisions/m4731_20080311_20682_de.pdf, §§ 359- 366; Commission européenne « Facebook/Whatsapp », COMP/M. 7217,en date du 03.10.2014, www.ec.europa.eu/competition/mergers/cases/decisions/m7217_20141003_20310_3962132_EN.p df, §§ 180-189.
Pour aller plus loin sur le lien entre l'exploitation des données personnelles et droit de la concurrence Voy. http://www.autoritedelaconcurrence.fr/doc/rapport-concurrence-donnees-vf-mai2016.pdf. Au contraire, certaines décisions ont envisagé un risque pour la concurrence. Par exemple, dans l'affaire *Thomson corporation/Reuters Group*, la Commission européenne a conditionné son autorisation de l'opération de fusion au respect d'une série d'engagements pris par les parties, dont celui de « vendre » une copie d'une partie de leur base de données aux concurrents qui en feraient demande, en raison du fait que les données issues des bases détenues par Thomson et reuters étaient considérées comme substituables en terme de qualité et de contenu, et n'avaient pas d'équivalent sur le marché, parmi les bases exploitées par leurs concurrents. Voy. Comm. CE, 19 février 2008, aff. M. 4726. Par ailleurs, dans une décision rendue le 17 septembre 2007, le Tribunal de première instance de l'Union européenne a confirmé la décision de la Commission européenne qui avait condamné la société Microsoft au paiement d'une amende de 497 millions d'euros, pour abus de position dominante, en ayant refusé à la société Sun Micrososystem la communication de spécifications techniques relatives à son système d'exploitation Windows, pour lui permettre l'interopérabilité de ses propres systèmes d'exploitation avec le système d'exploitation Windows. Voy. TPIUE, 17 septembre 2007, aff. C-201/04, Microsoft.

244 M. BOURGEOIS, *Droit de la donnée, principes théoriques et approche pratique*, Lexis Nexis, 2017, p. 10.

245 M.-C. PONTHOREAU, *La directive 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, *RFDA*, 1997, p. 125 et s.

la directive 2006/24/ CE sur la conservation des données[247] et le Règlement nº 45/2001[248] sur le traitement des données à caractère personnel par les institutions et organes communautaires. À ce cadre juridique de droit secondaire est venu s'ajouter une protection spécifique de rang primaire[249]. L'étude de ces instruments législatifs révèle que d'une part, les données à caractère personnel peuvent être considérées comme une « marchandise », élément indispensable au développement du marché intérieur [250] dans son volet numérique, et d'autre part, qu'elles peuvent être appréhendées sous l'angle d'un droit fondamental[251] garanti par le droit primaire de l'Union européenne et mis en œuvre par le droit dérivé. Ce qui explique l'existence d'une pyramide de textes ou un « renvoi en cascade »[252]. Une fois assurée la protection des données personnelles dans le cadre du marché intérieur[253], les préoccupations sécuritaires suite aux attaques du 11 septembre 2001 et à celles de Madrid et Londres, ont conduit l'Union européenne à attacher une attention particulière à la lutte contre le terrorisme et les formes graves de criminalité transfrontière dans « l'objectif fondamental »[254] d'offrir aux citoyens un espace de liberté, de sécurité et de justice. Ainsi les nouvelles technologies de l'information et de la communication ont permis des modes opératoires d'investigation particulièrement intrusifs et inédits. C'est pourquoi a été élaboré un cadre juridique spécifique dans le cadre de l'ex-troisième pilier car la directive 95/46/CE à l'égard de la protection des données personnelles s'appliquait aux seuls domaines de l'ex-premier pilier. Ce morcellement législatif a rendu souvent difficile la distinction de la frontière entre les « piliers » de l'Union européenne et cela a été source de contentieux[255]. La donnée peut être également appréhendée sous l'angle

246 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques). Ladite directive fait aujourd'hui l'objet d'une importante réforme.

247 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

248 Règlement (CE) n° 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données

249 Voy. l'article 8 de la Charte des droits fondamentaux.

250 Voy. G. RESTA, *Dignita, persone, mercati*, Torino, 2014, p. 153 ; *Libera circolazione e protezione dei dati personali,* t. I e II, a cura di R. PANETTA, con prefazione di S. RODOTÀ, Milano, Passim, 2006.

251 Sur la consécration d'une culture du droit fondamental à la protection des données personnelles distincte du droit à la vie privée voy.: G. FINOCCHIARO, « Alcune riflessioni sulle norme sul trattamento dei dati personali », in *Contr. e impr*., 2006, p. 1426 ss ; S. RODOTA, *Tecnologie e diritti*, Bologna, Passim, 1995.

252 O. DE SHUTTER, *Traité établissant une Constitution pour l'Europe, Commentaire article par article*, II –L. Burgorgue-Larsen, A. Levade, F. Picod (dir.), Bruylant, 2005, p. 124.

253 La directive 95/46/CE s'applique aux seuls traitements qui relèvent du champ d'application du droit communautaire de l'Union européenne et exclut donc les traitements rélatifs aux titres V et VI du Traité sur l'Union européenne (ex-troisième pilier) et en tout état de cause, les traitements ayant pour objet la défense nationale, la sécurité publique, le droit pénale de même que l'exercice d'activités exclusivement personnelles ou domestiques (art. 3§2).

254 J. MONAR, « The Area of Freedom, Security and Justice », *in* A.VONBOGDANDYand J.BAST (dir.), *Principles of European Constitutional Law*, Hart/C.H. Beck & Nomos, 2009, pp. 551-585, sp. p. 554 et s.

255 Voy. Les recours en annulation de la Cour de justice, 30 mai 2006, aff. jointes C-317/04 et C-318/04, Parlement c. Conseil, qui a annulé la décision du Conseil 2004/496/CE du 17 mai 2004 relative à la conclusion d'un accord entre l'UE et les États-Unis concernant le traitement et le transfert de données PNR, et la décision 2004/535/CE de la Commission du 14 mai 2004

de sa nature politique, elle constitue alors une information nécessaire pour l'autorité publique pour lutter contre le terrorisme et les formes graves de criminalité. Toutefois, cette information, pour être traitée par les autorités publiques, doit respecter un certain nombre de garanties. C'est en fonction de cette préoccupation que la décision-cadre 2008/977/JAI du 27 novembre 2008 a été adoptée[256] afin de garantir un équilibre entre l'élaboration des fichiers et des systèmes d'enregistrement des individus et les droits et libertés fondamentales[257] . Il est possible de constater une protection hétérogène, dérivant de plusieurs sources, qui s'inscrit dans l'ancienne architecture en piliers [258] . Toutefois, l'article 16 du Traité de Lisbonne consacre dans son paragraphe 2 la compétence du législateur communautaire pour l'adoption de règles en matière de protection des données personnelles dans toutes les matières, même pour la coopération judiciaire en matière pénale et la coopération policière[259]. Or, l'évolution technologique est un défi pour la législation en matière de protection des données et une réforme du cadre général[260] a été nécessaire afin d'apporter des réponses et une cohérence au système[261]. Cependant, ladite reforme laisse deux instruments juridiques différents pour le marché intérieur et pour l'ex-troisième pilier. La *summa divisio* entre marché intérieur et ELSJ laisse des éléments hétérogènes et pose des problèmes quant à l'efficacité de la protection[262]. Le propos du présent

relative au niveau de protection « adéquat » des données PNR transférées vers le *United States Bureau of Customs and Border Protection* ; Voy. aussi CJUE (Grande Chambre), 10 février 2009, aff. C-301/06, *Irlande c.Parlement et Conseil*, qui a rejeté le recours en annulation de la directive 2006/24/CE du 15 mars 2006 concernant la collecte de données générales des communications éléctroniques.

256 Décision-cadre 2008/977/JAI, 27 nov. 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale : JOCE n° L 350, 30 déc. 2008, p. 60 à 71.

257 Ladite décision-cadre visait donc à protéger les données personnelles traitées dans le cadre de la coopération policière et judiciaire en matière pénale dans le domaine de l'ex-troisième pilier.

258 Depuis le Traité de Maastricht l'Union européenne repose sur trois piliers : les communautés européennes (1er pilier), la politique étrangère et de sécurité commune (2e pilier) et la coopération policière et judiciaire en matière pénale (3e pilier), cette structure a été abolie avec le Traité de Lisbonne.

259 Par conséquent, la révision de la directive n° 95/46 CE à travers l'élaboration du règlement 679/2016 relatif à la protection des données personnelles tout comme la nouvelle directive 680/2016 en matière de coopération judiciaire et policière en matière pénale constitue un acte législatif examiné à travers la procédure de codécision.

260 La réforme de la protection des données est un ensemble de mesures législatives que la Commission a proposé en 2012 pour actualiser et moderniser les règles contenues dans la directive de 1995 sur la protection des données et dans la décision-cadre de 2008 relative à la protection des données traitées dans le cadre de la coopération policière et judiciaire en matière pénale. La réforme se compose d'un règlement général sur la protection des données et d'une directive relative à la protection des données à caractère personnel traitées à des fins de répression. Voy. Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données COM(2012) 10 final - 2012/0010 (COD). La révision de la décision cadre n° 2008/977 JAI à travers l'adoption d'une directive relative à la protection des données personnelles en matière de justice et de police constitue un acte législatif examiné à travers la procédure de codécision.

261 Même si les données sont soumises à la même base juridique par le traité de Lisbonne (article 16 TFUE), elles continuent à faire l'objet de différents instruments de droit dérivé lorsqu'il s'agit des domaines qui renvoient à l'ex-premier pilier ou à l'ex-troisième pilier. Voy. en ce sens B. CORTESE, « La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona », in *Il Diritto dell'Unione europea*, 2013, 313 ss.

262 Dans son arrêt du 30 mai 2006, la Cour de justice a annulé la décision de la Commission constatant le niveau de protection adéquate des données PNR tranférées vers les États-Unis et la décision du Conseil approuvant la conclusion d'un accord sur leur transfert vers ce pays, estimant que ces décisions n'étaient pas fondées sur une base juridique adéquate. La question posée par la Cour portait sur l'impact de la distinction entre les piliers de l'action de l'Union européenne sur la protection des données à caractère personnel. Dans son arrêt, la Cour de justice a réaffirmé le principe selon lequel c'est bien la finalité du traitement

Titre est d'étudier si la directive 95/46 soumise au premier pilier (Chapitre I) et ensuite la décision-cadre 2008/977/JAI soumise au troisième pilier (Chapitre II) ont progressivement établi une ligne de partage qui a permis à la réforme d'aboutir.

des données qui détermine le pilier auquel celui-ci est rattaché. Suite à cet arrêt le Contrôleur européen de la protection des données a exprimé la nécessité d'adopter un instrument spécifique dans le cadre du troisième pilier (en 2008 la décision-cadre sera adoptée). En revanche, le groupe de l'article 29 estime que l'arrêt de la Cour montre une fois de plus les difficultés dues à la division artificielle entre piliers et la nécessité d'un cadre transpiliers cohérent en matière de protection des données (Voy. WP29, avis 5/2006).

CHAPITRE I. LE RÉGIME DE PROTECTION DANS LE MARCHÉ INTÉRIEUR

32 La protection offerte dans l'ex-premier pilier. L'intégration économique et sociale résultant du fonctionnement du marché intérieur a conduit à une augmentation des flux transfrontaliers de données à caractère personnel. Les échanges de données à caractère personnel entre acteurs publics et privés, se sont intensifiés dans l'ensemble de l'Union européenne. Ainsi la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données a été adoptée sur le fondement de l'article 100 A § 1 du Traité de l'Union européenne selon lequel les mesures relatives au rapprochement des dispositions législatives, réglementaires et administratives des États membres ayant pour objet l'établissement et le fonctionnement du marché intérieur relèvent de la procédure de codécision. Il semble alors que, dans un premier temps, ce n'est donc pas l'exigence de la protection des droits fondamentaux en soi qui a amené à l'élaboration de la directive mais l'établissement et le bon fonctionnement du marché intérieur. La transposition de la directive 95/46 au sein des États membres ne s'est pas faite de manière uniforme. Cependant, les acteurs publics et privés ont besoin de règles claires. De plus, le droit à la protection des données personnelles est entré dans une nouvelle phase. Ce défi de concilier achèvement du marché intérieur et protection des données personnelles, a fait l'objet d'une reforme aboutissant à l'adoption du nouveau règlement 679/2016 établissant un cadre juridique uniforme applicable à l'ensemble de l'Union européenne. Ce nouveau cadre juridique est plus cohérent et renforce les droits des individus. Toutefois, le droit à la protection des données personnelles comprend toujours des intérêts opposés tant qu'une unification dans une seule catégorie (droit fondamental de l'individu et libre circulation des données) ne semble pas possible[263]. La construction et la nature du droit à la protection des données personnelles comme droit fondamental nous porte à nous interroger sur l'efficacité du régime juridique qui a été élaboré (Section I) et qui a porté à la réforme en laissant présager une protection des droits fondamentaux encore perfectible (Section II).

263 G. FINOCCHIARO, *Introduzione al Regolamento europeo sulla protezione dei dati*, Zanichelli, 2017, p. 10 ss ; M. BOCCHIOLA, *Privacy. Filosofia e politica di un concetto inesistente*, Roma, Passim, 2014, p. 13 et ss. Ainsi le Règlement 679/16 dispose dans son art. 1.3 que « la libre circulation des données à caractère personnel au sein de l'Union n'est ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

Section I. Les sources du droit à la protection des données personnelles, expression législative hétérogène

33 Les textes. Le texte fondateur en matière de protection des données personnelles au sein de l'Union européenne est la directive 95/46/CE du 24 octobre 1995[264]. Elle est le fruit de l'acquis européen en matière de protection des données à caractère personnel, et s'inspire de l'art. 8 CEDH et de la Convention n°108[265].

Toutefois, depuis le traité de Lisbonne, la protection des données à caractère personnel est un droit fondamental au regard de la législation de l'Union européenne[266]. En d'autres termes, l'Union dispose désormais d'une base juridique spécifique qui lui permet d'adopter des textes législatifs pour assurer la protection de ce droit fondamental. Ainsi, d'autres instruments ont complété le cadre juridique dans plusieurs domaines : la directive 2009/136 du 25 novembre 2009, ayant elle-même modifié la directive 2002/58 du 12 juillet 2002 sur le traitement des données dans le réseau de télécommunication, modifiée par la directive 2006/46/CE sur la conservation des données générées ou traitées dans le cadre de la fourniture de services de communications électroniques et annulée par l'arrêt *Digital Rights* du 2014, ainsi que le règlement 45/2001/CE[267]. L'idée du législateur était d'harmoniser les régimes de traitement des données à caractère personnel des différents États membres afin de faciliter les échanges de données dans l'Union européenne et améliorer la construction du marché intérieur (§1). La protection offerte par la directive 95/46/CE[268] est complétée par un cadre législatif spécifique :

---

264 Directive 95/46/CE du Parlement et du Conseil, 24 oct. 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données : JOCE n° L 281, 23 nov. 1995, p. 31 à 50.

265 Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel n°108. Elle est considérée comme la deuxième génération de réglementation concernant l'importation des valeurs du Conseil de l'Europe à l'environnement en ligne.

266 Contrairement à d'autres droits fondamentaux de la Charte, la protection des données est inscrite à l'article 16 TFU et donne au législateur une compétence concourante avec les États, pour l'adoption, selon la procédure ordinaire, des règles relatives à la protection des personnes physiques à l'égard du traitement des données personnelles, ainsi qu'à la libre circulation libre de telles données. En autres termes, cette protection n'est pas laissée à la seule action négative de la Cour de justice mais également à l'action positive du législateur de l'UE. Sur la portée de la Charte des droits fondamentaux après le Traité de lisbonne voy. : G. DI FEDERICO (ed.), *The EU Charter of Fundamental Rights, From Declaration to Binding Instrument*, Dordrecht, 2011, p. 162; S.I. SÁNCHEZ, *The Court and the Charter: The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights*, in Common Market Law Review, 2012, p.1564 ss.; K. LENAERTS, *The Court's Outer and Inner Selves: Exploring the External and Internal Legitimacy of the European Court of Justice*, in M. ADAMS, H. DE WAELE, J. MEEUSEN, G. STRAETMANS, *Judging Europe's Judges. The Legitimacy of the Case Law of the European Court of Justice*, Oxford- Portland, 2013, p.13 ss.

267 Règlement du Parlement et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

268 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

on y trouve le règlement 45/2001/CE[269], la directive 2002/58/CE[270] sur les communications électroniques et la directive 2006/24 sur la conservation des données (§2).

§1. La directive 95/46 comme instrument pour la réalisation du marché intérieur

34 Une harmonisation instrumentale à la réalisation du marché intérieur. La directive 95/46/CE constitue le texte fondateur de droit dérivé en matière de protection de données personnelles[271], son objectif principal était d'assurer une protection équivalente de haut niveau dans tous les États membres de la Communauté afin d'éliminer les obstacles aux échanges de données nécessaires au fonctionnement du marché intérieur[272]. Ainsi dans un premier temps, les données personnelles étaient considérées comme une marchandise indispensable au développement de l'économie numérique[273]. Par conséquent, dans cette phase, la protection des données a été instrumentalisée afin de réaliser le marché intérieur et ne pas fausser la concurrence[274] . Toutefois, dès le debout la Cour de justice a interprété la directive 95/46, estimant l'absence de nécessité d'un élément transfrontalier et de lien avec la libre circulation. Ainsi dans l'affaire *Österreichischer Rundfunk*[275], la Cour de justice a jugé qu'il n'était pas nécessaire de démontrer un lien effectif entre la libre circulation et le traitement en cause pour que la directive 95/46/CE s'applique. En effet, tout traitement est susceptible de circuler entre les États membres de l'Union[276]. De surcroît, l'obligation de démontrer systématiquement un tel lien effectif serait nuisible à la sécurité juridique ainsi qu'à l'effet utile de la directive[277]. Ici la Cour analyse de façon détaillée le texte de la directive et démontre que l'intention du législateur communautaire était bien que la directive s'applique nonobstant l'absence éventuelle de lien direct avec la libre circulation.
La Cour de justice confirme ce principe dans l'affaire *Lindqvist*. Ici elle rappelle que la directive 95/46, bien que fondée sur l'article 100 A du Traité, « ne présuppose pas l'existence d'un lien

269 Règlement du Parlement et du Conseil, du 18 décembre 2000, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

270 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

271 Elle a été adoptée sur la base de l'art. 100 TCE, actuel art. 95 TUE.

272 Voy. le Considérant 8 directive 95/46 et le Premier rapport de la Commission sur la mise en œuvre de la directive relative à la protection des données, COM (2003)265 final, 15 mai 2003.

273 M. ALINCAI, *Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel*, Revue de l'Union européenne n° 576, mars 2014, p. 172.

274 Voy. le considérant 7 de l'exposé de motifs de la directive 95/46.

275 CJCE, Österreichischer Rundfunk, Aff. C-465/00, C-138/01 et C-139/01, 20 mai 2003.

276 CJCE, Österreichischer Rundfunk, Aff. C-465/00, C-138/01 et C-139/01, 20 mai 2003, § 40.

277 CJCE, Österreichischer Rundfunk, Aff. C-465/00, C-138/01 et C-139/01, 20 mai 2003, § 42.

effectif avec la libre circulation entre États membres dans chacune des situations visées par l'acte fondé sur une telle base »[278]. C'est seulement dans un second temps que la directive est perçue comme un instrument de protection du droit fondamental à la protection des données personnelles. Ainsi comme l'a souligné l'Avocat général Tizzano dans l'affaire *Lindqvist* : « le législateur communautaire a considéré que pour déterminer un niveau de protection équivalent dans tous les États membres, il fallait tenir compte de la nécessité de sauvegarder les droits fondamentaux des personnes »[279]. Concernant la mise en œuvre de la directive, la Cour de justice dans l'affaire *Österreichischer Rundfunk* a déclaré la directive 95/46 d'application directe puisque ses dispositions sont suffisamment claires, précises et inconditionnelles pour être invoquées par un particulier et appliquées par les juridictions nationales à défaut de mesures d'application prises dans les délais ou à l'encontre de toute disposition nationale non conforme à la directive[280]. La Cour de justice a eu l'occasion de rappeler que la directive 95/46 était une directive d'harmonisation complète [281] . De surcroît, un État membre ne peut prévoir de dispositions divergentes que dans les domaines où la directive prévoit explicitement une telle marge de manœuvre et pour autant qu'aucune autre disposition du droit communautaire n'y fasse obstacle[282]. Ainsi la Cour de justice a jugé qu'un État membre ne peut pas prévoir des dispositions plus strictes que la directive en raison du degré d'harmonisation complète de celle-ci : dans l'affaire *Asnef et Fecedem contre Espagne* [283] , la législation espagnole prévoyait l'obligation pour les traitements fondés sur l'article 7 sous f) de la directive (portant sur la notion d'intérêt légitime du responsable de traitement) de ne porter que sur des données provenant de sources librement disponibles au public[284]. Ainsi la Cour de justice à travers sa jurisprudence a précisé l'objet de la protection offerte par la directive 95/46 (A) et son champ d'application (B).

A. L'objet de la protection

35 L'interprétation de la Cour de justice. La jurisprudence de la Cour de justice a précisé que l'objet de la directive 95/46 est la liberté accordée à l'individu de décider si et dans quelle mesure rendre ses propres renseignements disponibles et dans le pouvoir d'en contrôler leur

278 CJCE, Lindqvist Aff. C-101/01, 6 novembre 2003, § 40.

279 Voy. Conclusions de l'Avocat général M. A. TIZZANO du 19 septembre 2002 dans l'affaire Bodil Lindqvist C-101/01,§ 7.

280 CJCE, Rechnungsshof et a. c. Österreichischer Rundfunk, aff. Jointes C-465/00, C-138/01, C-139/01, 20 mai 2003 point 101, « Il convient donc de répondre à la seconde question que les articles 6, paragraphe 1, sous c), et 7, sous c) et e), de la directive 95/46 sont directement applicables, en ce sens qu'ils peuvent être invoqués par un particulier devant les juridictions nationales pour écarter l'application des règles de droit interne contraires à ces dispositions ». Cependant cette liste n'est pas limitative.

281 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10, pt. 29 et CJUE 19 octobre 2016 « Breyer contre Allemagne » Aff. C-582/14, pt. 58.

282 CJCE « Lindqvist » Aff. C-101/01, 6 novembre 2003 § 96 et § 99.

283 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10.

284 CJUE 24 novembre 2011 « ASNEF et FECEMD contre Administracion del Estado » Aff. C-468/10 et C-469/10.

circulation[285], sans que cela se traduise par une sorte de droit absolu[286]. D'ailleurs, la Cour de justice a adopté une interprétation large de la notion de donnée personnelle employée à l'article 3, paragraphe 1, de la directive 95/46 : elle englobe, conformément à la définition figurant à l'article 2, sous a) de celle-ci, « toute information concernant une personne physique identifiée ou identifiable »[287]. Des exemples de cette interprétation extrêmement large sont l'adresse IP[288] – considérée comme une donnée personnelle –, les images d'un dispositif de vidéosurveillance[289] ou encore les métadonnées de communication[290]. Toutefois, le législateur a exclu du champ d'application les traitements «effectués par une personne physique pour l'exercice d'activités exclusivement "personnelles ou domestiques" »[291] et les traitement qui correspondent aux activités prévues au titre V du Traité sur l'Union européenne (politique étrangère et de sécurité commune) et à la coopération judiciaire et policière, ou les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités relatives au droit pénal. Toutefois lesdites exceptions ne couvrent pas la totalité des traitements de données personnelles dont le responsable de traitement est un État ou une autre personne morale de droit public national[292]. D'ailleurs, dans l'arrêt *Huber contre Allemagne*[293], la Cour de justice a rappelé que si les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et le droit pénal sont exclus du champ d'application de la directive, ceci n'est pas le cas pour les données collectées et traitées dans le cadre de la règlementation sur le droit de séjour[294]. Afin de souligner que la directive ne s'applique pas uniquement aux traitements effectués à des fins commerciales et économiques, la Cour de justice a inclus le traitement des données dans le cadre d'une activité associative, religieuse et sans but lucratif dans le champ d'application de la directive[295]. Selon l'article 3.1 de la directive 95/46/CE : « La présente directive s'applique au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer

---

285 S. RODOTA, *Tecnologie e diritti*, Bologna, 1995, p. 102.

286 CJUE, affaires jointes C-92/09 e C-93/09, Volker und Markus Schecke e Eifert, 9 novembre 2010, point 48, Voy sur ce point l'affaire, C-543/09, du 5 mai 201, §50 ayant pour objet un renvoi préjudiciel proposé par le Bundesverwaltungsgericht, selon la CJ »le droit à la protection des données personnelles n'apparaît pas comme une prérogative absolue, mais il va considérer à la lumière de sa fonction sociale".

287 CJCE « Lindqvist » Aff. C-101/01, 6 novembre 2003, § 24.

288 CJUE 24 novembre 2011 « Scarlet contre SABAM » Aff. C-70/10, § 5. Ainsi une adresse IP (Internet Protocol) correspond au numéro identifiant une interface technique (ordinateur, router, imprimante) connectée avec le réseau Internet. Une adresse ip peut être fixe (elle sera toujours la même lorsqu'un terminal se connecte à Internet) ou dynamique (l'utilisateur se verra attribuer une nouvelles adresse IP à chaque connexion par son fournisseur d'accès à Internet. Cette définition a été reprise par la Cour de justice dans son arrêt du 19 octobre 2016, aff. C-582/14 §36.

289 CJUE, Frantisek Rynes, Aff. C-212/13, 11 décembre 2013, § 21.

290 CJUE, Tele2 Sverige Aff. C-203/15 et C-698/15, 21 décembre 2016, § 97 et 100.

291 Voy. Article 3 paragraphe 2 de la directive 95/46.

292 D'ailleurs, les institutions de l'Union sont soumises au règlement 45/2001/CE.

293 CJCE, Huber contre Allemagne, Aff. C-524/06, 16 décembre 2008.

294 CJCE 16 décembre 2008 « Huber contre Allemagne » Aff. C-524/06, § 44 et § 45.

295 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, § 39.

dans un fichier ». La Cour de justice s'est prononcée sur ce qui constitue ou non un traitement automatisé dans l'affaire *Lindqvist* [296] . Ici la Cour a répondu sans ambiguïté que dès lors qu'Internet est utilisé pour faire apparaître ces données, il s'agit d'un traitement automatisé. Toutefois, elle ne dégage pas de critères généraux permettant de définir plus précisément la frontière entre un traitement automatisé en tout ou partie et un traitement non-automatisé, et il n'est donc pas, à ce stade, possible de conclure au fait que le simple emploi d'un appareillage informatique suffise à faire qualifier un traitement d'automatisé en tout ou partie. Le champ d'application est très large puisque la directive s'applique au traitement de données personnelles, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelés à figurer dans un fichier. Cette protection est limitée aux affaires du marché intérieur, elle s'applique aux seuls traitements qui relèvent du champ de d'application du droit communautaire de l'Union européenne et exclut donc les traitements relatifs aux titres V et VI du Traité sur l'Union européenne (ex-troisième pilier, ainsi la protection des données en matière de coopération dans le domaine de la police et de la justice pénale ne relève pas de son champ d'application) et en tout état de cause, les traitements ayant pour objet la défense nationale, sécurité publique, droit pénale, etc., de même que l'exercice d'activités exclusivement personnelles ou domestiques (art. 3§2). A ce titre, la Cour de justice dans sa jurisprudence[297], avait jugé qu'il ne serait pas approprié d'interpréter l'expression de l'article 3, §2 de la directive : « activités qui ne relèvent pas du champ d'application du droit communautaire » comme ayant une portée telle qu'il serait nécessaire de vérifier, au cas par cas, si l'activité spécifique en cause affecte directement la libre circulation entre États membres. Dans l'arrêt *Bodil Lindqvist*[298] elle avait ensuite précisé que l'opération consistant à faire référence sur une page Internet à diverses personnes, à les identifier soit par leur nom soit par d'autres moyens constitue un traitement de données de sorte que ce traitement ne rentre ni dans la catégorie d'activités ayant pour objectif la sécurité publique ni dans la catégorie d'activités exclusivement personnelles ou domestiques qui sont hors du champ d'application de la directive [299] . La Cour de justice a été appelée à se prononcer à nouveau sur le champ d'application matériel de la directive dans l'affaire PNR[300]. Ici, elle a estimé que la décision « d'adéquation » sur la base de l'article 25, 6 de la directive 95/46[301] ne pouvait pas entrer dans

---

296 CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, § 26 :« [...] il convient de relever que faire apparaître des informations sur une page Internet implique, selon les procédures techniques et informatiques appliquées actuellement, de réaliser une opération de chargement de cette page sur un serveur ainsi que les opérations nécessaires pour rendre cette page accessible aux personnes qui se sont connectées à Internet. Ces opérations sont effectuées, au moins en partie, de manière automatisée.

297 CJCE aff. C-465/00, C-138/01 ET C-139/01, Osterreichischer Rundfunk, §42, 20 mai 2003.

298 CJ aff. C-101/01, Bodil Lindqvist, 6 novembre 2003, §43.

299 Mme Lindqvist estimait que l'insertion des données des collègues de la paroisse se référant aux activités bénévoles et religieuses n'entraient pas dans le champ d'application de la directive.

300 CJCE, Parlement européen c. Conseil, aff. C-317/04 et C-318/04, 30 mai 2006, §44 et §56-60.

301 À la suite des attentats du 11 septembre 2001, les États-Unis ont contraint les transporteurs aériens à transmettre aux autorités publiques les données relatives aux passagers contenues dans les systèmes de réservation (PNR). La Commission a rendu ainsi une décision d'adéquation aux transferts sur la base de l'article 25§6 de la directive 95/46. Le conseil a alors procédé avec la décision 4004/496/CE à la conclusion d'un accord entre la Communauté européenne et les États-Unis. Le Parlement a alors demandé l'annulation de deux textes puisqu'il estimait qu'ils n'entraient pas dans le champ d'application de la directive.

le champ d'application de la directive étant donné que le transfert de données PNR « constitue un traitement ayant pour objectif la sécurité publique et les activités de l'État relatives à des domaines du droit pénal »[302]. Selon la Cour, le fait que les données PNR soient initialement collectées par la compagnie aérienne dans le cadre d'une activité qui relève du droit communautaire, comme la vente des billets d'avion, qui comporte une prestation de service, importe peu la finalité commerciale, c'est la finalité d'exercer des activités propres aux États qui est prise en compte ; ainsi la directive 95/46 n'est pas susceptible de s'appliquer à ce transfert. La Cour souligne que les activités mentionnées à titre d'exemple à l'article 3§2 de la directive sont des activités étatiques et que des traitements mis en œuvre par des opérateurs privées (comme les compagnies aériennes) peuvent s'insérer dans un cadre institué par les pouvoirs publics et visant la sécurité publique. Ainsi elle a annulé la « décision d'adéquation » ainsi que la décision 4004/496/ CE du Conseil du 17 mai 2004 dont le fondement juridique (art. 95 CE) avait pour but le bon fonctionnement du marché intérieur. Il en résulte que tous les transferts vers une autorité publique à des fins policières et judiciaires (Titre VI du Traité UE) sont exclus du champ d'application de la directive, tout comme les activités de sécurité commune relevant du Titre V du Traité. Cependant, la Cour de justice a rappelé en 2015 que l'article 13 de la directive 95/46/CE permet d'échapper à certaines des exigences de loyauté des traitements notamment pour des raisons liées à la sûreté de l'État, à la défense, ou la sécurité publique[303]. Toutefois, l'emploi de cette dérogation doit être prévu par la loi et ne saurait être fondé uniquement sur une convention non-publiée passée entre deux établissements publics[304]. La Cour s'est prononcée à nouveau sur ce critère de finalité du traitement dans l'affaire Huber[305], où le registre centralisé des étrangers vivant en Allemagne était mis en cause. La Cour a estimé que la première finalité de la législation en cause était la lutte contre la criminalité, ne rentrant pas dans le champ d'application de la directive en raison des exclusions prévues à l'art. 3.2 de la directive 95/46.
Par ailleurs, l'objet de la directive 95/46, c'est-à-dire ses principes (1), les droits des personnes concernées (2) et les organes de protection (3) ont été repris dans le RGPD. Leur analyse est nécessaire.

1) Les principes directeurs

La directive 95/46 incorpore et élargi les principes déjà contenus dans le Convention 108[306]. Cependant, la Cour de justice est intervenue sur l'interprétation des notions présentes dans la

302 CJCE aff. C-317/04 et C-318/04, 30 mai 2006, §52, ci-après arrêt PNR.

303 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, § 9.

304 CJUE 1er octobre 2015 « Smaranda Bara e.a. » Aff. C-201/14, § 40 et 41.

305 CJCE, Heinz Huber c. Allemagne, aff. C524/06, 16 décembre 2014, §44.

306 Voy. Pour des commentaires sur la directive, M-Cl. PONTHOREAU, *La directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, la société de l'information à l'épreuve des droits de l'homme*, RMCUE 1998, p. 537 et s.

directive, le contenu des principes énoncés (a), les acteurs du traitement (b) le contenu des droits octroyés à la personne (c) et sa mise en œuvre par les autorités de contrôle (d). Cette interprétation se révèle particulièrement importante car ces notions ont été reprises et parfois enrichies dans le nouveau règlement général sur la protection des données personnelles, leur analyse est donc indispensable.

a) L'interprétation de la base légale pour le traitement

36 Les conditions de fond et de forme. Le traitement[307] de données à caractère personnel est licite s'il répond à des conditions de fond et de forme. Ainsi un traitement doit trouver sa source dans une cause licite s'appuyant sur des finalités déterminées et légitimes et porter sur un objet proportionné étant nécessaire à la poursuite de la finalité[308]. La finalité doit être explicite et déterminée. Cela signifie qu'elle doit être décrite de manière claire et intelligible [309]. Cette condition est nécessaire pour garantir aux personnes concernées la transparence sur le traitement mis en œuvre, la prévisibilité et le contrôle sur leurs données[310]. L'article 7 de la directive 95/46 fixe les conditions de légitimité des traitements de données. Ce critère a été reprise à l'art. 6 du RGPD. Ainsi, un traitement de données à caractère personnel n'est licite que sur l'un des fondements suivants: s'il est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ; au respect d'une obligation légale à laquelle le responsable du traitement est soumis, à l'exécution d'un contrat auquel la personne concernée est partie ; le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel ; le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; ou lorsque la personne concernée a donné son consentement[311].

37 Notion de consentement. A la différence des autres fondements légaux, le traitement s'appuie ici sur la volonté de la personne concernée. Pour être valable le consentement doit être univoque[312], libre, spécifique et éclairé. La Cour de justice a eu l'occasion de se prononcer sur

307 La directive définit : «traitement de données à caractère personnel» toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

308 Voy. l'avis du G29 sur la notion de finalité du 9 avril 2014 p.26.

309 Voit l'art. 5.1 b) du RGPD.

310 Voy. l'avis du G29 n° 03/2013 du 2 avril 2013 p.13-16.

311 Voy. art. 6 du RGPD.

la notion de consentement prévu par la directive 95/46[313]. Dans l'affaire *Volker et Markus Schecke*[314], elle a estimé que le consentement ne peut être constitué par la simple signature d'un formulaire mentionnant l'existence d'un traitement mais celui-ci doit être spécifique et décrire les finalités du traitement. Ainsi la Cour de justice a confirmé cette interprétation de l'article 7 de la directive 95/46 dans l'affaire *Michael Shwarts* et elle a déclaré que la demande d'un passeport, alors même que celui-ci est indispensable aux citoyens de l'UE pour voyager, ne manifeste pas le consentement de la personne susceptible de légitimer le traitement [315]. La directive 95/46 ne prévoyait pas explicitement la possibilité pour la personne concernée de retirer son consentement. L'art. 7.3 du RGPD a prévu cette possibilité, il résulte que les opérations de traitement réalisées postérieurement au retrait du consentement devront cesser à moins que le responsable ne puisse appuyer son traitement sur un autre fondement juridique. L'article 6 de la directive 95/46 fixe les conditions de « qualité des donnés », selon lequel le responsable de traitement doit veiller à traiter les données de manière loyale et licite[316]. Cette condition est reprise par l'art.5 du RGPD. Cela implique que les personnes concernées aient reçu une information préalable assurant les règles appliquées (principe de transparence), les finalités de l'utilisation des données (principe de finalité) et que les données soient traitées et collectées pour des finalités déterminées, explicites et légitimes ; elles doivent être exactes et si nécessaire mises à jour. Ainsi la Cour de justice a précisé dans l'affaire *Bara*[317], que l'obligation d'information concerne même les administrations publiques qui sont tenues d'informer les individus du transfert de leurs données personnelles vers une autre administration et du traitement dont elles feront l'objet entre les mains du destinataire. Dans l'affaire *Rotterdam contre Rijkeboer*[318], la Cour de justice a affirmé que : « le droit au respect de la vie privée implique que la personne concernée puisse s'assurer que ses données à caractère personnel sont traitées de manière exacte et licite, c'est-à-dire, en particulier, que les données de base la concernant sont exactes et qu'elles sont adressées à des destinataires autorisés. Ainsi qu'il est énoncé au quarante-et-unième considérant de la directive, afin de pouvoir effectuer les vérifications nécessaires, la personne concernée doit disposer d'un droit d'accès aux données la concernant qui font l'objet d'un traitement »[319]. Des dérogations aux conditions générales de licéité des traitements de données sont prévues également dans les domaines artistique et journalistique. Ainsi l'article 9 de la directive prévoit des règles spécifiques et cela en raison

312 Voy. le considérant 32 du RGPD. « Il ne saurait y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité ».

313 Selon l'article 7 a) le traitement peut être effectué si la personne a indubitablement donné son consentement.

314 CJ, Volker et Markus Schecke GbR et Hartmut Eifert c. Land Hessen, 9 novembre 2010, aff. Jointes C-92/09 et C-93/09, §63.

315 CJUE, Michael Shwartsc. Stadt Bochum, aff. C-291/12, 17 octobre 2013, §32.

316 La Cour de justice a eu l'occasion de confirmer que les dispositions de la directive garantissant le traitement loyal et licite des données personnelles(art. 6 et 7) pouvaient etre invoquées par un particulier devant les juridictions nationales pour écarter l'application des règles de droit interne contraires à ces dispositions, aff. Osterreichischer Rundfunk et autres, 20 mai2003.

317 CJUE, Bara, aff. C 201/14, 1 octobre 2015.

318 CJCE 7 mai 2009 « College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer » Aff. C-553/07.

319 CJCE 7 mai 2009 « College van burgemeester en wethouders van Rotterdam v M. E. E. Rijkeboer » Aff. C-553/07 §49.

du rapport entre la protection des données personnelles et la liberté d'expression. Plus récemment, la Cour de justice a précisé la portée de l'exception de l'activité de journalisme dans la diffusion de données à caractère personnel[320]. Dans l'affaire *Satamedia* la Cour de justice relève que les exemptions de l'article 9 s'appliquent aux entreprises de média, mais également à toute personne exerçant une activité de journalisme, le fait qu'une publication de données soit liée à une finalité lucrative n'exclut pas qu'elle puisse entrer dans le champ d'application de l'article 9.

38 Règles spéciales applicables à certains traitements. La directive 95/46 prévoyait dans son article 8, des règles spécifiques qui s'appliquaient au traitement des données sensibles (à savoir celles relevant de l'origine raciale, ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, les données relatives à la santé[321], la vie sexuelle et les sanctions pénales). Le règlement 679/16 a ajouté à cette liste les données biométriques[322] et génétiques[323].

39 Le traitement relatif aux flux transfrontaliers des données. Certains types de traitement sont encadrés par des règles particulières. Le législateur, conscient que les flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international, a pris soin d'envisager la relation entre l'Union et les États tiers[324]. Le principe est que les données à caractère personnel peuvent être transférées uniquement vers des pays tiers qui garantissent un niveau de protection « adéquat »[325], à défaut le transfert n'est autorisé que dans certaines circonstances [326]. En vertu de l'article 25§6, la Commission européenne peut

320 CJCE, aff. C-73/07, Satamedia, 16 décembre 2008.

321 La Cour de justice dans l'affaire *Lindqvist* déclare qu'il convient d'adopter une interprétation large de données relatives à la santé de sorte qu'elle comprenne tous les aspects tant physiques que psychique de la santé d'une personne.

322 Le RGPD définit les données biométriques, comme « les données à caractère personnel résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, qui permettent ou confirment son identification unique, telles que des images faciales ou des données dactyloscopiques. Voy. l'art. 4§14 du RGPD.Voy. en ce sens N.GRAHAM, « Top 10 tips for processing biometric data », *Privacy Laws & Business International Report*, n° 141, juin 2016, p. 12 et 13.

323 Le RGPD définit les données génétiques comme « les données à caractère personnel relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, notamment, d'une analyse d'un échantillon biologique de la personne physique en question ». Voy. l'art. 4 §13 du RGPD.

324 Directive 95/46/CE, consid. 56.

325 Directive 95/46/CE, art 25 §1. Ni l'article 25, paragraphe 2, de la directive 95/46 ni aucune autre disposition de celle-ci ne contiennent de définition de la notion de niveau de protection "adéquat". En particulier, l'article 25, paragraphe 2, de ladite directive se borne à énoncer que le caractère adéquat du niveau de protection offert par un pays tiers « s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transfert de données» et énumère, de façon non exhaustive, les circonstances devant être prises en considération lors d'une telle appréciation. Toutefois, d'une part, ainsi qu'il ressort des termes mêmes de l'article 25, paragraphe 6, de la directive 95/46, cette disposition exige qu'un pays tiers « assure» un niveau de protection adéquat en raison de sa législation interne ou de ses engagements internationaux. D'autre part, également selon cette disposition, le caractère adéquat de la protection assurée par le pays tiers s'apprécie « en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes».

326 Les autres pays européens non membres de l'Union qui se sont dotés d'une législation assurant une protection suffisante des données personnelles sont l'Islande, le Liechtenstein, la Norvège, la Suisse, l'Andorre ainsi que les îles de Guernesey, Jersey, Man et Féroé. Au-delà de l'Europe, les flux de données personnelles sont libres vers le Canada, l'Argentine, l'Uruguay, la Nouvelle Zélande et l'Israël. Aux États-Unis, seules les entreprises qui ont volontairement adhérés d'abord au « EU-U.S.

constater que le niveau de protection dans un État tiers est adéquat et permettre le transfert de données. La Commission avait notamment reconnu que le système de transfert dit « *Safe Harbor »,* développé en coopération avec le ministère du Commerce des États-Unis, assurait un niveau de protection « adéquat »[327] et elle avait donc permis le transfert de données à caractère personnelles depuis l'Union vers les entreprises inscrites dans le programme *Safe Harbor* installées aux États-Unis. Toutefois, suite à une plainte d'un militant autrichien, M. Schrems, contre l'autorité irlandaise de protection des données refusant de remettre en cause l'accord *Safe Harbor,* la Haute Cour irlandaise a posé une question préjudicielle à la Cour de justice pour savoir si l'entrée en vigueur de la Charte des droits fondamentaux de l'Union européenne, et notamment son article 8, pouvait remettre en cause une « décision d'adéquation » de la Commission lorsqu'il est démontré que l'État tiers visé par la décision d'équivalence enfreint les principes défendus par le droit de l'Union en matière de protection des donnée. La CJUE a répondu par l'affirmative à la question et invalidé l'accord *Safe Harbor*.

b) Les acteurs du traitement

40 La qualification de responsable de traitement. Concernant les acteurs du traitement, l'art 2, d) de la directive définit le responsable du traitement comme une personne qui « seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement de données à caractère personnel ». Le RGPD est venu y ajouter la notion de responsable conjoint de traitement [328] . La qualification de responsable de traitement est centrale car il supporte la majeure partie des obligations légales[329]. Dans l'affaire *Google Spain*[330], la première question était de savoir si, par son activité d'exploitation et d'indexation de données sur Internet, le moteur de recherche Google peut être considéré comme un « responsable de traitement » au sens de la directive. Dans un avis 1/2008 le Groupe de travail article 29 (G29)[331] distinguait le rôle des moteurs de recherche lorsqu'ils agissent exclusivement en tant qu'intermédiaires (et

Safe Harbor » et à la suite de son invalidité au « *Privacy Shield Framework* » peuvent librement recevoir des données provenant de l'Union européenne. Par contre, le transfert de données personnelles vers les autres pays que ceux mentionnés ci-dessus, ou vers des entreprises américaines n'ayant pas adhéré au « *Privacy Shield Framework* », ne peut pas s'effectuer sans avoir recherché des garanties appropriées, soit par la signature de clauses contractuelles types ou de règles contraignantes d'entreprise.

327 Décision n° 2000/520/CE de la Commission du 26 juillet 2000.

328 Voy. l'art. 4§7 du RGPD: le responsable du traitement est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre ».

329 M.CLEMENT FONTAINE « La plasticité de la notion de responsable de traitement », *Revue des affaires européenne*, Bruylant 2018, p. 35 et s.

330 CJUE, *Google Spain*, aff. C 131/12, 13 mai 2014, § 41.

331 Voy. l'avis du Groupe de Travail article 29» sur la protection des données http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2008/wp148_fr.pdf

donc pas en tant que responsables de traitement), de leur rôle actif en tant que « fournisseurs de contenus » (et donc en tant que responsables de traitement). La Cour de justice n'a pas suivi cette distinction élaborée par le G29 et a considéré tout simplement que « l'activité d'un moteur de recherche consistant à trouver des informations publiées ou placées sur Internet par des tiers, à les indexer de manière automatique, à les stocker temporairement et, enfin, à les mettre à la disposition des internautes selon un ordre de préférence donné constitue un traitement de données personnelles », elle a estimé que Google Inc. devait être considéré comme « le responsable de traitement »[332] puisqu'il détermine les finalités et les moyens de cette activité. En l'espèce, l'objectif était de vendre sur le territoire espagnol des espaces publicitaires associés à des résultats de recherche. Un tel traitement se fonde sur la base légale de l'article 7 sous f) de la directive 95/46/CE, c'est-à-dire l'intérêt légitime du responsable de traitement[333]. Dans un avis de 2010[334], le G29 a estimé qu'il est préférable de considérer comme responsable de traitement la société ou l'organisme en tant que tel plutôt qu'une personne en son sein, sauf si la personne physique utilise les données à des fins personnelles en dehors du contrôle de la personne morale. L'autre critère retenu par le G29 dans son avis est celui du rôle décisionnel joué dans la définition des finalités et dans la définition des moyens. Selon ce même avis, la détermination des finalités l'emporte sur la mise en œuvre des moyens sauf si les moyens concernent des aspects essentiels, à savoir, les aspects qui touchent à la licéité du traitement (choix des données traitées, durée de conservation).

41 Le responsable conjoint de traitement. Le RGPD reprend la notion déjà existante dans la directive et consacre la notion de responsable conjoint [335] de traitement lorsque deux ou plusieurs responsables de traitement déterminent conjointement les finalités et les moyens du traitement. Ainsi le RGPD permet de répartir les rôles et les responsabilités des responsables conjoints dans le contrat qui les lie[336].

42 Le sous-traitant. Le sous-traitant est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement. Selon l'avis 1/2010 du G29[337], existent quatre critères factuels pour déterminer si on est en présence d'un sous-traitant : premièrement, le nombre d'instructions préalables données par le responsable du traitement, deuxièmement la surveillance exercée par

---

332 Voy. point 41de l'arrêt.

333 CJUE, Google contre Espagne, Aff. C-131/12, 13 mai 2014, § 73.

334 Voy. l'avis du G29 n°1/2010, 16 février 2010 p. 16.

335 Voy. La page d ela Commission européenne dediée, disponible à l'adresse: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/controller-processor/what-data-controller-or-data-processor_fr

336 Voy. une lecture combinée des art. 82.2 et 82.4 du RGPD. Il s'agirait d'une dérogation à la règle de solidarité.

337 L'avis 1/2010 du G29 est disponible à l'adresse : https://cnpd.public.lu/dam-assets/fr/publications/groupe-art29/wp169_fr.pdf

le responsable du traitement sur l'exécution de l'opération, troisièmement, la visibilité qu'il a vis-à-vis de la personne concernée et dernièrement l'expertise des parties. Si les finalités du traitement relèvent exclusivement de l'expertise propre au prestataire, la qualification de responsable du traitement sera préférée à celle de sous-traitant.

43 Les tiers. Le tiers, désigne une personne physique ou morale, une autorité publique, un service ou un organisme autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, placées sous l'autorité directe du responsable du traitement ou du sous• traitant, sont autorisées à traiter les données à caractère personnel. Dans son avis de 2010 le G29 indique que la notion de tiers doit être interprétée comme désignant tout sujet qui n'a aucune légitimité ni autorisation pour traiter les données personnelles. Pour illustrer la notion de tiers, le G29 prend l'exemple d'un employé d'une société qui, dans l'exercice de ses fonctions, prend connaissances des données auxquelles il n'a pas le droit d'accéder[338].

44 Les destinataires. Le destinataire désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement[339]. Le fait qu'il puisse s'agir d'un tiers, signifie qu'une personne ou un service peut être considéré comme un destinataire du traitement dès lors qu'elle est habilitée à recevoir communication de ces traitements. Toutefois la désignation du destinataire ne relève pas de la seule liberté des responsables de traitement, encore faut-il que ses missions soient en lien avec la finalité du traitement.

2) Les droits des personnes concernées par un traitement

45 L'exercice des droits. Toute personne dont les données font l'objet d'un traitement disposent d'un droit d'accès, de rectification, d'effacement ou d'opposition. La personne dont les données font l'objet d'un traitement et qui souhaite exercer ses droits doit en informer le responsable de traitement. Le RGPD a raccourci le délai pour répondre à une demande à un mois, même lorsque le responsable décide de ne pas y faire droit, il doit exposer ses motifs ainsi que la voie de recours pour contester sa décision auprès de l'autorité de contrôle nationale ou auprès d'une juridiction[340].

---

338 Voy. l'avis du G29 n°1/2010, 16 février 2010 p. 33.

339 Voy. l'art. 4§9 du RGPD.

340 Voy. l'art. 12.4 du RGPD.

46 Le droit d'accès. Le droit d'accès offre à la personne dont les données sont traitées la possibilité d'obtenir, sans contrainte et sans délai ou frais excessifs, la confirmation que les données sont traitées et par qui, les finalités du traitement et les destinataires de celles-ci ; la personne concernée a aussi le droit de demander l'effacement, le verrouillage des données et la notification de ces modifications aux tiers auxquels les données sont transmises. Ainsi les responsables de traitement doivent garantir un droit d'accès aux personnes concernées « sans contrainte, à des intervalles raisonnables et sans délais ou frais excessifs »[341]. Concernant le droit d'accès, la Cour de justice s'est prononcée sur les modalités d'exercice de ce droit ainsi que sur son contenu. Dans une affaire de 2013, la Cour de justice a précisé que « l'exercice du droit d'accès peut donner lieu à la perception de frais, mais que ceux-ci ne doivent pas être excessifs et donc ne doivent pas excéder le coût de la communication »[342]. À l'égard du contenu du droit d'accès, la Cour de justice a estimé qu'un accès à l'identité des personnes ayant demandé à accéder aux données ainsi qu'au contenu de l'information transmise doit être possible pendant tout le temps durant lequel les données sont conservées, dans le cas échéant, cela ne permet pas d'établir un juste équilibre entre les obligations du responsable et les intérêts et droits des personnes concernées[343].

47 Le droit d'opposition. Le droit d'opposition est ouvert uniquement lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public, ou aux intérêts légitimes poursuivis par le responsable du traitement[344]. En vertu de l'article 14 premier alinéa sous a) de la directive 95/46/CE, les personnes concernées disposent d'un droit d'opposition au traitement de leurs données[345]. Ce droit d'opposition s'applique notamment aux traitements de données qui se fondent sur l'exercice d'une mission de service public (art. 7 sous e) de la directive), sur l'intérêt légitime du responsable du traitement (art. 7 sous f) de la directive[346] ou lorsque la personne concernée souhaite s'opposer à la poursuite du traitement de ses données personnelles passé le délai de conservation utile à la réalisation des finalités légitimes de ce traitement (art. 12 sous b)[347] ou encore lorsque le consentement n'est pas le fondement légitime du traitement (par ex. en matière de prospection commerciale). Cependant, le droit d'opposition n'est pas absolu **:** il faut « tenir compte de manière plus spécifique de toutes les circonstances entourant la situation de la personne concernée » [348] . Avant l'affaire *Google Spain*, l'affaire de la CourEDH *Wegrzynowski et Smolczewski c. Pologne*[349] avait établi la non obligation pour un journal de

---

341 CJUE, X. contre Bois-le-Duc, Aff. C-486/12, 12 décembre 2013.

342 CJUE, Gerechtshoft te's-Hertogenbosch, aff. C-486/12, 12 décembre 2013.

343 CJ, Rikeboer, aff. C-553/07, 7 mai 2009.

344 Voy. l'art. 21. 1 renvoyant à l'article 6.1 points e), et f) du RGPD.

345 CJUE 9 mars 2017 « Salvatore Manni » Aff. C-398/15, § 47.

346 CJUE, Salvatore Manni, Aff. C-398/15, 9 mars 2017, § 47.

347 CJUE, Salvatore Manni, préec., § 46 et CJUE 13 mai 2014 « Google contre Espagne » Aff. C-131/12, § 70.

348 CJUE, Salvatore Manni, préec.§ 47.

349 CEDH1, Wegrzynowski et Smolczewski c. Pologe, no. 33846/07 6 juillet 2013.

retirer complètement de ses archives Internet un article jugé inexact par un tribunal. Prenant en compte l'ensemble des circonstances, la Cour admet que la Pologne a respecté son obligation de ménager un équilibre entre les droits garantis par l'article 10 (liberté d'expression) et ceux protégés par l'article 8 (droit au respect de la vie privée) de la Convention. Elle estime qu'une restriction à la liberté d'expression destinée à protéger la réputation de M. Smolczewski aurait été disproportionnée au regard de l'article 10. Partant, elle conclut qu'il n'y a pas eu violation de l'article 8. La CourEDH a ainsi conclu : « Il ne relève pas de l'autorité judiciaire de réécrire l'histoire, en ordonnant de faire disparaître toutes traces d'une publication qu'elle a même été déclaré, avec une décision définitive, constituer une violation injustifiée de la réputation d'un individu ».

48 Le droit à la rectification. Ce droit était déjà prévu par la directive 95/46 et permet aux personnes d'avoir un contrôle actif sur leurs données en pouvant intervenir sur leur contenu[350]. Il s'agit d'un corollaire au principe d'autodétermination informationnelle. Ainsi la personne concernée doit pouvoir demander au responsable de traitement de mettre à jour les données ou de rectifier les données lorsqu'elles sont inexactes ou lacunaires.

3) Des mécanismes de contrôle indépendants

49 Les autorités de contrôle nationales. Une des caractéristiques du modèle de protection européenne, c'est la création d'autorités de contrôle nationales, prévues par l'art. 28 de la directive ainsi que par l'art. 8 de la Charte des droits fondamentaux[351]. Il s'agit d'un organisme national indépendant chargé de surveiller l'application des dispositions de la directive[352] et désormais du Règlement 279/16. Dans l'affaire *Digital Rights,* la Cour de justice réaffirme le rôle essentiel des autorités et de leur indépendance dans la mise en œuvre du droit à la protection des données personnelles[353]. La jurisprudence de la Cour de justice a consacré l'indépendance des autorités de contrôle dans le cadre de recours en manquement contre l'Allemagne, l'Autriche et la Hongrie. Dans une affaire opposant la Commission à l'Allemagne, la Commission a demandé à la Cour de justice de déclarer que l'Allemagne avait mal transposé la disposition de la directive 95/46 concernant l'exigence d'une action « en toute indépendance » des autorités de contrôle chargées de garantir la protection des données et partant, avait manqué à ses obligations découlant de l'art. 28, §1 de la directive[354]. Dans cet

350 Voy. l'art. 16 du RGPD.

351 Voy. Access to Data protection remedies in EU Member States, European Union Agency for fundamental rights, Luxembourg publications Office of the European Union, 2013.

352 I. FALQUE-PIERROTIN, « Des problématiques concurrentielles imposant la mise en place d'une véritable interrégulation », *Concurrences* 2-2013, p. 30.

353 Point 68 décision Digital Rights Ireland. Voy. aussi sur ce point l'affaire de la CJUE, Commission c. Autriche, C-614/10, point 37.

354 CJUE, 9 mars 2010, Commission c. Allemagne aff. C-518/07.

affaire la Cour de justice précise que l'article 28§1 prévoit une indépendance qui n'est pas seulement fonctionnelle[355]. Ainsi la Cour a conclu que « lors de l'exercice de leurs missions, les autorités de contrôle doivent agir de manière objective et impartiale. À cet effet elles doivent être à l'abri de toute influence extérieure, y compris celle, directe ou indirecte, de l'État ou des Länder »[356]. Dans une autre affaire[357], la Cour condamne la Hongrie pour violation du principe d'indépendance de l'autorité nationale de contrôle, selon ce principe l'État doit respecter la durée du mandat. L'affaire précise les qualités que doivent posséder les autorités de contrôle[358]. Ainsi, afin de garantir l'indépendance de l'autorité, les fonctionnaires doivent pouvoir aller jusqu'au bout du mandat fixé par les textes au moment où ils ont été nommés. De même, la Cour de justice a condamné l'Autriche en estimant que l'autorité de protection des données autrichienne n'exerçait pas sa mission en toute indépendance[359].

50 Le G29. Pour renforcer la mise en œuvre de la directive, l'article 29, énonce la création d'un Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (ci-après G29), composé d'un représentant de l'autorité de contrôle désigné par chaque État membre, d'un représentant de l'autorité créé par les institutions et organismes communautaires et d'un représentant de la Commission. Ce groupe prend le nom de Groupe29. Ses missions font l'objet de l'article 30 de la directive [360] . Les avis du G29 ne sont pas juridiquement contraignants toutefois ils peuvent influencer grandement la pratique des autorités de protection nationales [361] . Un comité est aussi prévu à l'article 31 de la directive. Il est composé de représentants des États membres, présidé par le représentant de la Commission et il assiste celle-ci. Des projets de mesures à prendre lui sont soumis pour avis par l'organe européen comme pour les décisions relatives au niveau de protection adéquat présentées par un pays, ou celles relatives aux mesures à prendre lorsqu'il y a une opposition d'un État membre ou de la Commission elle-même à un transfert de données, ainsi que celles concernant les clauses contractuelles type. À différence du G29, ses travaux ne sont pas publics. Toutefois le G29 s'est révélé être par sa composition un organe peu flexible, c'est pour cette raison que l'article 64 du nouveau règlement le remplace par le Comité européen de la protection des données doté de personnalité juridique[362]. Ce nouvel organe rendra des avis contraignants ayant comme mission

---

355 F. KAUFF-GAZIN, « Vers une conception européenne de l'indépendance des autorités de régulation ? », *Europe*, 2010, étude 9.

356 CJCE, *Commission c. Allemagne*, C-518/07, mars 2010, § 27.

357 CJUE, *Commission c. Hongrie*, aff. C-288/12, 8 avril 2014.

358 CJUE, 8 avril 2014, aff. C-288/12, Commission c. Ungherie, point 50 et 67.

359 CJUE, *Commission c. Autriche*, aff. C-614/10, 16 octobre 2012.

360 Cette organisation a pour mission de contribuer à l'élaboration des normes européennes en adoptant des recommandations ; de rendre des avis sur le niveau de protection dans les pays hors l'Union européenne : de conseiller la Commission européenne sur tout projet ayant une incidence sur la protection des données et des libertés des personnes. Ses travaux, bien que n'ayant aucune force contraignante sur le plan juridique, font autorité en matière d'analyse et d'interprétation de la directive européenne.

361 Ch. KUNER, *European data protection law, Corporate compliance and regulation*, Oxford university press, 2éd. 2007, n°1.24, p. 12.

principale d'assurer la coopération, la cohérence et l'échange d'informations entre les différentes autorités de protection. Il est composé d'un membre de chaque autorité de protection dans les États membres et du Contrôleur européen à la protection des données (CEPD), institué par le règlement 45/2001/CE du Parlement et du Conseil du 18 décembre 2000 [363] . La Commission a le droit de participer aux activités et réunions du Comité sans droit de vote.

B. Le Champ d'application territorial

51 L'extension du champ de la protection. Afin de comprendre l'apport du RGPD vis-à-vis de l'extension territoriale de protection[364], il est nécessaire de parcourir l'application territoriale de la directive 95/46. Les règles posées par la directive 95/46/CE s'appliquaient « au traitement de données à caractère personnel, qu'il soit automatisé ou non, réalisé par les personnes et organismes privés ou publics établis[365] sur le territoire de l'Union européenne ou ayant recours à des moyens de traitement dans l'Union européenne ». L'application territoriale de la directive relative à la protection des données personnelles s'étendait au-delà des 28 États membres de l'Union et incluait les États qui font partie de l'EEE[366].
Les dispositions de droit national applicable des États membres était régies par l'article 4[367] de la directive, lorsque le responsable était établi sur le territoire de l'État membre. S'il était établi sur le territoire de plusieurs États membres, il devait assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable[368]. Ainsi il est possible de distinguer le critère du lieu d'établissement du responsable de traitement et le critère de l'activité. Par rapport à la Directive 95/46/CE, le champ d'application du RGPD a été étendu et contient désormais le critère du ciblage du public du traitement des données, tant qu'on peut parler d'application extraterritoriale. Par ailleurs, cette extension est conforme à la

362 Voy. le site internet du Comité, disponible à l'adresse/ https://edps.europa.eu/data-protection_fr

363 Le CEDP est nommé par le Parlement et le Conseil pour une durée de cinq ans sur la base d'une liste établie par la Commission. Il peut mener des enquêtes et en dernier recours saisir la Cour de justice et si nécessaire la Commission, le Parlement, et le Conseil.

364 F. JAULT-SESEKE, « La portée extraterritoriale ou a-territoriale du RGPD », in *Revue des affaires européennes*, Bruylant, 2018, p. 43 et s.

365 Ici le respect de la législation européenne est soumis au principe du lieu d'établissement.

366 Accord sur l'espace économique européen, JO 1994 L1, qui est entré en vigueur le 1° janvier 1994, (Islande, Liechtenstein et Norvège).

367 Voy. aussi les considérants 18 à 21.

368 Cette distinction n'aura plus d'application lorsqu'en mai 2018 le règlement s'appliquera à tous les états membres avec une discipline uniforme et dans le cas d'un responsable de traitement établi dans plusieurs États membres, le règlement prévoit la compétence d'une seule autorité de contrôle, sur la base du critère de l'établissement principal.

jurisprudence de la Cour de justice de l'Union européenne, qui en 2014 s'était prononcée en faveur de l'application extraterritoriale de la Directive 95/46/CE dans l'affaire Google Spain[369].

52 Les critères du lieu d'établissement et du cadre d'activité. La notion d'établissement a été précisée par la jurisprudence et par le G29. Ainsi ne caractérisent pas un établissement : la simple accessibilité d'un site Internet dans l'État membre dont l'application de la loi nationale est invoquée [370]; un serveur ou un ordinateur puisqu'il s'agit simplement d'une installation technique ou d'un outil de traitement d'informations[371]. Il s'agit d'un établissement « toute activité réelle et effective même minime exercée au moyen d'une installation stable » qui peut résulter d'indices tels que la rédaction d'annonces en langues locales, l'ouverture d'un compte en banque dans l'État membre, la présence d'un simple agent du responsable du traitement dans l'État membre dont l'application de la loi est invoquée[372]. Dans l'arrêt *Weltimo* du 1er octobre 2015[373], la Cour de justice s'est prononcée sur un cas dans lequel le responsable de traitement disposait d'un établissement principal dans un pays membre (ici la Slovaquie), mais dirigeait ses services vers un autre État membre (la Hongrie) au moyen d'un site web publiant des annonces immobilières. L'affaire au principal ayant abouti au renvoi préjudiciel sur lequel la Cour de justice s'est prononcée portait en substance sur la question de la compétence de l'autorité hongroise de protection des données à sanctionner cette société. La Cour a tout d'abord rappelé les termes de l'arrêt *Google Spain,* selon lesquels « l'expression "dans le cadre des activités d'un établissement"[374] ne saurait recevoir une interprétation restrictive »[375]. En effet, une interprétation restrictive pourrait porter atteinte à l'objectif de la directive 95/46/CE d'assurer une protection « efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée, à l'égard du traitement des données »[376]. La Cour de justice reprend la formule de l'arrêt *Google Spain*, dans lequel, en se basant sur le considérant 19 de la directive 95/46/CE, elle avait affirmé que l'établissement sur le territoire d'un État membre suppose l'exercice effectif et réel d'une activité au moyen d'une installation stable, la forme juridique de cet établissement n'ayant pas d'importance[377]. Dès

369 CJUE, Google c. Espagne, Aff. C-131/12, 13 mai 2014, § 48.

370 CJUE, Verein für Konsumenteninformation c. Amazon aff. C-191/15, 28 juillet 2016.

371 Voy. l'avis du G29 n°8/2010 du 6 décembre 2010, p. 13.

372 CJUE, Weltimmo, Aff. C-230/14, 1er octobre 2015 § 31 et s.

373 CJUE, Weltimmo Aff. C-230/14.

374 G. CAGGIANO, *L'interpretazione del criterio di collegamento del « contesto delle attività di stabilimento » del responsabile del trattamento dei dati personali*, In *Il diritto all'oblio dopo la sentenza Google Spain*, a cura di G. RESTA e V. Z. ZENCOVICH, Roma3press. sp. p.43 et ss.

375 CJUE, Weltimmo, Aff. C-230/14, § 25.

376 Voy. §25.

377 CJUE, Google c. Espagne, Aff. C-131/12, 13 mai 2014, § 48.

lors, il suffit pour dire qu'un responsable de traitement dispose d'un établissement au sens de la directive 95/46/CE, « d'évaluer tant le degré de stabilité de l'installation que la réalité de l'exercice des activités dans cet autre État membre, en tenant compte de la nature spécifique des activités économiques et des prestations de services en question. Cela vaut tout particulièrement pour des entreprises qui s'emploient à offrir des services exclusivement sur Internet »[378]. Nous verrons que le RGPD apporte une innovation en posant un critère alternatif, le rattachement lié à la localisation du public ciblé par le traitement. La directive 95/46/CE et le RGPD ne sont pas les seuls instruments pour lq protection des données personnelels. D'autres instruments sont venus compléter le cadre législatif encadrant le traitement des données personnelles.

§2. Les directives sur la vie électronique

53 Renforcer la confiance et la sécurité dans le marché unique numérique. La directive 95/46 a été adoptée lorsque Internet n'existait pas. Ainsi l'évolution de l'informatique a offert de nouvelles perspectives de risque pour la vie privée, pour cette raison un cadre juridique spécifique a été conçu pour faire face aux enjeux technologiques. La directive 97/66/CE[379] est venue préciser les principes applicables au traitement des données à caractère personnel et à la protection de la vie privée dans le secteur des télécommunications, il s'agit de la première directive sectorielle. Ce texte a été remplacé par la directive 2002/58/CE [380] concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, ce texte a été complété par la directive 2006/46/CE du 15 mars 2006 relative à la rétention des données, et révisée par la directive 2009/136/CE du 25 novembre 2009[381], modifiée par le « paquet télécom » en 2009 (A). Toutefois, à cause de l'ingérence que la directive comportait dans la vie privée des personnes concernées, elle a été invalidée par la Cour de justice en 2014 dans l'affaire « *Digital rights* ». Cette invalidation intégrale et *ab initio* a entraîné de lourdes conséquences pour les législations nationales qui avaient transposé la directive. Ainsi la question autour de la conservation des données a fait l'objet d'une nouvelle décision de la Cour de justice dans l'affaire « *Tele2* » (B).

A. La première législation en matière de communications électroniques

---

378 CJUE, Weltimmo, Aff. C-230/14, § 29.

379 Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications OJ L 24, 30.1.1998, p. 1–8.

380 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) OJ L 201, 31.7.2002, p. 37–47

381 Directive 2009/136/CE du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques.

54 Des instruments garantissant la confidentialité des communications. L'évolution de l'informatique offre de nouvelles perspectives de risque pour notre vie privée. Cela pose la nécessité d'ajustements continus des règles de protection. La législation dans ce domaine est un chantier ouvert, puisque le besoin de nouvelles règles est de plus en plus fort afin de faire face aux instruments technologiques toujours plus performants, capables de scruter, classifier, contrôler chacun de nous. L'impact des nouvelles technologies a suggéré au législateur communautaire de compléter et en partie préciser certaines dispositions de la directive 95/46. Il s'agit tout d'abord de la directive 97/66 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[382]. Ainsi la directive 97/66 prévoyait des mesures sur la conservation des données des utilisateurs dans un but de sécurité publique[383]. Cette approche de mise en balance entre droits fondamentaux et sécurité publique a été confirmée plus tard avec l'adoption du « paquet télécom » en 2002[384] après les attentats du 11 septembre 2001. Quelques années plus tard la directive 2002/58/CE[385] (directive *e-privacy*), faisant partie du « paquet télécom », abroge et remplace la directive 97/66[386]. Elle contient des règles fondamentales destinées à garantir la confiance des utilisateurs dans les services des communications électroniques toujours dans la logique de renforcer le marché intérieur lié à l'économie numérique. Ladite directive garantit une défense de l'internaute contre le « spam », en établissant le système de consentement préventif de l'utilisateur (« *opt-in* »), ainsi que des règles spécifiques pour l'installation de marqueurs (« *cookies* »)[387] particulièrement intrusifs et capables de collecter des milliers d'informations et

---

382 Voy.. Directive 97/66/CE du Parlement européen et du Conseil du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Dans le cadre de leur activité, les fournisseurs de réseaux et services, ils traitent les données personnelles aux buts de la transmission d'une communication, de la facturation, des payements d'interconnexion, de la commercialisation et de la fourniture et d'autres services. Tel traitement concerne les données qu'ils indiquent la source, le destinataire, la date, l'heure, la durée et le type d'une communication, ainsi que les équipements de communication des utilisateurs et, dans le cas d la téléphonie mobile, donne sur l'emplacement des équipements.

383 Voy. art. 14 §1. Les États membres peuvent prendre des mesures législatives visant à limiter la portée des obligations et des droits prévus aux articles 5 et 6 et à l'article 8 paragraphes 1 à 4 lorsqu'une telle limitation constitue une mesure nécessaire pour sauvegarder la sûreté de l'État, la défense, la sécurité publique, la prévention, la recherche, la détection et la poursuite d'infractions pénales ou de l'utilisation non autorisée du système de télécommunications, comme le prévoit l'article 13 paragraphe 1 de la directive 95/

384 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)

385 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

386 La directive *e-privacy* a été modifiée par la directive 2009/136/CE.Voy. G. CAGGIANO, « La riforma del regime delle radiofrequenze nel quadro delle comunicazioni elettroniche », in *Studi sull'integrazione europea*, 2010, p.79 et s.; G. CAGGIANO, « La regolazione delle reti delle comunicazioni e dell'energia nel diritto dell'Unione europea », in *Studi sull'integrazione europea,* 2011, p.41 et s.

387 Il faut aussi mentionner la directive 2009/136/CE, Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection

de les croiser pour créer un profil de l'utilisateur, ses goûts, etc. La directive établit que les États membres doivent mettre en place des mesures visant à empêcher et prohiber à des sujets tiers d'écouter et de mémoriser les communications électroniques sans le consentement des utilisateurs. En ce qui concerne la sûreté des services, le fournisseur d'un service de communication électronique doit garantir que les données personnelles sont accessibles seulement au personnel autorisé, protégées contre la destruction, perte ou altération accidentelle. Les éventuelles violations doivent être communiquées à la personne intéressée, ainsi qu'à l'autorité nationale de contrôle. À son tour, la directive 2002/58 a été modifiée par la Directive 2006/24/CE[388] (*Directive data Retention*) adoptée à la suite des attentats de Madrid et Londres en 2004 et 2005. Son considérant 10 mentionne explicitement les attaques terroristes de Londres[389]. En effet, la conservation des données joue un rôle très important dans le cadre de la lutte contre le terrorisme et d'autres formes de crimes graves. Une modification du texte de la directive 2002/58/CE était alors nécessaire car elle prévoyait la possibilité de conserver des données de trafic et de localisation pour la recherche, la détection et la poursuite d'infractions pénales, mais ne contenait aucune obligation à ce sujet. D'ailleurs, la proposition du règlement *e-privacy*[390] actuellement examinée par le Conseil et le Parlement européen, vise à la mise à jour de la directive « *e-privacy* » en l'adaptant aux modifications apportées par le règlement général sur la protection des données personnelles (RGPD) mais également à l'évolution des usages, se concentrant principalement sur l'activité des fournisseurs d'Internet et non sur la surveillance et l'accès des métadonnées par les autorités publiques[391]. En effet, ce n'est pas la légitimité de l'objectif mais la durée de la conservation, la nécessité, la stricte proportionnalité de la récolte, la transparence de l'accès par les pouvoirs publics et l'existence de recours juridiques et administratifs par les personnes concernées qui sont mises en cause[392].

---

des consommateurs (Texte présentant de l'intérêt pour l'EEE). Le but de la directive 2009/136 est la plus grande tutelle des consommateurs contre les violations des données personnelles, les communications dite "spam."

388 Directive 2006/24 du Parlement et du Conseil européen du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

389 Voy. le 10ème considérant : Le 13 juillet 2005, le Conseil a réaffirmé, dans sa déclaration condamnant les attentats terroristes de Londres, la nécessité d'adopter dans les meilleurs délais des mesures communes relatives à la conservation de données concernant les télécommunications.

390 Disponible à l'adresse : https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications.

391 la Commission européenne distingue deux notions, à savoir le contenu des communications électroniques à proprement parler et les métadonnées associées à ces communications. Le principe de confidentialité s'entend ici de manière stricte, c'est-à-dire qu'il est interdit de traiter les données de communications électroniques, sans le consentement des utilisateurs et sauf à bénéficier de l'une des exceptions prévues dans le texte. Dans cette logique, les données de communications électroniques doivent être anonymisées ou effacées par les opérateurs une fois que ces derniers en ont assuré l'acheminement. Ces deux principes, déjà présents dans la directive de 2002 modifiée en 2009, sont reproduits dans la proposition de règlement. Voy. L'étude Eurobaromètre menée en amont de la proposition de règlement disponible en anglais à l'adresse : https://ec.europa.eu/digital-single-market/en/news/eurobarometer-eprivacy.

392 Toutefois, la proposition n'inclut aucune disposition spécifique sur la conservation des données. Elle dispose que les États membres peuvent légalement limiter certaines obligations et certains droits, lorsqu'une telle restriction constitue une mesure nécessaire et proportionnée pour sauvegarder des intérêts publics spécifiques, y compris la sécurité nationale, la défense, la sécurité publique et la prévention., détection ou répression d'infractions pénales ou exécution de sanctions pénales. Par conséquent, les États membres seraient en mesure de conserver ou de créer des cadres nationaux de conservation des données prévoyant des mesures de rétention ciblées, dans la mesure où ces cadres sont conformes avec le droit de l'Union, en tenant

B. La directive « *Data Retention* » sur la conservation des données

55 Une invalidation radicale *ex tunc*. Le raisonnement de la CourEDH aboutit, comme d'ailleurs celui de la Cour de justice, à définir toute collecte de données à caractère personnel comme une ingérence dans la vie privée des personnes, qui doit être légitime (principe de licéité et de loyauté des traitements) et proportionnée à la finalité (légitime) recherchée. Cette proportionnalité entraîne notamment l'obligation de limiter la collecte des données collectées au strict nécessaire, l'obligation de ne pas conserver les données au-delà d'un délai nécessaire à la réalisation de la finalité légitime du traitement [393] . Dans son article 11, la directive 2006/24/CE modifie l'article 15 de la directive 2002/58/CE394 en généralisant l'obligation de conservation des données des utilisateurs de la part de *Service Provider*[395]. Ainsi la directive 2006/24 légitime la collecte de métadonnées par les fournisseurs de services électroniques sans aucun lien avec les enquêtes en cours, afin de la recherche, de la détection et de la poursuite d'infractions graves, telles qu'elles sont définies par chaque État membre dans son droit interne[396]. La directive 2006/24 avait déjà fait l'objet de l'examen de la Cour de justice par un recours en annulation sous l'angle de sa base légale[397] mais le fondement choisi pour adopter

compte de la jurisprudence de la CJUE sur l'interprétation de la directive sur la protection de la vie privée et de la Charte des droits fondamentaux de l'Union européenne. Voy. the explanatory memorandum to the Proposal for a Regulation on Privacy and Electronic Communications COM(2017) 10 final, point 1.3.

393 Voy. art. 6 paragraphe 1 sous e) de la directive 95/46/CE.

394 Ainsi l'art. 15, §1, permet aux États membres de limiter les droits et les obligations inhérents à la vie privée lorsque la mesure est « nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, c'est-à-dire, la sûreté de l'État la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ».

395 Selon l'art. 15§1. Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale - c'est-à-dire la sûreté de l'État - la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne.

396 On notera que la possibilité de conservation des données existait déjà avant l'adoption de la directive 2006/24 sur la base de la Convention sur la Cybercriminalité du Conseil d'Europe (voy. art. 16). Toutefois cette conservation intervient suite à la décision d'un juge et non ex ante comme dans la directive 2006/24 pour toutes les données enregistrées et stockées par les ISP.

397 Voy. L' arrê t du 10 févr. 2009, aff. C-301/06, Irlande c/ Parlement européen et Conseil. La Cour de justice avait déjà examiné la directive 2006/24 dans le cadre d'un recours en annulation, et avait validé sa base juridique ancrée dans le pilier « marché intérieur ». Elle avait estimé que son objectif prépondérant concernait le fonctionnement du marché intérieur » (v. §85 de l'arrêt du 10 février 2009) en non la lutte contre le terrorisme. Pour la Cour de justice l'objet essentiel du texte est d'encadrer les obligations des opérateurs de télécommunications et non de réglementer l'accès à ces données par les autorités publiques. Pour l'Irlande le centre de gravité de la directive 2006/46 ne concernait pas le fonctionnement du marché intérieur et ne relevait pas du droit communautaire. Pour l'Irlande, l'objectif principal du texte était de faciliter la recherche, la détection et la poursuite d'infractions pénales. Dès lors, le texte aurait dû relever du troisième pilier, du titre VI du TUE. La CJ n'a pas suivi cette argumentation. Dans le même sens (base légale) on peut rappeler cette fois-ci l'annulation de la décision relative à la conclusion de l'accord PNR, CJ 30 mai 2006, aff. C-317/04 et C-318/04, UE c. États-Unis. Dans ce cas, ce sont les finalités de sécurité publique de prévention et de répression du terrorisme qui ont prévalu, conduisant à l'annulation d'actes pris sur le

le texte, l'article 95CE, a été contesté sans succès devant la Cour de justice[398] (1). Dans un second temps, c'est le contenu entier de la directive qui est remis en question devant la Cour de justice (2)

1) Une base légale incertaine

56 Le contentieux interpiliers. Suite aux attaques terroristes à New York le 11 septembre 2001, à Madrid le 11 mars 2004 et à Londres le 7 juillet 2005, la France, la Suède, l'Irlande et le Royaume- Uni proposaient d'adopter une directive sur la rétention des données dans le cadre du troisième pilier intergouvernemental sur la justice et les affaires intérieures[399]. Toutefois le Conseil et le Parlement, suivant les conclusions du rapporteur [400] , ont adopté la directive 2006/24 sur la conservation des données sur la base du premier pilier (marché intérieur). Ainsi 25 des 27 États membres l'avaient transposée dans leur droit national. Cependant, l'Irlande, soutenue par la Slovaquie, a formé recours afin d'obtenir l'annulation de la directive au motif qu'elle n'avait pas été adoptée sur la base juridique appropriée. Ainsi les requérants estimaient que le but central de la directive n'était pas le fonctionnement du marché intérieur, mais la recherche, la détection et la poursuite d'infractions pénales. De telles activités devaient trouver un fondement juridique dans le cadre du titre VI du Traité consacré à la coopération policière et judiciaire en matière pénale. La Cour de justice a rejeté le recours en suivant les conclusions de l'Avocat général et a approuvé le choix de l'art. 95 comme base juridique puisque « le contenu matériel de la directive vise pour l'essentiel les activités des fournisseurs de services dans le secteur du marché intérieur à l'exclusion des activités étatiques relevant du titre VI du traité UE »[401]. La directive en cause est intervenue précisément dans une situation où à la suite des attentats terroristes du 11 septembre 2001 à New York et du 11 mars 2004 à Madrid, plusieurs États membres avaient mis en place des mesures imposant aux fournisseurs de services de communications électroniques des obligations relatives à la conservation des données, afin de détecter et réprimer les infractions pénales relatives au terrorisme. Les divergences entre ces mesures avaient une incidence directe sur le fonctionnement du marché intérieur. Ainsi la directive visait effectivement « au bon fonctionnement du marché intérieur »[402]. La Cour de justice a estimé que la directive, même si elle avait comme but complémentaire la détection et la poursuite d'infractions graves, avait été adoptée à juste titre

fondement du pilier communautaire. Elle avait donc annulé la décision 2004/496 du Conseil, prise elle aussi en application de l'article 95 CE.

398 R. SICURELLA, V. SCALIA, « Data mining and Profiling in the Area of Freedom, Security and Justice. State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection », in *NJECrimL*, 2013, 4, p. 432 ss.

399 Voy. déclaration sur la lutte antiterroriste du 25 mars 2004 du Conseil de l'UE.

400 Voy. les conclusions du rapporteur Alexander Nuno Alvaro.

401 Voy. §84 de la décision.

402 Voy. §66-72 de la décision CJUE Irlande c. Parlement européen et Conseil C-306/06, 10 février 2009.

sur la base légale de l'art. 95[403], puisqu'elle s'appliquait à des opérateurs économiques (*Service Providers*) et non à des activités relevant du troisième pilier. L'arrêt a été rendu à une époque où la construction en piliers rendait difficile l'ancrage entre le pilier communautaire et l'ELSJ.

2) L'invalidation de la Directive « *Data Retention* »

57 Une conservation des données jugée disproportionnée. Suite au recours en annulation, c'est le texte tout entier de la directive 2006/24 (ci-après Directive *Data Retention* ou Directive sur la rétention des données) qui a été contesté, par voie préjudicielle, afin que la Cour de justice se prononce sur la question de sa validité vis-à-vis du droit de l'Union européenne et notamment vis-à-vis des articles 7 et 8 de la Charte des droits fondamentaux. Ainsi, comme souligné par l'avocat général Cruz Villaron, la « directive constitue une ingérence caractérisée dans le droit fondamental des citoyens au respect de la vie privée »[404]. En effet, la Haute Cour irlandaise et la Cour constitutionnelle autrichienne avaient saisi la Cour de justice afin de savoir si la directive sur la conservation des données viole, ou non, les articles 7 et 8 de la Charte des droits fondamentaux[405]. Selon la Cour de justice, les éventuelles restrictions au droit à la protection des données personnelles doivent être limitées au strict nécessaire [406] . D'ailleurs la proportionnalité de la mesure restrictive doit s'apprécier au regard des objectifs qu'elle poursuit.

58 La dualité fonctionnelle de la directive sur la conservation des données. La dualité fonctionnelle de la directive posait problème, la Cour de justice a constaté que l'objectif matériel de la directive était bien de contribuer à la lutte contre la criminalité grave [407] car la conservation des données afin de permettre aux autorités nationales d'y accéder « répond à un objectif d'intérêt général de l'Union »[408]. Toutefois, l'atteinte aux droits garantis par la Charte

---

403 Aujourd'hui art. 114 TFUE. Pour un commentaire sur la base juridique de la directive voy. : F. FABBRINI, « Lotta al terrorismo e tutela dei dati personali alla luce della sentenza Irlanda c. Parlamento e Consigli *o* », in *Quad. cost.*, 2009, 419 ss.

404 Il lui est à nouveau présenté, par la voie préjudicielle cette fois, afin qu'elle se prononce sur la question de sa validité. Deux demandes lui sont adressées, l'une par la Haute Cour irlandaise (High Court), saisie d'un litige par l'ONG Digital Rights Ireland (Elle défend les droits fondamentaux « à l'ère numérique ». V. www.digitalrights.ie/about/) au sujet de la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques, et l'autre par la Cour constitutionnelle autrichienne (Verfassungsgerichtshof), suite aux recours constitutionnels introduits auprès d'elle à la fois par le gouvernement du Land de Carinthie (Kärntner Landesregierung) et par MM. Seitlinger, Tschohl et plus de onze mille autres requérants, au sujet de la conformité à la Constitution fédérale (Bundes-Verfassungsgesetz) de la loi de transposition de la directive.

405 Deux demandes lui sont adressées, l'une par la Haute Cour irlandaise saisie d'un litige par l'ONG Digital Rights Ireland au sujet de la légalité de mesures législatives et administratives nationales concernant la conservation de données relatives à des communications électroniques et l'autre par la Cour constitutionnelle autrichienne, suite aux recours constitutionnels introduits auprès d'elle à la fois par le gouvernement du Land de Carinthie et par M. Seitlinger, Tschohl et plus de onze mille autres requérants, au sujet de la conformité à la Constitution fédérale de la loi de transposition de la directive.

406 Voy. §65 décision Digital Rights Ireland.

407 Voy. § 41 de la décision.

408 Voy. §44 de la décision.

est disproportionnée. La Cour de justice a estimé que « la directive comporte une ingérence d'une vaste ampleur et d'une gravité particulière dans les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sans que cette ingérence soit limitée au strict nécessaire »[409]. Ici c'est le manque de proportionnalité de la directive qui fait défaut[410]. Cette criticité avait déjà été soulignée par des États membres qui avaient présenté un projet de décision-cadre sur la conservation des données[411]. Ainsi la Cour de justice prononce l'invalidité de la directive sur la rétention des données avec effets *ex tunc*[412].

a) L'impact de l'invalidation de la directive « *Data Retention »*

59 Des conséquences dans les ordres juridiques des États membres. Les textes de transpositions de la directive 2006/24 (ci-après directive *Data Retention*) avaient fait l'objet de jugements défavorables bien avant son invalidation par la Cour constitutionnelle allemande, la Cour administrative de Bulgarie, le Conseil constitutionnel de Roumanie et la Cour suprême de Chypre. Toutefois, ces juridictions s'étaient limitées à examiner la législation nationale sans mettre en cause la directive. Ainsi des constatations de manquement pour défaut de transposition de la directive 2006/24/ CE dans le délai imparti avaient été prononcées par la

409 La Cour de justice a déclaré la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006 invalide, dans les affaires jointes C-293/12 et C-594/12, Le 8 avril 2014. Il faut se poser la question des conséquences susceptibles de découler au niveau national de l'arrêt rendu par la Cour de justice de l'Union européenne le 8 avril 2014, dit « Digital Rights », et notamment son impact probable sur la législation qui avait transposé cette directive en droit interne. Deux constats s'imposeraient à présent. D'une part, la loi qui transpose en droit interne la directive européenne a une existence propre et distincte par rapport à la directive transposée et invalidée par la Cour, de sorte qu'elle continue à s'appliquer. D'autre part, toute modification éventuelle de la loi nationale concernée, et cela malgré son existence propre et indépendante par rapport à la directive invalidée, sera conditionnée par les initiatives éventuellement à prendre et les traveaux menées au sein de l'UE. Il s'agit ici normalement de savoir si la Commission européenne prendra l'initiative de proposer une nouvelle directive en vue de remplacer la directive invalidée, et de tenir compte de la réforme de la protection des données personnelles actuellement en cours. En vertu de l'art. 266 TFUE, il appartient à l'institution dont émane l'acte annulé de prendre toutes les mesures nécessaires pour exécuter l'arrêt de la Cour. Si elle doit prendre un acte en conséquence, elle doit veiller à remplacer l'acte annulé par un acte qui n'est plus entaché d'illégalité. L'inexécution peut donner lieu à un recours en carence ou un recours en responsabilité. Par contre En ce qui concerne les arrêts préjudiciels en appréciation de validité, ils permettent de constater l'invalidité d'un acte communautaire nonobstant l'expiration des délais de recours en annulation. On peut d'ailleurs soulever les mêmes moyens que dans un recours en annulation mais la Cour n'annule pas l'acte : elle se borne à constater son invalidité. Le juge interne doit alors en tirer les conséquences, en pratique écarter l'acte communautaire déclaré contraire.

410 M. NINO, « L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE: prospettive ed evoluzioni future del sistema europeo di Data Retention », in *Dir. Un. Eur*., 2014, 803, spec. 806 ss.

411 Le 28 avril 2004 la France, l'Irlande, la Suède et le Royaume-Uni ont présenté au Conseil une initiative afin d'adopter une décision-cadre fondé sur les artt. 31, n. 1, lett. c), UE e 34, n. 2, lett. b), UE. Ce projet concernait la conservation des données stockées par les services de communication électronique et accessibles par les autorités publiques afin de détecter, rechercher les crimes graves et le terrorisme. (document du Conseil n. 8958/04).

412 On notera que la Cour aurait pu limiter les effets de l'arrêt dans le temps, comme demandait l'Avocat général.

Cour de justice à l'encontre de l'Irlande[413], de la Grèce[414], l'Autriche[415], de la Suède[416]. Bien plus, la Suède a été condamnée au paiement d'une amende 3 millions d'euros [417] et l'Allemagne s'est vue signifier par la Commission l'introduction d'une requête en vue de sa condamnation au paiement d'une astreinte journalière de 315.036,54 euros[418]. L'arrêt *Data Retention* est crucial pour ses conséquences. L'annulation pose des problèmes pour les États membres qui ont adopté une législation sur la base de la directive 2006/24 annulée même si le service légal du Parlement européen avait pris soin de souligner que l'invalidation *ab initio* de la directive n'affecterait pas le droit national[419]. Cependant, maintenir de telles législations pourrait être jugé contraire à l'art. 13.1 de la directive 95/46 qui autorise des dérogations pour la lutte contre le crime mais toujours dans le respect des principes généraux du droit et de l'art. 6 TUE. Si la directive 24/2006 viole les droits fondamentaux, il semble évident que les mesures nationales de transpositions les violent aussi et sont contraires au droit de l'Union. Ainsi les décisions au sein des États membres se sont enchaînées : celle de la Cour suprême administrative de Bulgarie[420] ; celle de la Cour constitutionnelle de Roumanie du 8 octobre 2009[421]; celle du Tribunal constitutionnel fédéral allemand[422]; celle de la Cour suprême de Chypre[423]; celles de la Cour constitutionnelle de la République tchèque[424]. Or d'autres contentieux sont en instance devant la Cour constitutionnelle hongroise à raison du recours introduit par la *Társaság a Szabadságjogkért* ou *Hungarian Civil Liberties Union* (« TASZ ou HCLU ») devant la Cour constitutionnelle slovaque du fait d'un recours introduit par des parlementaires soutenus par le *European Information Society Institute*. Ainsi en Roumanie, la nouvelle législation de transposition de la directive 2006/24/CE s'est heurtée à de telles réticences et résistances des organisations de la société civile, du contrôleur national des données à caractère personnel, du gouvernement lui-même, que le ministre roumain des Affaires européennes a été contraint de présenter le texte non pas comme membre du gouvernement mais comme membre du Parlement. Or, de telles décisions déclarant inconstitutionnelles les mesures nationales de transposition de la directive 2006/24/CE n'ont pas été sans incidence à l'échelle de l'Union européenne. En effet,

---

413 CJUE, Commission contre Irlande, affaire C 202/09, 26 novembre 2009.

414 CJUE, Commission contre Grèce, affaire C 211/09, 26 novembre 2009.

415 CJUE, Commission contre Autriche, affaire C-189/09, 29 juillet 2010.

416 CJUE, Commission contre Suède, affaire C-185/09, 4 février 2010.

417 CJUE, Commission contre Suède, affaire C-270/11, 30 mai 2013.

418 Requête C-329/12 déposée le 11 juillet 2012.

419 Voy. « Summary of the meeting of the European Parliement Commitee on Civil Liberties, Justice and home affaires, held in Brussels on 10 April 2014 », document 8940/14, 11 april 2014, p. 5.

420 Du 11 décembre 2008 (décision n°7)

421 Décision n°1258.

422 du 2 mars 2010 (BVerfG, 1 BvR 256/08)

423 du 1er février 2011 (demandes civiles 65/2009, 78/2009, 82/2009 et 15/2010-22/2010).

424 Rendue pour la première le 22 mars 2011 (Pl. ÚS 24/10: Data Retention in Telecommunications Services) et rendue pour la seconde le 4 janvier 2012.

la Commission s'est efforcée d'obtenir que les États ne disposant pas ou plus de dispositions nationales de transposition de la directive en disposent le plus rapidement possible, quitte à les menacer d'introduire des recours en manquement devant la Cour de Luxembourg.

b) Le respect du droit à la protection des données à caractère personnel dans la mise en œuvre du droit de l'Union. L'affaire *Tele2/ Watson*

60 Des indications sur la conservation des données au législateur national. La Cour de justice est revenue sur la question dans les affaires jointes C-203/15, *Tele2Sverige AB/Post-och telestyrelsen*[425] et C-698/15, *Secretary of State for Home Department/Tom Watson e.a.*[426] (ci-après *Tele2/Watson*). L'affaire se pose en continuité avec l'arrêt *Digital Rights Ireland Ltd*[427]. Ici, ce sont les législations nationales de transposition de la directive 2006/24/CE invalidée par la Cour de justice qui sont mises en cause. On notera qu'à ce jour le législateur de l'Union européenne n'a toujours pas élaboré une nouvelle directive remplaçant la directive invalidée. Le renvoi préjudiciel concernait l'obligation générale imposée aux fournisseurs de services de communications électroniques en Suède et au Royaume-Uni, conformément à la directive 2002/58 sur la vie privée (article 15, paragraphe 1)[428], de se conformer à la directive sur la conservation des données (*Data Retention*). C'était la disposition de la directive *e-privacy* du 2002 qui était mise en cause, s'agissant d'une législation antérieure à la directive 2006/24 et pas « touchée » par le jugement d'invalidité de cette dernière. Or, la Cour de justice, avant de

---

425 Les deux affaires tranchées par la Cour portaient sur l'obligation générale imposée aux fournisseurs de services de télécommunications, en Suède et au Royaume-Uni, de conserver les données relatives aux communications électroniques. Dans la première affaire, et suite à l'invalidation de la directive 2006/24/CE – modifiant la directive 2002/58/CE (vie privée et communications électroniques) – Tele2Sverige, fournisseur de services de communications électroniques établi en Suède, avait notifié aux autorités qu'elle cesserait de conserver les données relatives aux communications électroniques. Suite à une injonction de conservation de ces données, elle a introduit un recours juridictionnel devant le tribunal administratif puis interjeté appel. C'est alors la juridiction de renvoi qui a saisi la Cour de justice, afin que celle-ci se prononce sur la question de savoir si l'obligation généralisée et indifférenciée de conservation des données relatives aux communications électroniques est compatible, compte tenu de l'arrêt DRI, avec l'article 15 de la directive 2002/58/CE, lu à la lumière des articles 7, 8 et 52 § 1 de la Charte des droits fondamentaux de l'Union.

426 Dans la seconde affaire, des particuliers, MM. Watson, Brice et Lewis, ont formé un recours juridictionnel contre l'article 1ier de la loi britannique DRIPA (Data Retention and Investigatory Powers Act de 2014) en invoquant son incompatibilité avec les articles 7 et 8 de la Charte ainsi qu'avec l'article 8 de la CEDH. La Cour d'Appel, saisie par le Ministre de l'Intérieur de l'arrêt de la High Court of Justice ayant estimé que la législation britannique instituant un régime généralisé de conservation des données de communications électroniques violait les articles susvisés de la Charte, a alors jugé utile de saisir la Cour de justice. Son renvoi préjudiciel portait principalement sur la question des conséquences de l'arrêt DRI sur la législation national

427 CJUE, aff. C-293/12 et C-594/12, 8 avril 2014.

428 Voy. l'art. 15 §1 : Les États membres peuvent adopter des mesures législatives visant à limiter la portée des droits et des obligations prévus aux articles 5 et 6, à l'article 8, paragraphes 1, 2, 3 et 4, et à l'article 9 de la présente directive lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale — c'est-à-dire la sûreté de l'État — la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques, comme le prévoit l'article 13, paragraphe 1, de la directive 95/ 46/CE. À cette fin, les États membres peuvent, entre autres, adopter des mesures législatives prévoyant la conservation de données pendant une durée limitée lorsque cela est justifié par un des motifs énoncés dans le présent paragraphe. Toutes les mesures visées dans le présent paragraphe sont prises dans le respect des principes généraux du droit communautaire, y compris ceux visés à l'article 6, paragraphes 1 et 2, du traité sur l'Union européenne

se poser la question de l'admissibilité de l'obligation de conservation généralisée des données, va d'abord résoudre le point de savoir si ces législations relèvent du champ d'application du droit de l'Union[429]. L'article 15 § 1 de la directive 2002/24 autorise les États membres à adopter des mesures législatives visant à limiter la portée des droits et obligations prévus, telles que des mesures de conservation de données. Ainsi elle estime que relèvent du champ d'application de la directive les mesures prévoyant l'accès des autorités nationales auxdites données. La Cour souligne tout d'abord que le principe de proportionnalité[430] n'est pas respecté. Ainsi la Cour constate que les législations nationales prévoient « une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique, et qu'elle oblige les fournisseurs de services de communications électroniques à conserver ces données de manière systématique et continue, et ce sans aucune exception »[431]. La Cour, rappelant son arrêt *Digital Rights* ainsi que les conclusions de l'Avocat général Cruz Villalon, souligne le manque de proportionnalité concernant la collecte massive de métadonnées, « prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-*ci* »[432]. Elle estime qu'une telle réglementation constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte, qui s'avère d'une « vaste ampleur et doit être considérée comme particulièrement grave »[433]. La Cour souligne que la lutte contre la criminalité grave et le terrorisme constitue un objectif d'intérêt général, mais un tel objectif, aussi fondamental soit-il, ne saurait justifier à lui seul qu'une règlementation comme celle incriminée soit considérée comme nécessaire[434]. Ainsi la Cour condamne les législations nationales comme excédant les limites du strict nécessaire, mais elle liste aussi les conditions dans lesquelles une législation nationale peut de manière proportionnée permettre, à titre préventif, la conservation des données relatives au trafic et des données de localisation, à des fins de lutte contre la criminalité grave. Ainsi la conservation devrait être « soit ciblée en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que

---

429 Saisie par voie préjudicielle par des juridictions d'appel suédoise et britannique, la CJUE était invitée à répondre à la question de savoir si les régimes nationaux qui imposent aux fournisseurs une obligation générale de conservation des données sont compatibles avec le droit de l'Union. Elle est par la même appelée à préciser l'interprétation à apporter dans un contexte national à l'arrêt Digital Rights Ireland.

430 En se référant à sa jurisprudence antérieure arrêts CJCE Satamedia, aff. C- 73/07 ; CJUE Volker und Markus Schecke & Eifert, C-92/09 et 93/09 ; CJUE, Digital Rights Ireland précité ; CJUE Schrems, C-362/14.

431 Voy. § 97 de l'arrêt.

432 Voy., par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, point 27.

433 Voy. point 101, (dès lors dans les mêmes termes que dans l'arrêt DRI, mais en faisant référence aussi Elle fait référence, à son arrêt DRI, mais rend également hommage à l'arrêt de la Cour EDH, Szabo et Vissy c/Hongrie du 12 janvier 2016 et à l'arrêt Zakharov c/Russie du 4 octobre 2015 de la Cour EDH, toutefois la Cour de justice s'appui de façon majeure sur sa propre, et abondante, jurisprudence).

434 Voy. § 105 de l'arrêt.

la durée de conservation retenue, limitée au strict nécessaire »[435]. « La réglementation nationale concernée doit se fonder sur des critères objectifs pour définir les circonstances et les conditions dans lesquelles doit être accordé aux autorités nationales compétentes l'accès aux données des abonnés ou des utilisateurs inscrits »[436]. Et elle impose en particulier comme une condition essentielle que « l'accès des autorités nationales compétentes aux données conservées soit, en principe, sauf cas d'urgence dûment justifié, subordonné à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante »[437]. La Cour déclare, en contradiction avec l'Avocat général Saugmandsgaard Øe, que l'article 15, paragraphe 1, de la directive 2002/58, lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte, « doit être interprété en ce sens qu'il s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique »[438]. Ainsi c'est au législateur communautaire de faire application de l'arrêt de la Cour de justice et de corriger les éléments d'incompatibilité avec sa décision. Il revient également au juge national d'écarter la norme interne incompatible avec le droit de l'Union[439]. Ainsi, en ce qui concerne le respect des limites de conservation des données dans la législation nationale, il n'existe pas de dispositions d'harmonisation mais une clause générale permettant aux États membres de légiférer sur les restrictions à condition que ces « restrictions respectent l'essence des droits et libertés fondamentales et constituent des mesures nécessaires et proportionnées dans une société démocratique destinée à sauvegarder un ou plusieurs intérêts publics conformément au Règlement général de 2016 »[440].

---

435 Voy. § 97 de l'arrêt.

436 Voy. § 119 de l'arrêt.

437 Voy. § 120 de l'arrêt.

438 L'approche adopté par la CJUE dans l'affaire Digital Ireland a certainement été prise en compte dans l'avis 1/15 rendu le 8 septembre 2016 relatif à l'accord PNR UE/Canada qui condamne le principe même du système PNR.

439 Concernant l'impact de l'affaire CJUE Tele2/Watson voy. le Document du conseil Doc. Council 5884/11, 1 February 2017 Legal Service to Permanent Representatives Committee, Judgment of the Court of 21 December 2016 in joined Cases C-203/15 and C-698/15 (Tele2 and Watson). Concernant les difficultés des États-membres dans la mise en oeuvre des indications de la CJ voy. doc. Council 6713/17, 1 March 2017, Retention of electronic communication data, next steps, par. 3: » Many delegations expressed their concerns on the implications of the judgement, which might hinder the effectiveness of the investigations and prosecutions of crimes.". Concernant le débat au sein du Conseil voy. le Doc. 8798/17, 4 May 2017, Access criteria for competent authorities to retained communication data, Exchange of views; doc. 11107/17, 12 July 2017, Processing and storage of data in the context of the draft ePrivacy Regulation, Introduction and preliminary exchange of views; doc 11110/17, 12 July 2017, Requirements of the Tele 2 judgement regarding Data Retention, Continuation of discussion. En ce sens on remarque le cas du droit italien dans lequel existe une obligation générale de conservation des données dans l'art. 132 de la loi informatique et libertés révisé en 2008 suite à l'adoption de la Directive sur la conservation des données. Cette disposition reste en vigueur car elle n'a pas été abrogée par le législateur italien et les juges italiens, ils sont restés «sourds» aux indications de la Cour de justice. Au contraire, les termes de conservation ont été étendus par le législateur italien par la « loi communautaire de 2017 » prévoyant que les opérateurs téléphoniques et télématiques maintiennent pour une période de soixante-douze mois, sans les mécanismes de consentement ni les règles d'accès des autorités publiques, les données téléphoniques et télématiques. Voy. Legislatura 17ª, Aula, Resoconto stenografico della seduta n. 894 del 10.10.2017, discussione e approvazione del disegno di legge n. 2886. (article 24). Pour une critique sur l'art. 132 de la loi informatique et libertés italienne voy.: R. FLOR, « Data Retention ed art. 132 cod. privacy: vexata quaestio (?) », in *Diritto penale contemporaneo*, 9 marzo 2017 (Nota a Trib. Padova, ord. 15 marzo 2017). La nouvelle prévision de la législation italienne semble être en contradiction avec l'arrêt de la Cour de justice, qui limite la marge d'appréciation nationale dans la conservation des données en se basant sur le principe de nécessité et de proportionnalité stricto sensu.

440 Voy. la proposition de l'art. 11, renvoyant à l'art. 23, par. 1, lett. da a) a e), du règlement (UE) 2016/679, en ce qui concerne la surveillance et l'inspection, il reviendra au législateur nationale d'établir les procédures entre le fournisseur de services de communications électroniques et l'autorité compétente pour garantir l'accès, le nombre de demandes reçues, les motifs juridiques et leur réponse.

Section II. La réforme. La troisième génération de règlementation

61 La nécessité de la refonte. La protection des données personnelles a connu plusieurs phases, dans un premier temps ce droit était rattaché au droit au respect de la vie privée[441], dans un second temps il a été pris en compte comme un droit autonome [442], dernièrement le cadre juridique de ce droit a fait l'objet d'une réforme en relation aux risques liés aux nouvelles technologies et afin de bâtir les fondements d'un marché unique numérique. Ainsi, la protection des données personnelles est, avec la révolution numérique, entrée dans une nouvelle ère au point de faire parler d'une troisième génération de règlementation [443] . Cette nouvelle valorisation des données a émancipé définitivement la protection des données personnelles du droit à la vie privée pour constituer un but en soi. Il s'agit de garantir une protection liée à la personne que ce soit dans sa sphère réelle, virtuelle, publique, privée, personnelle ou professionnelle. En effet, l'évolution des technologies et le développement massif du volume et de la variété des données en circulation ont créé de nouvelles menaces. Les technologies permettent aux entreprises privées ou aux autorités publiques d'utiliser les données à caractère personnel ont augmenté de manière exponentielle. De plus en plus, les personnes physiques rendent des informations les concernant accessibles publiquement et à un niveau mondial via les réseaux sociaux de toute sorte.

Ces évolutions ont requis un cadre de protection des données solide et plus cohérent dans l'Union, assorti d'une application rigoureuse des règles, car il importe de susciter la confiance qui permettra à l'économie numérique (enjeux stratégiques pour l'Union européenne) de se développer dans l'ensemble du marché intérieur. C'est dans ce contexte qu'en janvier 2012, la Commission européenne a proposé un cadre de réforme sur la protection des données, précisant que les règles actuelles en la matière devaient être modernisées compte tenu des évolutions technologiques et de la mondialisation[444]. Conformément aux projets de l'Union européenne concernant un marché unique numérique, l'informatique dématérialisée, l'Internet des objets (ci-après IoT), le Big Data et d'autres technologies sont considérés comme des éléments clés de la compétitivité et de la croissance. Les modèles d'affaire exploitent de nouvelles capacités de collecte massive, de transmission instantanée, de combinaison et de réutilisation

---

441 Voy. Art. 8 CEDH.

442 La Convention 108 adopté par le Conseil de l'Europe en 1980 est le premier texte international à avoir fixé les principes devant concilier la libre circulation, des données avec le respect des droits et des libertés fondamentales des personnes physiques.

443 N. MARTIAL-BRAN, J. ROCHEDELD, E. GATTONE, « Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation ? », Dalloz, 2013, p. 2788 et s.

444 Proposal for a regulation of the European Parliament and of the Council on the protection of individualswith regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), Insterinstitutional File : 2012/0011 (COD), 27 janv. 2012 ; Proposal for a directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the freemovement of such data, Insterinstitutional File : 2012/0010 (COD), 27 janv. 2012.

d'informations à caractère personnel en vue de finalités qui n'avaient pas été prévues et dont la justification est exposée dans des politiques de protection de la vie privée longues et peu compréhensibles. La réforme a consisté en une proposition de règlement général sur la protection des données, destinée à remplacer la directive relative à la protection des données personnelles[445], ainsi qu'une nouvelle directive relative à la protection des données dans les domaines de la coopération policière et judiciaire en matière pénale[446]. L'initiative de réforme, s'insère dans le programme « Agenda Digital pour l'Europe »[447] et plus généralement dans le cadre « Stratégie Europe 2020 »[448], les deux buts poursuivis sont d'une part, renforcer le droit fondamental à la protection des données personnelles et d'autre part, promouvoir le marché numérique européen en favorisant des opportunités dans le domaine de la *digital economy*[449], en renforçant la confiance des citoyens vis-à-vis des services *on line*[450]. Ainsi il est possible de retrouver une double logique[451], liée d'une part au développement du marché intérieur mais qui s'accompagne d'autre part d'un renforcement des droits fondamentaux. En effet, il est indéniable que le règlement 2016/679 (ci-après le RGPD ou le Règlement) tenant à harmoniser les règles nationales existantes et à moderniser la directive 1995/46/CE a pour but de renforcer la protection des données à caractère personnel dans une société de plus en plus digitale, en redonnant aux citoyens le contrôle des données personnelles qui les concernent, que celles-ci soient collectées et utilisées par les acteurs économiques privés ou par les acteurs du secteur public. D'ailleurs, l'instrument choisi est le règlement afin d'assurer une application uniforme de la législation dans chaque État membre. Selon le principe de subsidiarité[452] une telle action

---

445 COM (2012)11 Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données).

446 COM (2012)10 Proposition de Directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquê tes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données.

447 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52010DC0245R(01):EN:NOT

448 http://ec.europa.eu/europe2020/index_en.htm.

449 Le 11 avril 2016, la Commission a également lancé une consultation publique relative à l'évaluation et à la révision de la directive sur la vie privée et les communications électroniques 449 aux fins d'assurer la cohérence avec le règlement. Le groupe de travail de l'article 29449 et le Contrôleur européen de la protection des données ont recommandé la suppression de dispositions de cette directive afin d'éviter toute redondance.

450 ttp://www.coe.int/t/dghl/standardsetting/dataprotection/TPD_documents/T-PD-BUR_2012_01_EN.pdf

451 Expression de cette ambivalence, le considérant 13 du règlement dispose : « Afin d'assurer un niveau cohérent de protection des personnes physiques dans l'ensemble de l'Union, et d'éviter que des divergences n'entravent la libre circulation des données à caractère personnel au sein du marché intérieur, un règlement est nécessaire pour garantir la sécurité juridique et la transparence aux opérateurs économiques, y compris les micro, petites et moyennes entreprises, pour offrir aux personnes physiques de tous les États membres un même niveau de droits opposables et d'obligations et de responsabilités pour les responsables du traitement et les sous-traitants, et pour assurer une surveillance cohérente du traitement des données à caractère personnel, et des sanctions équivalentes dans tous les États membres, ainsi qu'une coopération efficace entre les autorités de contrôle des différents États membres. Pour que le marché intérieur fonctionne correctement, il est nécessaire que la libre circulation des données à caractère personnel au sein de l'Union ne soit ni limitée ni interdite pour des motifs liés à la protection des personnes physiques à l'égard du traitement des données à caractère personnel ».

452 Le principe de subsidiarité est consacré à l'article 5 du traité sur l'Union européenne. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.

est plus efficace au niveau de l'Union européenne[453]car la nature transfrontière des données peut mener à de graves préjudices lorsque les législations diffèrent d'un pays à l'autre, cette action de l'Union européenne doit respecter le principe de proportionnalité [454] . Ainsi le Règlement s'est substitué à la mosaïque des 28 législations nationales[455], son principal mérite sera sans doute de réaliser l'uniformisation des règles que la directive n'avait su assurer grâce aussi à un champ d'application plus étendu (§1). Le règlement représente donc une avancée par rapport à la directive mère, si ses principes sont maintenus[456] de nouveaux droits sont établis pour tenir compte des avancée technologiques ainsi que des nouveautés concernant la mise en œuvre du règlement grâce à de nouveaux acteurs (§2).

§1. Le champ d'application du règlement 679/16

62 Une application uniforme. Le règlement est entré en vigueur depuis le 25 mai 2016 et il est applicable à compter du 25 mai 2018. En vertu de l'article 288, alinéa 2, du traité sur le fonctionnement de l'Union européenne, le règlement s'applique directement dans tous ses éléments et dans tous les États membres. Par son application directe uniforme[457], le règlement impose aux États membres une application complète de tous les principes qu'il contient, sans possibilité de s'y soustraire en se retranchant derrière le droit national. Ainsi, à l'inverse de la directive, le règlement s'applique sans prise de mesures nationales de mise en œuvre. Le règlement comprend 99 articles, soit plus du double des 34 articles de la directive 95/46/CE. D'ailleurs, le champ d'application du règlement est plus étendu par rapport à celui de la directive 95/46. En vertu du principe de non-rétroactivité de la réglementation nouvelle, les effets futurs des traitements existants sont soumis au principe d'application immédiate de la réglementation nouvelle. Tant le champ d'application matériel (A) que territorial est étendu (B).

---

453 Art. 5§3 TUE : En vertu du principe de subsidiarité, dans les domaines qui ne relèvent pas de sa compétence exclusive, l'Union intervient seulement si, et dans la mesure où, les objectifs de l'action envisagée ne peuvent pas être atteints de manière suffisante par les États membres, tant au niveau central qu'au niveau régional et local, mais peuvent l'être mieux, en raison des dimensions ou des effets de l'action envisagée, au niveau de l'Union.

454 Art 5§4 TUE En vertu du principe de proportionnalité, le contenu et la forme de l'action de l'Union n'excèdent pas ce qui est nécessaire pour atteindre les objectifs des traités.

455 Comme le rappelle le considérant 3 du règlement, la directive 95/46/CE visait à harmoniser la protection des données à caractère personnel, mais sa transposition en droit interne avait entraîné des divergences entre les États membres.

456 Voy. les principes de la directive 95/46 : traitement licite et loyale, sur la base du consentement donné suite à l'information sur les finalités du traitement et le droit d'exercer le droit d'accès, de rectification, d'effacement.

457 L'effet direct du règlement fut originellement confirmé par l'arrêt Politi du 14 décembre 1971 de la Cour de justice de l'Union européenne : « En raison de sa nature même et de sa fonction dans le système des sources du droit communautaire, tout règlement produit des effets immédiats et doit être, comme tel, apte à conférer aux particuliers des droits que les juridictions nationales ont l'obligation de protéger ».

A. Le champ d'application matériel

63 L'objet de la protection. Le règlement s'applique à toute information concernant une personne physique identifiée ou identifiable[458] lorsque le traitement automatisé en tout ou en partie est contenu ou destiné à figurer dans un fichier. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci[459]. Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues anonymes de telle manière que la personne concernée ne soit pas ou plus identifiable. Ainsi le règlement ne s'applique pas au traitement de telles informations anonymes, y compris à des fins statistiques ou de recherche. Le règlement codifie la jurisprudence de la Cour de justice, qui a conclu que les adresses IP sont « des données protégées à caractère personnel, car elles permettent l'identification précise desdits utilisateurs » [460] . De plus, sur la base des avancées technologiques, les « données de localisation » et « un identifiant en ligne » tels les « témoins de connexion (*cookies*) » ont été ajoutés comme exemples d'identifiants[461]. Une nouveauté est constituée également par les concepts d'identité « génétique » et « économique »[462]. Ainsi les données génétiques, biométriques [463] ou concernant l'orientation sexuelle d'une personne

458 Voy.: UE, règl. (UE) n° 2016/679, 27 avr. 2016, cons. 30Au nombre des éléments permettant d'identifier une personne, figurent, notamment, les témoins de connexion (cookies) et les adresses IP. Ainsi la Cour de justice admet que ces adresses constituent des données personnelles. Voy. CJCE, 10 oct. 2016, aff. 58214, BRDA 22 /16 inf.21

459 La définition de donnée à caractère personnel introduit un critère de proportionnalité dans la mesure où le caractère identifiable d'une personne physique doit être déterminé sur le fondement de « moyens raisonnablement susceptibles d'être utilisés » prenant en considération « l'ensemble des facteurs objectifs » tels les technologies et les coûts (Règl. (UE) 2016/679, consid.

460 CJUE, 24 nov. 2011, aff. C-70/10, Scarlet Extended SA, § 51. – CJUE, 19 avr. 2012, aff.C-461/10, BonnierAudio et a., § 51 et 52. Voy. l'art. 4 du RGPD.

461 Voy. le Règl. (UE) 2016/679, consid. 30 et l'art. 4§1.

462 F. J. ZUIDERVEEN BORGEUISIUS, « Singling out peoplewithout knowing their names – Behavioural targeting, pseudonymous data, and the newData Protection Regulation », in. *Computer Law & Security Review*, avr. 2016, vol. 32, n° 2, p. 267.

463 N. GRAHAM, « Top 10 tips for processing biometric data, in *Privacy Laws & Business International Report*, n° 141, juin 2016, p. 12 et 13.

physique ont été ajoutées à la liste des données sensibles « catégories particulières de données à caractère personnel » dont le traitement est interdit sauf exceptions[464]. De plus, le législateur a encadré le traitement des données personnelles des mineurs en prévoyant que « le traitement des données à caractère personnel relatives à un enfant est licite lorsque l'enfant est âgé d'au moins 16 ans ». Toutefois, le règlement prévoit que les États membres peuvent « prévoir par la loi un âge inférieur pour ces finalités pour autant que cet âge inférieur ne soit pas en-dessous de 13 ans »[465] . Concernant les données à caractère personnel relatives aux condamnations pénales et aux infractions elles font l'objet d'une disposition distincte, l'article 10 du règlement énonce que leur traitement « ne peut être effectué que sous le contrôle de l'autorité publique » ou après que des garanties appropriées ont été prévues dans le droit d'un État membre.

En revanche, le RGPD ne s'applique pas aux traitements de données à caractère personnel effectués[466] dans le cadre d'une activité qui ne relève pas du champ d'application du droit de l'Union et par les États membres dans le cadre d'activités qui relèvent du champ d'application du chapitre 2 du titre V du traité sur l'Union européenne ; par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre des menaces pour la sécurité publique et la prévention de telles menaces (1) ; par une personne physique dans le cadre d'une activité strictement personnelle ou domestique [467] (2) ou à certains catégories particulières de données (3).

---

464 Voy. le Règl. (UE) 2016/679, art. 9, § 1 : : le traitement des données sensibles est possible lorsque la personne concernée a donné son consentement exprès, sauf s'il existe une disposition spéciale de droit national ou communautaire privant d'effet le consentement en présence d'un traitement de données sensibles. C'est par exemple le cas de l'art. L 1111-18, alinéa 2 du Code de la santé publique qui interdit l'accès par le professionnel (une compagnie d'assurance notamment) au dossier médical lors de la souscription par le client d'un contrat relatif à une protection complémentaire en matière de frais de santé ainsi qu'à l'occasion de tout autre contrat exigeant l'évaluation de l'état de santé. Hormis ce cas, il sera possible de traiter des données sensibles avec le consentement des personnes concernées à la condition que celui-ci soit exprès, libre, spécifique et éclairé ; si le traitement est nécessaires à la sauvegarde des intérêts vitaux (lorsque la personne soit dans l'incapacité de donner son consentement) ; Les traitements relatifs à la prévention, détection et administration de soins médicaux (le traitement nécessaires aux fins de la médicine préventive ou à la médicine du travail, de l'appréciation de la capacité de travail du travailleur de diagnostic médicaux de la prise en charge sanitaire ou sociale sur la base du droit de l'Union européenne ou d'un État membre ou en vertu d'un contrat conclu avec un professionnel de la santé ; Les traitements rendu public par la personne, cette exception permet à un responsable de traiter des données sensibles au sujet d'une personne qui les a volontairement rendues publiques, elle ne devrait pas s'appliquer lorsque les données ont été rendues publiques par un tiers. ; Gestion des membres d'une association ou tout autre organisme à but non lucratif (l'organisme doit poursuivre une finalité religieuse, philosophique ou syndicale dans le cadre de son activité légitime (en dehors de ces cas il faut recueillir le consentement de la personne) ; Traitements nécessaires pour des motifs d'intérêts public dans le domaine de la santé (à exclusion que ces données soient traitées par des tiers tels que les compagnies d'assurances ou les banques) tels que la protection contre les menaces transfrontières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité de soins de santé, et des médicaments ou des dispositifs médicaux ; Les traitements relatifs à la recherche aux études et évaluations dans le domaine de la santé ; Les données nécessaires à la constatation, l'exercice ou la défense d'un droit ; Les traitements de données à des fins statistiques, d'archivage, historiques (sur la base du droit de l'Union ou du droit de l'État membre qui doit respecter l'essence du droit, et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux de la personne concernée ; Exécution des obligations et droits propres au responsable du traitement en matière de droit de travail, sécurité sociale et la protection sociale ; Traitements autorisé par l'intérêt public, cette dérogation peut être utilisée pour des traitements intéressant la sûreté de l'État ou la sécurité nationale.

465 Voy. RGPD (UE) 2016/679, art. 8, § 1.

466 Voy. RGPD (UE) 2016/679, art. 2.

467 Soulignons que les traitements effectués dans le cadre d'une activité exclusivement personnelle ou domestique continueront à être exclus de la réglementation. Toutefois, celle-ci s'appliquera au responsable de traitement au sous-traitant qui fournit les moyens de traiter des données personnelles pour de telles activités (considérant 18).

1) Les exclusions d'application relevant de la répartition des compétences

64 Les activités qui ne relèvent pas du champ d'application de l'Union. Le règlement ne s'applique pas à des questions de protection des libertés et droits fondamentaux ou de libre flux des données à caractère personnel concernant des activités qui ne relèvent pas du champ d'application du droit de l'Union, telles que les activités relatives à la sécurité nationale[468]. En effet, la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces et la libre circulation de ces données, fait l'objet d'un acte juridique spécifique de l'Union. Le présent règlement ne devrait dès lors pas s'appliquer aux activités de traitement effectuées à ces fins. Toutefois, les données à caractère personnel traitées par des autorités publiques en vertu du présent règlement devraient, lorsqu'elles sont utilisées à ces fins, être régies par un acte juridique de l'Union plus spécifique, à savoir la directive (UE) 2016/680 du Parlement européen et du Conseil.

2) Les exclusions d'application relevant du type de traitement

65 Les activités purement personnelles ou domestiques. Dans le prolongement de la directive 95/46, le règlement ne s'applique pas aux traitements de données à caractère personnel effectués par une personne physique au cours d'activités strictement personnelles ou domestiques, et donc sans lien avec une activité professionnelle ou commerciale. Par activités personnelles ou domestiques le règlement entend l'échange de correspondance et la tenue d'un carnet d'adresses, ou l'utilisation de réseaux sociaux et les activités en ligne qui ont lieu dans le cadre de ces activités. Toutefois, le présent règlement s'applique aux responsables du traitement ou aux sous-traitants qui fournissent les moyens de traiter des données à caractère personnel pour de telles activités personnelles ou domestiques. De plus, le règlement ne s'applique pas aux données à caractère personnel des personnes décédées. Toutefois, il est prévu que les États membres peuvent prévoir des règles relatives au traitement des données à caractère personnel de ces personnes.

3) L'exclusion d'application relevant du traitement de certaines catégories de données personnelles

468 Voy. l'art. 2 du RGPD: « Le présent règlement ne s'applique pas au traitement des données à caractère personnel par les États membres dans le contexte de leurs activités ayant trait à la politique étrangère et de sécurité commune de l'Union ».

66 Le traitement des données sensibles. Le traitement des données sensibles est par principe interdit. Les exceptions sont prévues à l'art. 9 §2 du RGPD. Ainsi le traitement des données sensibles est possible si : la personne concernée a donné son consentement explicite au traitement de ces données à caractère personnel pour une ou plusieurs finalités spécifiques, sauf lorsque le droit de l'Union ou le droit de l'État membre prévoit que l'interdiction visée au paragraphe 1 ne peut pas être levée par la personne concernée; le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale ; le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; le traitement est effectué, dans le cadre de leurs activités légitimes et moyennant les garanties appropriées, par une fondation, une association ou tout autre organisme à but non lucratif et poursuivant une finalité politique, philosophique, religieuse ou syndicale ; le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ; le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ; le traitement est nécessaire pour des motifs d'intérêt public important ; le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection social ; le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique, tels que la protection contre les menaces transfrontalières graves pesant sur la santé, ou aux fins de garantir des normes élevées de qualité et de sécurité des soins de santé et des médicaments ou des dispositifs médicaux ; le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques ou si les données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel. Selon l'art. 10 du RGPD le traitement des données à caractère personnel relatives aux condamnations pénales et aux infractions ou aux mesures de sûreté connexes ne peut être effectué que sous le contrôle de l'autorité publique, ou si le traitement est autorisé par le droit de l'Union ou par le droit d'un État membre qui prévoit des garanties appropriées pour les droits et libertés des personnes concernées. Tout registre complet des condamnations pénales ne peut être tenu que sous le contrôle de l'autorité publique. Selon certains auteurs, les sanctions administratives sont couvertes par le texte[469].

B. Le champ d'application territorial

469 A. DEBET, J. MASSOT et N. METALLINOS, *Informatique et libertés. La protection des données à caractère personnel en droit français et européen*, Lextenso éd., 2015 p. 1219.

67 Un effet extraterritorial. L'application territorial du règlement va bien au-delà des frontières de l'Union [470] . Selon l'article 3 traitant du champ d'application territoriale, le règlement s'applique « dans le cadre des activités d'un établissement, d'un responsable de traitement de données ou d'un sous-traitant sur le territoire de l'union »[471]. Afin de garantir qu'une personne physique ne soit pas exclue de la protection à laquelle elle a droit en vertu du règlement, le traitement de données à caractère personnel relatives à des personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union sont soumis au règlement lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes, qu'un paiement soit exigé ou non.

Afin de déterminer si un tel responsable du traitement ou sous-traitant offre des biens ou des services à des personnes concernées qui se trouvent dans l'Union, le règlement prévoit qu'il y a lieu d'établir s'il est clair que le responsable du traitement ou le sous-traitant envisage d'offrir des services à des personnes concernées dans un ou plusieurs États membres de l'Union. Alors que la simple accessibilité du site Internet du responsable du traitement, d'un sous-traitant ou d'un intermédiaire dans l'Union, d'une adresse électronique ou d'autres coordonnées, ou l'utilisation d'une langue généralement utilisée dans le pays tiers où le responsable du traitement est établi ne suffit pas pour établir cette intention, des facteurs tels que l'utilisation d'une langue ou d'une monnaie d'usage courant dans un ou plusieurs États membres, avec la possibilité de commander des biens et des services dans cette autre langue ou la mention de clients ou d'utilisateurs qui se trouvent dans l'Union, peuvent indiquer clairement que le responsable du traitement envisage d'offrir des biens ou des services à des personnes concernées dans l'Union. Ainsi le responsable du traitement ou le sous-traitant (par exemple un fournisseur de nuages informatiques) peut donc être soumis au règlement sans pour autant être établi dans l'Union. Dans ce cas de figure, le responsable du traitement et le sous-traitant seront généralement tenus de donner un mandat écrit à un représentant européen. Le traitement de données à caractère personnel de personnes concernées qui se trouvent dans l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union est également soumis au règlement lorsque ledit traitement est lié au suivi du comportement de ces personnes dans la mesure où il s'agit de leur comportement au sein de l'Union. Afin de déterminer si une activité de traitement peut être considérée comme un suivi du comportement des personnes concernées, il y a lieu d'établir si les personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre

470 F. JAULT-SESEKE, « La portée extraterritoriale ou a-territoriale du RGPD », *in Revue des affaires européennes,* Bruylant, 2018, p. 43 et s.

471 En ce qui concerne le responsable de traitement ayant plusieurs établissements dans l'union européenne, l'établissement principal représente le lieu où sont prises la majorité des décisions quant aux traitements de données ; si aucune décision de ce type n'est prise sur le territoire de l'union, l'établissement principal sera considéré comme étant le lieu où sont exercées les principales activités de traitement dans le cadre des activités d'un établissement de responsable de traitement.
Quant au sous-traitant ayant plusieurs établissements dans l'union, l'établissement principal représente le lieu d'administration centrale. A défaut, l'établissement principal sera considéré comme le lieu où sont exercées les principales activités de traitement. En d'autres termes, lorsque le responsable du traitement (ou un sous-traitant) n'est pas basé dans l'union et entreprend le traitement de données personnelles liées à l'offre de biens ou services ou à l'observation du comportement de résidents de l'union, le règlement trouvera à s'appliquer.

des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit.
D'ailleurs, l'art. 25 du RGPD prévoit l'obligation pour le responsable du traitement ou le sous-traitant établi en dehors du territoire de l'Union européenne de désigner un représentant dans l'Union européenne.

§2. Des nouveaux droits et principes

68 Le régime de protection. Le RGPD a pour objectif de moderniser le cadre européen de la protection des données à caractère personnel, de prendre en compte les avancées technologiques et d'harmoniser les législations des États membres de l'Union européenne. En pratique, il vise à renforcer les droits des personnes, notamment par la création de droits à la limitation, à l'oubli, à la portabilité des données à caractère personnel et par la création de dispositions propres aux personnes mineures [472] ; responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants); favoriser la régulation grâce à une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des sanctions renforcées et des décisions communes concernant des traitements transnationaux. Dans le prolongement de la directive 95/46, le RGPD vient réaffirmer des principes essentiels (traitement licite et loyal, sur la base du consentement donné suite à l'information sur les finalités du traitement et le droit d'exercer le droit d'accès, de rectification, d'effacement). Cependant les droits des personnes sont d'une part renforcés[473] (A), et d'autre part apparaissent des mesures nouvelles de conformité afin de tenir compte de l'évolution technologique et de ses enjeux[474] (B).

A. Le renforcement des droits existants et l'élaboration des nouveaux droits

69 Le droit à l'information. Reprenant la directive 95/46/CE, le RGPD organise une régulation des données à caractère personnel en dotant les personnes concernées de droits

---

472 N. MARTIAL-BRAZ, « Les nouveaux droits des personnes concernées, Droit des personnes concernées, Droit à la mort numérique, mineurs, consentement,Droit à l'information, Droit de rectification, Droit à l'effacement, Droit à l'oubli numérique, Droit à la portabilité », *Revue des affaires européennes*, Bruylant, 2018, p. 7 ets.

473 Il y a des incontestables progrès qui se traduisent dans le texte par une meilleure information des personnes ; le consentement au traitement des données de la part de l'intéressé est renforcé en prévoyant qui doit être explicite, il est précisé que ce consentement ne sera pas présumé (pas de consentement tacite), une autre avancée concerne l'introduction de garanties pour les données relatives aux mineurs; le renforcement du droit à l'effacement, par ailleurs le droit à l'oubli numérique aidera les citoyens à mieux gérer les risques liés à la protection des données en ligne, en demandant leurs suppression les concernant si aucun motif légitime justifie leur conservation. De même le droit d'accès est amélioré, ainsi que le transfert des données d'un prestataire de service à l'autre (droit à la portabilité); l'interdiction de mesures fondées sur le profilage; une meilleure protection des données sensibles. Une exception au consentement est constituée par la réalisation de l'intérêt légitime du Responsable de traitement.

474 Le texte du règlement n. 2016/679 a été publié le 4 mai 2016 sur le *Journal officiel de l'Union européenne* et il sera applicable à partir du 25 mai 2018.

fondamentaux leur permettant d'interagir avec le responsable du traitement. Les articles 13 et 14 du RGPD renforcent le devoir d'information lorsque les données sont collectées auprès de la personne, sauf si la personne concernée dispose déjà des informations visées. Reprenant le cadre légal existant, le règlement prévoit que l'information donnée doit permettre d'identifier le responsable du traitement et/ou son représentant, l'éventuel délégué à la protection des données (ci-après DPO), le fondement juridique du traitement en sus de ses finalités ou les intérêts légitimes sur lesquels se fonde le responsable. Une autre information qui doit être portée à l'attention de la personne concernée porte sur la volonté d'effectuer un transfert de données vers un destinataire d'un pays tiers ou d'une organisation internationale, l'absence de décision d'adéquation du niveau de protection ou encore, le cas échéant, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition. Le responsable de traitement, lors du rappel des droits des personnes doit également faire référence aux nouveaux droits consacrés par le RGPD, à savoir le droit à la portabilité des données, le droit de retirer son consentement à tout moment et le droit d'introduire une réclamation auprès d'une autorité de contrôle. La nature obligatoire ou facultative éventuelle de la collecte donne lieu à une plus grande précision du caractère de l'information (caractère réglementaire, contractuel ou sur la base du consentement de l'exigence de fourniture des données). Le responsable de traitement doit également, le cas échéant, informer de l'existence d'une prise de décision automatisée comprenant un profilage ainsi qu'une information significative de la logique sous-jacente et les conséquences du traitement pour la personne[475]. Enfin, le responsable de traitement doit informer les personnes concernées d'un éventuel changement de finalités par rapport à la finalité initiale. L'article 14 du RGPD renforce également le devoir d'information lorsque les données n'ont pas été collectées auprès de la personne, tout en élargissant dans le même temps les exceptions générales. Il précise aussi que le responsable doit fournir les informations susmentionnées à la personne concernée soit dans un délai raisonnable qui n'excède pas un mois après la collecte - soit, s'il est envisagé de communiquer les informations à un autre destinataire ou d'utiliser les données pour une communication à la personne concernée, au plus tard lorsque les informations sont communiquées pour la première fois. Cependant, l'information ne doit pas être fournie si la personne dispose déjà des informations ou si cette transmission s'avère impossible ou nécessiterait des efforts disproportionnés. Une autre exception est prévue dans le cas où l'obtention ou la communication des informations fait l'objet de dispositions spécifiques dans le droit de l'Union ou dans la législation nationale ou si les données doivent rester confidentielles, sujettes à une obligation de secret professionnel conformément à la législation de l'Union ou d'un État membre, en ce compris d'origine statutaire.

70 Le consentement. Le règlement européen renforce notamment l'obligation de recueillir le consentement de la personne concernée par le traitement [476] car il incarne en effet le contrôle de la personne sur le devenir de ses données. Ainsi, le consentement est défini comme « toute manifestation de volonté, libre, spécifique, informée et non ambigüe par

475 Voy. le Règl. (UE) 2016/679, article 22 et 4.

476 Voy. le Règl. (UE) 2016/679, article 7.

laquelle la personne concernée accepte, par une déclaration ou par un acte positif univoque, que des données à caractère personnel la concernant fassent l'objet d'un traitement »[477]. La personne concernée par le traitement doit donc donner son consentement par un acte positif libre, spécifique éclairé et univoque[478]. La charge de la preuve du consentement repose sur le responsable de traitement[479]. Si le consentement de la personne concernée est requis dans le contexte d'une déclaration écrite qui concerne également d'autres questions, la demande relative au consentement doit être présentée sous une forme qui la distingue clairement de ces autres questions, d'une façon compréhensible et facilement accessible, en des termes clairs et simples. Cette nouvelle règle implique que le consentement à des conditions générales contenant une acceptation de traitement ne suffit pas. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement préalablement donné. Le retrait ne permet donc pas d'invalider le traitement antérieur au retrait et ne vaudrait dès lors que pour le traitement futur. La personne concernée doit en être informée avant de donner son consentement.

71 La qualité des données. La qualité des données à caractère personnel est mesurée par trois grands principes : la minimisation, l'exactitude et la mise à jour des données collectées. Le principe de minimisation des données, ou « limitation des données au minimum » est le principe selon lequel des données à caractère personnel ne peuvent faire l'objet d'un traitement que si, et pour autant que, les finalités du traitement ne peuvent être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel. Il consiste à : s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les finalités recherchées par le traitement ; si le traitement de données à caractère personnel s'avère nécessaire, limiter le traitement des données au minimum, en ce qui concerne les catégories de données traitées, le volume ou la quantité de données traitées, la question de savoir si les données collectées sont plus ou moins nécessaires au traitement. Au nom de ce principe, les données collectées doivent êtres adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées.

---

477 Voy. le Règl. (UE) 2016/679, art. 4, § 1.

478 Le consentement est considéré comme libre lorsqu'il peut être retiré à tout moment. Selon les termes du RGPD, « il est aussi simple de retirer que de donner son consentement ». Ainsi, la personne doit disposer d'une réelle liberté de choix et ne pas subir de contraintes de la part du responsable de traitement. A cet égard, un consentement ne sera présumé avoir été donné librement lorsqu'il existe entre la personne concernée et le responsable de traitement un lien de subordination ; Le consentement est spécifique lorsque a été donné pour un traitement déterminé, dont la finalité a été correctement détaillée par le responsable de traitement. L'objectif du législateur européen est d'éviter un consentement « trop général » qui permettrait au responsable de traitement de le réutiliser pour justifier des traitements ultérieurs ; Le consentement est éclairé la personne doit avoir reçu une information préalable. Celle-ci doit être complète et délivrée de façon claire et intelligible. Elle n'est ainsi pas « noyée » dans des conditions générales. En pratique, le responsable de traitement a tout intérêt à fournir une déclaration de consentement comportant l'ensemble des informations requises à faire accepter par la personne concernée ; Le consentement est univoque lorsque la procédure utilisée pour recueillir le consentement de la personne ne doit laisser aucun doute quant à l'octroi du consentement (accord écrit de la personne, etc.) A cet égard, le responsable de traitement doit veiller à se préconstituer des preuves afin de certifier que le consentement a été recueilli dans les conditions prévues par le RGPD.

479 Voy. le Règl. (UE) 2016/679, art. 7, § 1.

72 Les droits préexistants. Le droit d'accès. La personne concernée a le droit de demander au responsable du traitement si ses données font ou non l'objet d'un traitement et lorsqu'elles le font de se voir communiquer toutes les informations précitées (finalité du traitement, catégories de données concernées, destinataire des données, l'existence d'un transfert hors UE, etc.). Ce droit n'est toutefois pas absolu. Le responsable du traitement peut en effet s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique.

En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe néanmoins au responsable de traitement. La personne concernée a le droit d'obtenir du responsable de traitement, dans les meilleurs délais, la rectification des données personnelles la concernant qui sont inexactes. Compte tenu des finalités du traitement, la personne concernée a en outre le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire. Le RGPD accorde à la personne concernée un droit de s'opposer à tout moment à un traitement de données à caractère personnel la concernant. Cependant ce droit n'est pas absolu et un motif légitime devra être avancé par la personne qui souhaite se prévaloir de ce droit. Trois fondements conditionnent l'exercice du droit d'opposition : la personne concernée ne pourra s'opposer au traitement que lorsqu'il est fondé sur l'exécution d'une mission d'intérêt public, sur des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, sur des traitements à des fins de prospection.

Le responsable de traitement ne pourra plus traiter les données à caractère personnel de la personne ayant actionné ce droit, à moins qu'il ne démontre qu'il existe des motifs légitimes et impérieux pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.480

73 Les nouveaux droits. Le droit à la portabilité, le droit à la limitation et d'opposition. Le RGPD étend considérablement le droit des personnes concernées. Ces droits élargis sont généralement caractérisés par un plus grand contrôle de leur part sur leurs données et une meilleure compréhension de leur utilisation. Le règlement renforce les principes qui doivent guider le responsable dans le traitement en prévoyant un droit à la limitation du traitement[481], le traitement de données personnelles est limité à ce qui est nécessaire au regard de ses objectifs et l'accès aux données est restreint aux seules personnes compétentes. Lorsqu'un traitement est frappé d'une demande de limitation valable, les données à caractère personnel ne peuvent plus être traitées, à l'exception de la conservation. L'art. 18.1 du RGPD ouvre aux personnes concernées le droit de solliciter la limitation du traitement de leurs données, dans les quatre cas suivants : l'exactitude des données à caractère personnel est contestée par la personne concernée pendant une durée permettant au responsable du traitement de vérifier l'exactitude des données à caractère personnel. Ce cas est commun avec le droit à rectification : la limitation permet ici à la personne concernée de restreindre les conséquences néfastes d'un traitement de données inexactes, en en réduisant les effets au minimum, les données sont conservées le temps nécessaire à l'instruction de sa demande de rectification auprès du responsable de traitement ;

480 Voy. le Règl. (UE) 2016/679, art. 21.

481 Voy. le Règl. (UE) 2016/679, art. 18.

le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation. Ce cas correspond à une hypothèse dans laquelle le droit à l'effacement est également applicable : le droit à la limitation permet à la personne concernée d'éviter la destruction de ses données et d'obtenir ainsi leur conservation. Ex: données sensibles qui auraient été collectées en dehors des exceptions autorisées par l'art. 9.2 du RGPD, mais que la personne souhaiterait conserver pour les utiliser ultérieurement ; le responsable de traitement n'a plus besoin des données à caractère personnel aux fins du traitement, mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice, la défense de droits en justice ; la personne concernée s'est opposée au traitement, en vertu de l'art.21§1, pendant la vérification des motifs légitimes poursuivis par le responsable du traitement (sur le points de savoir s'ils prévalent sur ceux de la personne concernée). Les cas c) et d) sont également communs au droit à l'effacement : Dans le cas c) l'exercice du droit à la limitation est d'autant plus intéressant que l'effacement est exclu pour les données dont le traitement est « nécessaire à la constatation, à l'exercice ou à la défense de droits en justice ». Dans le cas d) le droit à la limitation permet de diminuer les effets d'un traitement dès l'envoi d'une demande d'opposition et de ne pas en subir les conséquences néfastes le temps de l'examen de cette demande. Un nouveau droit est prévu à l'art. 20[482], il s'agit du droit à la portabilité de ses données. En pratique il s'agit du prolongement du droit d'accès et consiste dans la possibilité d'obtenir auprès du responsable de traitement une copie des données faisant l'objet du traitement automatisé dans un format électronique structuré et de transférer les propres données à un nouveau responsable du traitement, (si l'on pense à la personne concernée qui veut changer de service *provider* pour le service email, services bancaires online etc.). Les traitements concernés par le droit à la portabilité sont limités par des conditions de forme et de fond. En effet, sont visés uniquement les traitements effectués à l'aide de procédé automatisés et son exclus les traitements non automatisés (les traitements manuels). Sur le fond, sont visés les traitements fondés sur le consentement de la personne concernée ainsi que ceux qui sont nécessaires à l'exécution d'un contrat conclu entre cette dernière et le responsable de traitement. Il est donc possible de distinguer un régime applicable pour les traitements « choisis » (fondés sur l'exécution d'un contrat et sur le consentement) et exclus pour les traitements « subis » (fondés sur la nécessité comme la sauvegarde des intérêts vitaux, le respect d'une obligation légale).

Le RGPD introduit le droit de s'opposer au profilage. Le RGPD définit le profilage comme toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant son rendement au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses déplacements[483].

---

482 Voy. l'art. 20, les personnes concernées ont le droit de recevoir les données à caractère personnel qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, ainsi que le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.

483 Voy. le Règl. (UE) 2016/679, art.4.

Le règlement n'interdit pas le profilage mais l'encadre en prévoyant des garanties pour les personnes concernées par ce type de traitement. Ainsi, est prévu le droit pour la personne d'être informée de l'existence d'un profilage. Les informations doivent aussi porter sur la logique sous-jacente, ainsi que sur l'importance et les conséquences prévues de ce traitement pour la personne concernée[484]. Dans son article 22, le règlement consacre en outre le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, qui produit des effets juridiques vis-à-vis de la personne ou qui l'affecte de manière significative de façon similaire. En pratique, ces dispositions ont vocation à éviter que les responsables du traitement ne procèdent à un examen de la situation individuelle d'une personne et ne fondent leurs décisions que sur la seule consultation de fichiers de données personnelles en leur possession, sans permettre à l'intéressé de présenter ses observations le cas échéant. Le règlement prévoit une dérogation à ce principe dans trois cas : le profilage est prévu par la loi ; il est nécessaire à la conclusion ou à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ; il repose sur le consentement de la personne concernée.

Le profilage ne doit en effet pas aboutir à une discrimination fondée sur l'utilisation ou la production de données « sensibles », relatives à la « race ou à l'origine ethnique, aux opinions politiques, à la religion ou aux croyances, à l'appartenance syndicale, la santé, la génétique, l'orientation ou l'identité sexuelles[485] ». Deux exceptions à cette dernière règle sont néanmoins prévues par l'article 22, par le biais d'un renvoi à l'article 9, 2, a) et g) : la personne concernée a donné son consentement explicite ; le traitement est nécessaire pour des motifs d'intérêt public.

Ainsi, le profilage est autorisé dans la mesure où les principes de licéité sont respectés, à savoir si la personne en est informée et peut s'y opposer. La réalisation d'une étude d'impact est requise en cas de profilage lorsque celui-ci produit des effets juridiques à l'égard d'une personne ou l'affecte significativement.

L'article 35, 3, a) dispose en effet que l'analyse d'impact relative à la protection des données visée au paragraphe 1 est, en particulier, requise dans les cas suivants : « L'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, qui est fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ».

74 Le droit à un recours effectif. Outre le droit de porter plainte auprès de l'autorité de contrôle, les individus doivent avoir le droit à un recours juridictionnel effectif et à saisir les tribunaux. Le droit à un recours juridique est bien inscrit dans la tradition juridique européenne et est reconnu comme un droit fondamental, à la fois en vertu de l'article 47 de la Charte des droits fondamentaux de l'Union européenne.

En vertu de la législation de l'Union, il est clair que les deux dispositions du RGPD, qui consacre le droit à un recours juridictionnel effectif contre les autorités de contrôle, les contrôleurs et processeurs et de la jurisprudence de la CJUE.

---

484 Voy. le Règl. (UE) 2016/679, art. 13.

485 Voy. le Règl. (UE) 2016/679, art. 22.

Dans l'affaire *Schrems*[486], la CJUE a déclaré invalide la décision relative à l'adéquation de la sphère de sécurité *Safe Harbor*. Cette décision avait permis des transferts de données internationaux de l'Union vers des organisations américaines qui se sont auto-certifiées dans le cadre du programme *Safe Harbor*. La CJUE a estimé que le programme *Safe Harbor* présentait plusieurs lacunes, compromettant les droits fondamentaux des citoyens de l'UE à la protection de la vie privée, à la protection des données à caractère personnel et au droit à un recours juridique effectif. Concernant la violation des droits à la vie privée et à la protection des données, la CJUE a souligné que la législation américaine autorisait certaines autorités publiques à accéder aux données personnelles transférées des États membres aux États-Unis et à les traiter de manière incompatible avec leur finalité initiale et au-delà de ce qui était strictement nécessaire et proportionné à la protection de la sécurité nationale. En ce qui concerne le droit à un recours effectif, elle a constaté que les personnes concernées n'avaient aucun moyen de recours administratif ou judiciaire pour permettre l'accès aux données les concernant, leur rectification ou leur effacement, selon le cas. La CJUE a conclu que la législation ne prévoyant aucune possibilité de recours juridictionnel pour accéder, rectifier ou effacer leurs données personnelles « ne respecte pas l'essence du droit fondamental à une protection juridictionnelle effective, consacré par l'article 47 de la Charte ».

Ainsi lorsqu'un responsable du traitement ou un sous-traitant viole les droits d'une personne, la personne concernée a le droit de porter plainte devant un tribunal[487]. La personne concernée par le traitement des données peut choisir de saisir le tribunal dans l'État membre dans lequel le responsable du traitement ou le sous-traitant a un établissement, ou en alternative dans l'État membre dans lequel la personne concernée a sa résidence habituelle. Cela lui permet de mener des actions dans l'État où ils résident et dans une juridiction familière. En effet, la limitation du lieu des procédures à l'encontre des contrôleurs et des procureurs de l'État membre dans lequel ceux-ci ont un établissement pourrait décourager les personnes résidant dans d'autres États membres d'intenter une action en justice. La seule exception concerne les cas où le contrôleur ou le sous-traitant sont des autorités publiques et où le traitement est effectué dans l'exercice de leurs pouvoirs publics. Dans ce cas, seuls les tribunaux de l'État de l'autorité publique concernée sont compétents.

Si, dans la plupart des cas, les affaires concernant les règles de protection des données seront jugées par les tribunaux des États membres, certaines affaires peuvent être portées devant la CJUE. La première possibilité est celle où une personne concernée, un responsable du traitement, une autorité de traitement ou de contrôle demande une action en annulation d'une décision du Comité européen. L'action est toutefois soumise aux conditions de l'article 263 du TFUE, ce qui signifie que, pour être recevables, ces personnes et entités doivent démontrer que la décision du conseil les concerne directement et individuellement.

Le second scénario concerne des cas d'institutions ou d'organismes de l'Union traitant illégalement des données à caractère personnel. Dans les cas où les institutions de l'Union enfreignent la loi sur la protection des données, les personnes concernées peuvent introduire une plainte directement devant le Tribunal de l'Union. Le Tribunal est en premier lieu responsable de plaintes d'infractions au droit de l'Union par les institutions de l'Union. Ainsi,

---

486 CJEU, Gr. Ch. C-362/14, Maximillian Schrems v. Data Protection Commissioner , 6 Octobre 2015.

487 Voy. le Règl. (UE) 2016/679, art 79.

les plaintes contre le Comité européen en tant qu'institution de l'Union peuvent également être portées devant le Tribunal[488]. Ainsi sous le régime de la directive 95/46 le Tribunal avait déjà eu à s'exprimer dans l'affaire *Bavarian Lager*[489]. Ici la société *Bavarian Lager*, a demandé à la Commission européenne de donner accès au procès-verbal intégral d'une réunion organisée par la Commission et portant apparemment sur des questions juridiques pertinentes pour l'entreprise. La Commission a rejeté la demande d'accès de l'entreprise pour des raisons de protection des données prépondérantes. *Bavarian Lager*, en vertu de l'article 32 du règlement sur la protection des données des institutions de l'Uninion, elle a porté plainte devant le Tribunal de première instance décision. Dans sa décision, le Tribunal de première instance a annulé la décision de la Commission de rejeter la demande d'accès. La Commission européenne a interjeté appel de cette décision devant la CJUE. La CJUE a rendu un arrêt (devant la Grande Chambre) annulant l'arrêt du Tribunal de première instance et confirmant le rejet par la Commission européenne de la demande d'accès au procès-verbal complet de la réunion afin de protéger les données personnelles des personnes. La CJUE a estimé que la Commission avait raison de refuser de divulguer ces informations, étant donné que les participants n'avaient pas consenti à la divulgation de leurs données personnelles. En outre, *Bavarian Lager* n'a pas démontré la nécessité d'accéder à ces informations. Par ailleurs, le RGPD permet aux individus de porter plainte auprès d'une autorité de contrôle ou d'intenter une action devant un tribunal par le biais d'un organisme, une organisation ou une association à but non lucratif[490]. Ces entités à but non lucratif doivent avoir des objectifs statutaires d'intérêt public et être actives dans le domaine de la protection des données. Elles peuvent porter plainte ou exercer un recours juridictionnel au nom de la ou des personnes concernées. Le règlement donne aux États membres la possibilité de décider, conformément au droit national, si un organisme peut porter plainte au nom de personnes concernées, sans être mandaté par ces personnes concernées. Ce droit de représentation permet aux individus de bénéficier de l'expertise et de la capacité organisationnelle et financière de ces entités à but non lucratif, facilitant ainsi grandement l'exercice des droits des individus. Cela profite également au fonctionnement et à l'efficacité du système judiciaire, car des réclamations similaires sont regroupées et examinées ensemble.

75 Le droit aux dommages-intérêts. Le droit à un recours effectif doit permettre aux individus de réclamer une indemnisation pour tout dommage subi du fait du traitement de leurs données personnelles d'une manière qui enfreint la législation applicable. La responsabilité des contrôleurs et des transformateurs en cas de traitement illégal est explicitement reconnue dans le RGPD[491]. Afin d'assurer la mise en œuvre de ce droit, le législateur a notamment prévu la possibilité de demander la réparation du préjudice[492] matériel ou moral éventuellement subi par

488 Voy. le Règl. (UE) 2016/679, art. 32 (3).

489 CJEU,Gr. Ch., C-28/08 P, European Commission c. The Bavarian Lager Co. Ltd 2010.

490 Voy. le Règl. (UE) 2016/679, art. 80.

491 Voy. le Règl. (UE) 2016/679, art.82.

492 Le considérant 75 du règlement 2016/679 donne à titre d'exemple les cas de discrimination, de vol ou d'atteinte à la réputation.

un traitement illicite des données personnelles[493]. A l'instar de l'ancien régime, cette obligation de réparer s'inscrit dans une logique de responsabilité conjointe (avec possibilité d'une action récursoire lorsqu'un seul des responsables est amené à réparer *effectivement* le dommage)[494]. Ainsi, « tout responsable du traitement ayant participé au traitement est responsable du dommage causé par le traitement qui constitue une violation du […] règlement ».
Le règlement donne aux individus le droit de recevoir une compensation du responsable du traitement ou du sous-traitant pour les dommages matériels et non matériels. Le préjudice doit être interprété de manière large à la lumière de la jurisprudence de la Cour de justice d'une manière qui reflète pleinement les objectifs du règlement [495] . Ainsi les exceptions à la responsabilité sont très strictes et soumises à la preuve que le responsable du traitement ou le sous-traitant n'est en aucun cas responsable de l'événement à l'origine des dommages.

76 Le cas particulier du droit à l'effacement ou droit à l'oubli. Avec le temps, nous avons pris conscience des dérives auxquelles mène la conservation infinie de nos données, la mémoire sans limite de ce juge virtuel intemporel met en péril nos droits fondamentaux, tels que la vie privée et la protection des données à caractère personnel. Ainsi « L'oubli est une quête juridique aussi difficile à atteindre que le bonheur »[496]. Dans la lignée de l'arrêt *Google Spain*[497] qui a introduit un droit au déréférencement pour les internautes[498], le RGPD consacre un droit à l'effacement nommé « droit à l'oubli »[499]. De plus, la doctrine et l'opinion publique y étaient

493 Voy. le Règl. (UE) 2016/679, Art. 82.

494 le Règl. (UE) 2016/679, Art. 82, §5.

495 Voy. le Règl. (UE) 2016/679, considérant 146.

496 J.-M. BRUGUIÈRE, *Le droit à l'oubli numérique, un droit à oublier*, D. (D.S.), 2014, p. 202.

498 Rappelons les faits : Un ressortissant espagnol, Mr Costeja Gonzáles, souhaitait d'une part voy. supprimées, ou à tout le moins modifiées, certaines informations publiées dans un journal espagnol, « La Vanguardia Ediciones », toujours disponibles sur le site du quotidien, et mentionnant son nom en lien avec une vente aux enchères immobilière. Cette dernière avait été pratiquée à son encontre en 1998, en recouvrement de dettes de sécurité sociale qui avaient depuis lors été payées. D'autre part, il demandait que ces informations soient supprimées ou occultées dans la liste des résultats obtenus après saisie de son nom sur le moteur de recherche Google. Le journal et Google ayant tous deux refusé d'accéder à sa demande, Mr Costeja Gonzáles s'est alors tourné vers l'Agence espagnole de protection des données (Agencia Española de Protección de Datos, ou « AEPD »), laquelle a refusé d'ordonner au quotidien la suppression des données, mais a, en revanche, accueilli la réclamation dirigée contre *Google Spain* et Google Inc. En effet, l'AEPD estimait que les exploitants de moteurs de recherche étaient soumis à la législation en matière de protection des données, « *étant donné qu'ils réalisent un traitement de données pour lequel ils sont responsables et qu'ils agissent en tant qu'intermédiaires de la société d'information* ». Considérant que les liens vers les pages *web* concernées du journal espagnol étaient susceptibles de porter atteinte au droit de la protection des données et au droit à la dignité au sens large dont jouit Mr Costeja Gonzáles, droits qui engloberaient également la simple volonté de la personne intéressée que ces données ne soient pas connues par des tiers, l'AEPD a dès lors ordonné à Google le retrait des liens de son moteur de recherche. Le groupe américain avait alors introduit un recours auprès de l'Audiencia Nacional pour contester cette décision. Le tribunal espagnol, avant de statuer, a saisi la Cour de plusieurs questions préjudicielles relatives à l'interprétation de la directive 95/46/CE, notamment sur la question du champ d'application territorial de celle-ci ainsi que sur l'existence d'un « droit à l'oubli numérique ».

499 Ce droit peut être exercé lorsque les données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées, lorsque le consentement qui fondait le traitement est retiré, lorsque le traitement de données n'est pas conforme au règlement, notamment parce que la durée de conservation a expiré ou quand la personne exerce son droit d'opposition. Cependant ce droit n'est pas absolu, des intérêts publics ou privés doivent être pris en compte et le responsable du traitement pourra y résister (en particulier pour des motifs tirés du respect de la liberté d'expression ou d'une obligation légale).

majoritairement favorables [500] . Face à la multiplication de données stockées sans limites techniques de temps, cette capacité d'oublier est fondamentale car « si la mémoire peut être précieuse, la capacité d'oublier est également fondamentale »[501]. Ainsi Nietzsche valorisait l'oubli contre la mémoire, soulignant le caractère délétère des souvenirs qui gênent la vie et empêchent l'individu de progresser[502]. Le droit à l'effacement existait déjà dans la directive 95/46 qui le mêlait au droit à la rectification[503]. Ce droit a connu un développement important avec l'arrêt *Google Spain*[504] rendu par la Cour de justice le 13 mai 2014. Le RGPD a consacré un article propre au droit à l'effacement car seule une intervention extérieure semble pouvoir garantir ce qui, hier, résultait encore d'un simple processus psychologique[505]. Ainsi au titre de l'article 17[506] du RGPD, les personnes concernées ont le droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant lorsqu'elles ne sont pas ou plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou la durée de conservation a expiré[507]. Cette disposition trouve sa source dans l'affaire *Google Spain*, dans laquelle la Cour a jugé que les personnes physiques sont en droit (sous réserve de certaines conditions et garanties) de demander à un moteur de recherche de supprimer les liens renvoyant à des données à caractère personnel les concernant. Cependant, le droit à l'oubli inscrit dans le RGPD va bien au-delà du déréférencement visé dans l'arrêt *Google* précité. L'innovation est dans le second alinea de l'art. 17, prévoyant une nouvelle obligation pour le responsable de traitement qui, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les tiers responsables qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces

---

500 N. MALLET-POUJOL, « Une forme d'embargo numérique est nécessaire pour ne pas sombrer dans la tyrannie de la transparence » *Légipresse* 2002, n° 297, p.510

501 J. LE RIDER, « Oubli, mémoire, histoire dans la deuxième considération inactuelle », *Revue germanique internationale*, mis en ligne le 21 septembre 2011.

502 Voy. Nietzsche, *La Généalogie de la morale*, Deuxième dissertation, p.803.

503 Voy. l'art. 12 b) de la directive 95/46.

504 CJUE aff. C-131/12,13 mai 2014.

505 J. DUPONT-LASSALE, « Beaucoup de bruit pour rien ? La précarité du droit à l'oubli numérique consacré par la Cour de justice de l'Union européenne dans l'affaire Google Spain », *Rev. trim. D.H.*, 2015, p. 989.

506 Il y a des similitudes avec les plus anciens droits d'effacement et droit d'opposition. Le numérique a ajouté un nouveau droit permettant d'obtenir la suppression des liens comportant des données personnelles, dans certaines circonstances auprès du responsable du traitement. D'autre part l'art 17.2 impose aux responsables du traitement ayant rendu publiques les données de prendre « des mesures raisonnables pour informer le responsable qui traitent telles données que la personne concernée ait demandé l'effacement de tout lien vers ses données ».

507 Au titre de l'art. 17 du RGPD la personne concernée a droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais de données à caractère personnel la concernant lorsque le traitement: Est illicite (dépourvu de fondement juridique valable) ; Les données ne sont plus nécessaires (la durée du traitement a expiré) ; Retrait du consentement (qui constituait le fondement juridique du traitement) ; Exercice du droit d'opposition (le demandeur doit justifier les raisons tenant à sa situation). Le droit d'opposition est ouvert uniquement lorsque le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique, soit aux intérêts légitimes poursuivis par le responsable du traitement ou par un tiers ». Sont donc exclus du droit d'opposition: Les traitements fondés sur le consentement des personnes, les traitements nécessaires à l'exécution d'un contrat, les traitements nécessaires à la sauvegarde des intérêts vitaux de la personne. Si elle est reconnue fondée, l'opposition entraine la cessation du traitement ce qui ne signifie pas que les données sont effacées. Ainsi la personne peut avoir intérêt à demander également l'effacement des données.

données à caractère personnel, ou de toute copie ou reproduction de celles-ci. L'exercice du droit à l'oubli relève de l'autonomie informationnelle[508].
Il est cependant relatif et suppose que soit effectué un contrôle de proportionnalité entre les intérêts de la personne concernée et ceux du responsable du traitement, ou, le cas échéant du public en général (droit à l'information ou intérêt historique) ainsi l'article 17 prévoit des limites lorsque le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information; pour respecter une obligation légale auquel le responsable du traitement est soumis, pour des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques conformément, à la constatation, à l'exercice ou à la défense de droits en justice. Ce droit, qui n'est pas reconnu outre atlantique, renforce plus encore la specificité de la conception européenne du droit à la protection des données à caractère personnel et son lien étroit avec le droit à la vie privée[509].

77 La consécration du droit à l'oubli par la Cour de justice. Le droit à l'oubli a été consacré bien avant l'adoption du RGPD par la Cour de justice dans l'affaire *Google Spain*[510] en se basant sur le cadre juridique offert par la directive 95/46[511] laquelle subordonne le droit à l'effacement et le droit d'opposition à la récurrence de certains conditions[512].
L'affaire *Google Spain* s'exprime, sur la question préjudicielle, d'interprétation des art. 12 et 14 de la directive 95/46/CE, ayant comme objet le droit d'accès aux données et le droit d'opposition. Selon la Cour de justice ces droits peuvent se faire valoir même vis-à-vis du moteur de recherche, considéré comme un responsable du traitement[513]. Le moteur de recherche ne pourra pas effacer les données personnelles qui se trouvent près du responsable du traitement qui a publié les informations (dans l'affaire *Google Spain* le journal en ligne espagnol *Vanguardia*) mais il est tenu d'effacer le lien qui permet d'accéder à l'article et aux données en question. Ainsi se réalisera un droit à ne pas être trouvé sur le web plutôt qu'un vrai droit à l'oubli [514] . La Cour de justice rappelle que ce droit à l'oubli répond au principe de

---

508 C. DE TERWAGNE, « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle? » In, D. Dechenaud (Dir.), *Le droit à l'oubli numérique*, Larcier, 2015, p. 35-50.

509 V. la décision de la Cour d'appel des États-Unis, 9e circuit, Garcia c/Google Inc., n°12-57302 (2015) :« Le droit à l'oubli, bien que récemment affirmé par la Cour de justice de l'Union européenne, n'est pas reconnu aux États-Unis ».

510 CJUE (Gr. Chambre), 13 mai 2014, *Google Spain* SL, Google Inc. C. Agencia Española de Protección de Datos, aff. C-131/12.

511 Ce cadre ne change pas avec le règlement, ainsi les conditions pour demander l'effacement des donnée sont: a) lorsque les données ne sont plus nécessaires aux buts pour lesquels ils ont été recueillis; b), la personne concernée révoque le consentement sur lequel il se fonde le traitement, ou la période autorisée de conservation des données a expiré et il n'existe pas un autre motif légitime pour traiter les données; c) la personne concernée s'oppose au traitement de données personnelles aux sens de l'article 19.

512 Lorsque le traitement avait lieu dans la violation de la loi ou en présence de motif légitimes.

513 L'objet du renvoi préjudiciel était le suivant: si la personne concernée peut se tourner directement vers le moteur de recherche au lieu du responsable qui a publié l'information (le journal en ligne).

514 La doctrine a parlé de « right not to find ». Voy. M. SIANO, « Il diritto all'oblio in Europa e il recente caso spagnolo », in F. PIZZETTI(a cura di), Giappichelli, Torino 2013, p. 34 ; F. PIZZTTI, *La decisione della Corte di Giustizia sul caso*

proportionnalité de tout traitement, selon lequel, le traitement doit respecter le principe de « qualité des donnés », c'est-à-dire qu'elles soient adéquates, pertinentes et non excessives à l'égard des finalités pour lesquelles ont été recueillies, ainsi que rectifiées et mises à jour[515], ou qu'elles soient conservées pendant une durée excédant celle nécessaire, à moins que leur conservation s'impose à des fins historiques, statistiques ou scientifiques[516].

Toutefois, un tel droit n'est pas absolu et doit être mis en balance avec d'autres droits. La Cour de justice s'efforce de trouver un équilibre en utilisant le principe de proportionnalité[517]. Ainsi elle considère que « s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans sa vie publique, que l'ingérence dans ses droits fondamentaux est justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question alors le droit à l'effacement ne s'applique pas »[518]. Il s'agit pour le moteur de recherche d'opérer lui-même un contrôle de proportionnalité entre les articles 7 et 8 de la Charte des droits fondamentaux et le droit d'information et d'expression[519] , contrôle notamment réservé au juge[520]. Le bien juridique que la Cour de justice a garanti est celui à l'identité informationnelle, le moteur de recherche peut créer une vraie image, identité de la personne online, qui peut s'avérer non véridique par rapport à la véritable identité de la personne et lui causer un préjudice. Il y a l'abandon de la conception de la vie privée comme un simple « *excludere alios* » en sens statique, ou un simple « *right to be let alone* », comme conçu originairement par Warren et Brandeis[521], mais il y a l'affirmation d'un mécanisme dynamique de contrôle et de circulation des données, expression de l'autonomie informationnelle[522].

Google Spain: più problemi che soluzioni, in Federalismi.it, n.1, 2014 ; F. PIZZETTI, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino, Giappichelli, 2016, p. 18.

515 Voy. Conclusions de l'avocat Général point 96.

516 Point 92 de l'arrêt.

517 J. LE CLAINCHE, « CJUE : le droit à l'oubli n'est pas inconditionnel », *RLDI*, 2014, n° 107.

518 Voy. les conclusions de l'Avocat général point 120: »La présente affaire concerne à bien des égards la liberté d'expression et d'information, consacrée à l'article 11 de la Charte, qui correspond à l'article 10 de la CEDH. L'article 11, paragraphe 1, de la Charte dispose que «toute personne a droit à la liberté d'expression. Ce droit comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières». Voy également Y. PADOVA et D. LEBEAU-MARIANNA, *Entre droit des données personnelles et liberté d'expression, quelle place pour les moteurs de recherche ?*, *RLDI*, février 2013, n° 90. Voy. Point 97 de l'arrêt Google Spain. La CJUE précise que même un traitement initialement licite de données exactes peut devenir, avec le temps, incompatible avec cette directive lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Tel est notamment le cas lorsqu'elles apparaissent inadéquates, qu'elles ne sont pas ou plus pertinentes ou sont excessives au regard de ces finalités et du temps qui s'est écoulé, voy. Point 93 de l'arrêt.

519 Y. PADOVA, D. LEBEAU-MARIANNA, « entre droit des données personnelles et liberté d'expression, quelle place pour les moteurs de recherche? », *RLDI*, 2013/90

520 Voy. la ligne guide du G29 concernant les suites à donner à, l'arrêt *Google Spain* et le droit au déréférencement, WP225, « Guidelines on the implementation of the Cour of Justice of the European Union judgment on *Google Spain* ».

521 S. WARREN, L. D. BRANDEIS, *The right of privacy*, in *Harvard Law Review*, 1890, p. 193.

522 A. BENSOUSSAN, *Le droit à l'oubli, un droit de l'homme numérique*, *Le Figaro*, 21 juillet 2014, disponilbe à l'adresse : http://blog.lefigaro.fr/bensoussan/2014/07/le-droit-a-loubli-un-droit-de-lhomme-numerique.html

78 Des difficultés terminologiques. « Droit à l'oubli », « droit à l'effacement », « droit au déréférencement » ou « à la désindexation », « droit à l'oubli numérique ». La doctrine, le juge et le législateur européen, notamment, se sont tous trois penchés sur la notion générale de « droit à l'oubli », et ont chacun apporté des nouveautés dans la terminologie employée[523].

La doctrine anglophone oppose le plus souvent les termes de « *right to forget* » à ceux de « *right to be forgotten* », désignant respectivement « *la revitalisation d'un fait du passé* », soit le droit à l'oubli judiciaire, et « *le droit à l'effacement des données* »[524]. Néanmoins, d'autres termes tels que « *right to oblivion* » ou « *right to erasure* » sont aujourd'hui abondamment présents dans les articles et ouvrages traitant du sujet, et maintiennent malgré tout une certaine forme de confusion dans l'emploi du vocabulaire[525].

Une première signification du droit à l'oubli est celle donnée par la doctrine avant l'arrivée d'Internet. Avec cette expression la doctrine se référait[526] au droit à ne plus voir publiées des informations sur des faits qui se sont passées depuis un certain laps de temps[527]. Par exemple, le « droit à l'oubli du passé judicaire » a été reconnu par la jurisprudence dans différents États membres sur base du droit à la vie privée ou des droits de la personnalité, comme le droit à la dignité ou à la réputation[528].

Dans cette acception, le droit à l'oubli est conditionné par l'écoulement du temps. Toutefois, le développement des technologies de l'information et de la communication a conduit à repenser le droit à l'oubli sous forme de droit à l'oubli numérique. En effet une fois sur Internet, l'information ne peut pas être effacée, mais elle peut ne plus être accessible au public. Ici on est face à un *continuum* temporel et l'oubli se justifie avec l'expiration de la finalité pour laquelle les données avaient été collectées. Dans un second sens, le droit à l'oubli n'est plus conditionné par l'écoulement du temps mais est lié à la finalité et la légitimité de détenir une information. Cette évolution du droit à l'oubli reconnaît ce droit comme composante de l'autodétermination informationnelle[529]. Cela consiste en la possibilité de contrôler ses propres

---

523 N. XANTHOULIS, *Conceptualising a Right to Oblivion in the Digital World: A Human Rights-Based Approach*, 14 mars 2016, p.8, disponible à l'adresse : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2064503

524 E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *Revue du droit des technologies de l'information 2013*, p. 78 ; R.H. WEBER, « The Right to Be Forgotten : More Than a Pandora's Box *? »*, *J.I.P.I.T.E.C.*, 2011, p. 120.

525 C. CASTETS-RENARD et W.G. VOSS, « Proposal for an International Taxonomy on the Various Forms of the « Right to Be Forgotten » : A Study on the Convergence of Norms », *Colorado Technology Law Journal*, 2016, n°14, pp. 281-344.

526 T. AULETTA, « Diritto alla riservatezza e « droit à l'oubli», in ALPA-BESSONE-BONESCHI-CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, pp. 127 e ss.

527 Le premier domaine couvert fait référence au droit subjectif à l'oubli du passé judicaire. Il s'agit donc de permettre à quiconque de demander à ce que des informations diffusées dans la presse, replaçant son passé judicaire sur le devant de la scène, soient retirées. Pour être qualifiée de « fautive », la diffusion des informations doit être appréciée au regard de son contexte factuel (l'information est-elle utile à la poursuite d'un intérêt contemporain ? contribue-t-elle à un débat public ? jouit-elle d'un caractère historique ? etc. Voy. : E. DEFREYNE, *Le droit à l'oubli et les archives journalistiques*, *op. cit.*, p. 3.

528 C. DE TERWANGNE, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion*, op. cit., p. 111.

529 C. DE TERWANGNE, « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle *? »*, In, D. DECHENAUD (Dir.), *Le droit à l'oubli numérique*, Larcier, 2015, p. 36. P. KORENHO, *Timing the Right to Be Forgotten: A Study into "Time" as a Factor in Deciding About Retention or Erasure of Data*, mai 2014, p. 5. Disponible à l'adresse : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436436. Cela suppose concrètement de pouvoir demander au responsable

informations personnelles puisqu'avec son *eternity effect* [530] , Internet conserve toutes les informations sans limite dans le temps comme résumé par l'expression de la Commissaire à la justice Viviane Reding : « Dieu pardonne et oublie, mais le web jamais »[531]. Il ne s'agit pas d'effacer le passé mais c'est une question de décontextualisation des informations qui ne sont plus pertinentes mais qui remontent à la surface par les moteurs de recherche.

Avec l'expression « le droit à l'oubli numérique », le doctrine se réfère à l'article 17 de la proposition de règlement général de protection des données publiée en janvier 2012[532]. « Le droit à l'effacement » est la dénomination retenue par le Parlement et le Conseil pour ce même article 17 du nouveau règlement général.

Le « droit au déréférencement » ou « à la désindexation » se réfère au droit prétorien consacré par la Cour de justice de l'Union européenne dans son arrêt du 13 mai 2014, dit « arrêt *Google Spain* »[12]. Il permet aux individus de demander à ce que certaines données les concernant, obtenues par la saisie de mots clefs (leur nom et prénom par exemple) dans un moteur de recherche, soient retirées de la liste des résultats affichés. L'information n'est donc pas supprimée à la source, mais elle est rendue pratiquement introuvable[533].

79 Le débat sur l'existence d'un nouveau droit. Le débat en doctrine a donc porté sur l'existence d'un nouveau droit[534]. Sans rentrer trop dans le débat, il semble que le droit à l'oubli ne constitue pas un droit en soi du moment où il joue un rôle dans la concrétisation du droit à l'identité[535]. D'un point de vue méthodologique il ne s'agit pas d'un nouveau droit car les droits déjà existants et consolidés sont capables de l'englober (finalité du traitement, droit d'opposition, d'effacement) [536] . Il s'agirait donc d'un droit de maîtrise des informations

---

du traitement des données à ce que les données en question soient effacées, mais également de demander d'en interdire l'accès et l'utilisation aux tiers.

530 S. WALTZ, *Relationship between the freedom of the press and the right to informational privacy in the emerging Information Society*, 19eme Conférence international des commissaires à la protection des données, Bruxelles, 17-19 septembre 1997, p. 3.

531 V. REDING, *Why the EU needs new personal data rules ?*, The European Data Protection and Privacy Conference, Bruxelles, 30 novembre 2010, disponible à l'adresse : file:///Users/flavia/Desktop/SPEECH-10-700_EN.pdf.

532 Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère et à la libre circulation de ces données (règlement général sur la protection des données), *C.O.M.* (2012) 11 final, p. 57. *Voy*. également le commentaire de P. DE HERT et V. PAPKONSTANTINOU, « The proposed data protection Regulation replacing Directive 95/46/EC : A soundsystem for the protection of individuals », *Computer Law & Security Review*, 2012, pp. 130-142.

533 Récemment, G. VOSS et C. CASTETS-RENARD ont publié une étude proposant une taxonomie internationale reprenant les différentes formes du droit à l'oubli. Voy. : C. CASTETS-RENARD et W.G. VOSS, *Proposal for an International Taxonomy on the Various Forms of the « Right to Be Forgotten » : A Study on the Convergence of Norms*, *Colorado Technology Law Journal*, 2016, n°14, pp. 281-344.

534 Certains auteurs n'avaient pas hésité à définir ce droit comme un droit de troisième génération VOY. Y POUILLET, *le fondement du droit à la protection des données personnelles : propriétés ou libertés, in Nouvelles technologies et propriété*, Paris, Litec, 1992.

535 Voy, sur cet aspet, S. RODOTA, « Persona, riservatezza, identità. Prime note sistematiche sulla protezione dei dati personali », *in Rivista critica del diritto privato*, 4, 1997, pp. 583 ss. et V. ZENO ZENCOVICH, « Diritti della Personalità » , in Digesto delle Discipline Privatistiche - Sez. civile, vol. XIII, Utet, Torino, 1995, p. 431 et s.

536 M. C. FONTAINE, « Le droit à l'oubli » avec R. AMARO, *in La proposition de règlement européen relatif aux donnèes à caractèr personnel: Proposition du rèseau Trans Europe Experts N. Martial- Branzet f. Terryn (dir)*, coll. TEE-SC, tome 54, 2014, p. 422 et s.

personnelles[537], un droit à ne pas voir méconnu son droit à l'identité personnelle[538]. D'ailleurs il a été parfois présenté comme un « intérêt légitime à oublier et à se faire oublier »[539] plutôt qu'un véritable « droit »[540].

Ainsi selon une partie de la doctrine le concept trouve ses racines dans la mise en œuvre des principes de proportionnalité et de « limitation de la finalité »[541]. Selon une autre partie de la doctrine, le concept de droit à l'oubli est intégré au « droit d'opposition », lequel permet de demander à « bloquer l'utilisation des données »[542].

Au-delà du débat doctrinal, comme souligné : « l'autodétermination informationnelle » et « le rôle déterminant de la volonté de l'individu » sont au cœur de cette version moderne du droit à l'oubli[543]. L'identité est l'ensemble des différents éléments, elle n'est certainement pas une synthèse statique, le temps joue un rôle essentiel : l'identité change avec le temps. Dès lors, selon la Cour de justice, si les conditions prévues par la directive 95/46 sont effectivement satisfaites, l'exploitant d'un moteur de recherché est tenu de supprimer de la liste de résultats (affichées à la suite d'une recherche effectuée à partir du nom d'une personne) des liens vers des pages Web, publiées par des tiers et contenant des informations relatives à cette personne[544].

La Cour de justice affirme ici un droit à l'oubli numérique en se fondant d'une part sur le droit de rectification (article 12b) et d'autre part sur le droit à l'effacement et d'opposition (fondé sur l'article 14a) de la directive 95/46[545]. L'affirmation selon laquelle le droit à l'oubli serait un nouveau droit doit être nuancée puisque ce droit n'est accordé que dans certains cas limitativement énumérés et qui ne sont pas nouveaux. L'art. 12b de la directive 95/46 reconnaissait déjà un droit à la rectification, à l'effacement ou au verrouillage des données dont le traitement n'est pas conforme à la directive, notamment en raison du caractère incomplet ou inexact des données. Il est possible de conclure que le RGPD a simplement précisé ces droits.

Un autre débat concerne le champ d'application territorial du droit à l'oubli. En effet l'autorité

---

537 D. GUTMAN fut l'un des premiers à proposer ce droit de contrôle sur les informations personnelles. Voy.. D. GUTMAN, « Le sentiment d'identité », coll. Bibl. dr. Privé, Paris, *LGDJ*, 2000, p. 9 ss. Voy. aussi sur ce point L.L. CHRISTIANIS, « Dimensions philosophiques et religieuses des approches juridiques de l'identité », in J.POUSSON-PETIT, *L'identité de la personne humaine. Étude de droit français et de droit compare*, Bruxelles, 2002, 63, p. ss.

538 G. RESTA, *Autonomia privata e diritti della personalità*, Napoli, 2005, p. 166.

539 A. ROUVROY, « Réinventer l'art d'oublier et de se faire oublier dans la société de l'information », version augmentée du chapitre paru dans *La sécurité de l'individu numérisé – Réflexions prospectives et internationales*, Paris, L'Harmattan, 2008, p 25.

540 C. DE TERWANGNE, *Droit à l'oubli, droit à l'effacement ou droit au déréférencement* ?, *op. cit*., p. 246; C. DE TERWANGNE, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion, op. cit*., p. 113.

541 C. DE TERWANGNE, *Droit à l'oubli, droit à l'effacement ou droit au déréférencement* ? *op. cit.*, p. 246 ; C. DE TERWANGNE, *Internet Privacy and the Right to Be Forgotten/Right to Oblivion , op. cit.*, p. 113.

542 S. SIMITIS, « Collected courses of the Academy of European Law », Vol. VIII, n° 1, *The Hague, Kluwer Law International*, 1997, p. 130.

543 C. DE TERWANGNE, *Droit à l'oubli, droit à l'effacement ou droit au déréférencement ?, op. cit.*, p. 247.

544 C. CASTETS-RENARD, « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *RLDI*, 2014, n° 106, p. 68-75.

545 CJUE, *Google Spain* SL, Google Inc. C. Agencia Española de Protection de Datos, Mario Costeja Gonzales, aff. C-131/12, 13 mai 2014, §76.

de contrôle française (la CNIL) a jugé nécessaire d'étendre le droit à l'oubli à l'extension *google.com* et non seulement à *google.fr*. Les décisions de la CNIL sur le droit à l'oubli ont fait l'objet d'un appel devant le Conseil d'État [546] . D'ailleurs, la mise en œuvre du droit au déréférencement dans les affaires qui étaient soumises au Conseil d'État soulevait plusieurs difficultés sérieuses relatives à la portée de la directive européenne du 24 octobre 1995 sur la protection des personnes physiques à l'égard des traitements de données à caractère personnel, après la première interprétation donnée par la Cour de justice de l'Union européenne dans son arrêt Google Spain. Avant de statuer sur ces affaires, le Conseil d'État a donc décidé de saisir cette cour de plusieurs questions préjudicielles.

B. Les nouvelles mesures de conformité

La logique du RGPD développe une approche pragmatique en matière de protection des données personnelles. Abandonnant la logique déclarative issue de la loi informatique et libertés, le RGPD s'appuie sur une responsabilisation (*accountability*) des acteurs traitant des données qu'il s'agisse d'entreprises ou d'entités publiques responsables de traitements mais également de fournisseurs de solutions informatiques permettant la mise en œuvre effective de ces traitements. Ceux- ci devront à tout moment assurer une protection optimale des données et être en mesure de démontrer la conformité de leur traitement, ce qui implique de documenter cette conformité[547], ainsi le RGPD impose, dans certains cas aux responsables de traitement et aux sous-traitants de tenir un registre [548] des activités de traitement effectuées sous leur responsabilité. Cela en raison de la suppression de l'obligation de notification préalable des traitements à l'autorité de contrôle nationale toutefois, le RGPD impose des nouvelles obligations au responsable du traitement et au sous-traitant ; on passe d'une approche formelle et déclarative à une approche d'autorégulation et de responsabilisation des acteurs, il y a un passage d'une logique formelle à un logique de conformité substantielle[549]. Concrètement, le

546 Plusieurs requérants ont saisi le Conseil d'État de recours dirigés contre les décisions par laquelle la Commission nationale de l'informatique et des libertés (CNIL) a clôturé leurs plaintes tendant au déréférencement de résultats obtenus à la suite de recherches effectuée à partir de leurs noms sur le moteur de recherche Google.

547 L'obligation de documenter pesant sur les responsables de traitement et les sous-traitants est prévue aux articles 28, § 3, a), 30, § 1, e), 30, § 2, c), 33, § 5 et 49, § 6) du règlement. Le responsable de traitement doit adopter des procédures internes formalisées, diligenter des audits et créer des études d'impact afin de garantir, et pouvoir démontrer en cas de contrôle, la conformité des procédures de l'entreprise à la réglementation Sécuriser les données personnelles contre tout traitement non autorisé ou illégal, mais aussi contre la perte accidentelle, la destruction ou l'altération des données personnelles, en mettant en œuvre des mesures de sécurité physique, technique et organisationnelle appropriées.

548 Le registre doit, conformément à l'article 30 du RGPD, comporter les informations suivantes : Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ; Les finalités du traitement ; Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ; Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ; Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou vers une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, et les documents attestant de l'existence de garanties appropriées ; Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ; Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

549 Le RGPD introduit le principe de responsabilité solidaire entre responsable du traitement et sous-traitant (art. 82.4). La victime peut demander la réparation de l'intégralité du dommage soit au responsable de traitement soit au sous-responsable.

responsable de traitement doit établir le registre de traitements (art. 28) et dans certains cas réaliser une analyse d'impact [550] pour les traitements à risque et désigner un délégué à la protection des données[551]. Au titre de l'art 35 du RGPD, certains traitements sont soumis à une analyse d'impact obligatoire. De plus, le responsable de traitement sera dans l'obligation de consulter l'autorité de contrôle si le résultat de cette analyse révèle un « risque élevé » pour les droits et la vie privée de la personne. De plus le RGPD impose la tenue du registre des traitements recensant les traitements des données à caractère personnel. Une mesure d'*accountability* est prévue à l'art. 40 et 41 du RGPD et consiste dans l'adhésion à des codes de conduite et certifications[552].

80 La désignation d'un DPO. Le « Data protection Officer » (ci-après) DPO a vocation à remplacer l'actuel Correspondant Informatique et Libertés (CIL)[553].
Présenté comme le gardien du RGPD, il a vocation à s'assurer du respect des obligations mises à la charge des responsables du traitement et des sous-traitants par le RGPD et de piloter la mise en œuvre de l'ensemble des *process* dédiés à la conformité juridique des traitements. Aux termes de l'article 37 du RGPD, les responsables de traitement et les sous-traitants devront obligatoirement désigner un délégué s'ils appartiennent au secteur public[554] ; si leurs activités de base (principales) les amènent à réaliser un suivi régulier et systématique des personnes à

Lorsque l'une des parties a réparé l'intégralité du préjudice, celle-ci dispose ensuite d'un recours contre son cocontractant à la hauteur de sa part de responsabilité dans le dommage. Il est souligné comme la responsabilité solidaire est valable uniquement si les parties sont toutes responsables du manquement à l'origine du dommage: cela ne devrait pas arriver si, dans leur contrat, celles-ci définissent clairement les rôles et responsabilités de chacune d'entre elles. Dans ce cas, chaque partie est seule responsable du dommage généré par un manquement aux obligations dont elle a la charge, et endosse seule cette responsabilité vis-à-vis d la victime.

550 Voy. Règl. (UE) 2016/679, consid. 76 et art. 35, § 1. Les analyses d'impact relatives à la protection des données deviendront obligatoires « lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement » pourra « engendrer un risque élevé pour les droits et libertés des personnes physiques ». Constitue notamment un risque élevé « l'évaluation systématique et approfondie d'aspects personnels », « le traitement à grande échelle » de données sensibles « ou de données à caractère personnel relatives à des condamnations pénales et à des infractions » et « la surveillance systématique à grande échelle d'une zone accessible au public".

551 Le groupe de travail « Article 29 » (G29), composé de représentants des autorités de protection des données des États membres de l'UE, a publié des lignes directrices sur le rôle des délégués à la protection des données et a fourni des recommandations concernant les bonnes pratiques. Si un délégué à la protection des données est désigné, l'organisation est tenue de publier les informations relatives au délégué à la protection des données et de les communiquer à l'autorité de contrôle compétente.

552 Le code de conduite est élaboré par les associations ou autres organismes représentant des catégories de responsables du traitement ou de sous-traitant puis soumis à l'autorité de contrôle compétente, qui rend un avis il est positif donne lieu à la publication du code de conduite. Lorsque le code concerne des traitements transfrontaliers, l'autorité de contrôle saisie soumettra le projet au CEDP qui rendra un avis adressé à l'autorité de contrôle national, qui s'il n'est pas suivi par l'autorité donnera lieu à une nouvelle décision contraignante. La Commission européenne peut décider par un acte d'exécution qu'un code de conduite sera d'application générale au sein de l'UE. Le contrôle de l'application du code est réservé à des organismes agrées. Chaque autorité de contrôle livre ou non l'agrément demandé. Concernant les certifications elles servent à une entreprise ou organisme pour démontrer qu'il met en œuvre des mesures garantissant sa conformité avec le RGPD. La certification est délivrée directement auprès d'une autorité ou d'un organisme de certification préalablement agrée par l'autorité de contrôle.

553 Décret n° 2005-1309, 20 oct. 2005, art. 45 et suivants.

554 Le G29 considère que les organismes de droit privé en charge d'une mission d'intérêt public ou exerçant des prérogatives de puissance publique (tels que des compagnies chargées d'une mission de transport public ou encore de fourniture d'énergie) devraient également désigner un DPO.

grande échelle [555]; si leurs activités de base[556] les amènent à traiter (toujours à grande échelle)[557] des catégories particulières de données, dites « sensibles », et des données relatives à des condamnations pénales et à des infractions [558]; en dehors de ces cas, la désignation d'un délégué à la protection des données sera bien sûr possible, et même recommandée. Toutefois, il n'existe pas de seuil en termes d'effectifs qui rend obligatoire la désignation d'un délégué à la protection des données. Les missions du DPO sont fixées à l'article 39 du RGPD : il informe et conseille le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombe en matière de protection des données ; il contrôle le respect du droit en matière de protection des données et des règles internes du responsable du traitement ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux opérations de traitement, et les audits s'y rapportant ; il dispense des conseils, sur demande, en ce qui concerne l'analyse d'impact relative à la protection des données et vérifie l'exécution de celle-ci en vertu de l'article 35 du RGPD ; il coopère avec l'autorité de contrôle ; il fait office de point de contact pour l'autorité de contrôle sur les questions relatives au traitement, y compris la consultation préalable visée à l'article 36, et mène des consultations, le cas échéant, sur tout autre sujet. Concrètement, le DPO doit être placé au cœur du système et être associé par le responsable du traitement et le sous-traitant à chaque opération, chaque projet susceptible d'affecter la vie privée des personnes et la protection de leurs données.

555 Au titre du considérant 97 du RGPD les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire. Le G29 en déduit que les activités de base incluent les opérations de traitement de données nécessaires au fonctionnement de l'activité principale de l'organisme (comme par ex le traitement des données des patients d'un hôpital, sans lequel ce dernier ne peut plus fonctionner, mais excluent tous les traitements mis en œuvre pour les besoins d'activités de support et qui sont communes à tout organisation (ex: la paye). Concernant le suivi régulier et systématique des personnes le considérant 24 du RGPD l'illustre par l'activité de suivi sur Internet consistant notamment en un profilage d'une personne physique. Le G29 donne des exemples: l'exploitation d'un réseau ou des services de télécommunication, mise en place d'un programme de fidélité, publicité comportementale, établissement de profils aux fins d'attribution de crédits, exploitation ou utilisation d'objets connectés (ex: voiture intelligente).

556 Selon les lignes directrices sur les délégués à la protection des données, les « activités de base peuvent être considérées comme l'ensemble des activités pour lesquelles le traitement de données fait partie intégrante des activités du responsable du traitement ou du sous-traitant ».

557 Ainsi, l'appréciation de l'obligation de désigner ou non un délégué à la protection des données doit se faire au cas par cas, en fonction notamment du nombre de personnes concernées par les traitements de données à caractère personnel, du volume des données traitées, de la durée ou de la permanence des activités de traitement, de l'étendue géographique de l'activité de traitement

558 Le considérant 91 du RGPD se réfère aux « opérations de traitement qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational qui peuvent affecter un nombre important de personnes concernées ». Le G29 a précisé qu'il contribuera à la diffusion d'exemples de seuils pertinents dégagés par la pratique, peuvent être considérés à grande échelle les types de traitements suivants: Traitements des données des patients réalisé par un hôpital; traitement des données des usagers d'un dispositif de transport public (via une carte de voyage enregistrant les déplacements); Traitements réalisé par un moteur de recherche à des fins de publicité comportementale; traitement de données de trafic, de contenu et de géolocalisation réalisé par des opérateurs de télécommunication. Il donne des indications pout établir si un traitement est réalisé ou non à grande échelle: le nombre de personnes concernées, le volume de données et/ou la variété des différents types de données traitées, la durée du traitement, l'étendue géographique du traitement. Ceux qui ne sont pas soumis à l'obligation de désigner un DPO restent libres de confier à un membre de leur personnel ou à un consultant extérieur la charge de veiller à la conformité des traitements.

81 La mise en œuvre d'une PIA. Le responsable de traitement doit mettre en place toutes les mesures appropriées, au regard des risques vis-à-vis de la personne fichée afin de démontrer et garantir le respect du règlement. Deuxièmement, en vertu de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment le traitement à grande échelle de catégories particulières de données, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact[559]. L'analyse d'impact ou *privacy impact assestement* (PIA) inclut notamment « une évaluation de la nécessité et de la proportionnalité des opérations de traitement »[560] , ainsi qu'une étude d'impact afin de faire face aux risques « relatifs à la sécurité et prendre les mesures appropriées de correction ».[561] Ces analyses préalables sur l'impact d'un traitement impliquent également la mise en œuvre de mécanismes de protection des données dès la conception. Cela consiste dans l'élaboration d'une politique sur la vie privée intégrant le principe de « *Privacy by design* », consistant notamment à prendre en compte les enjeux liés à la vie privée dès la conception et par défaut[562].

82 La sécurité des traitements. Le RGPD impose de prendre des mesures de sécurité physiques[563] et numériques[564] afin d'assurer la sécurité des traitements et de notifier à l'autorité les failles de sécurité généralisée à l'ensemble des responsables de traitement dans l'hypothèse où la violation conduit à un risque important vis-à-vis des données personnelles collectées, renforçant la protection de la vie privée[565]. La notification doit se faire auprès de l'autorité de contrôle compétente sans retard et, si possible, dans un délai de 72 heures après en avoir pris connaissance[566]. Le règlement insiste particulièrement sur les mesures de sécurité à mettre en place par le responsable de traitement et le sous-traitant. Celles-ci incluent notamment la pseudonymisation[567], le chiffrement des données à caractère personnel, l'entretien constant des

559 Néanmoins, quand bien même il ne traiterait pas des données à « grande échelle », un responsable de traitement, pourrait avoir à réaliser des analyses d'impact si les traitements mis en œuvre répondent à certaines caractéristiques. En effet, dès lors qu'il répondra à plus de deux des neuf critères déterminés par la CNIL et par le G29 (évaluation/scoring, décision automatique avec effet légal ou similaire ; surveillance systématique ; collecte de données sensibles ; collecte de données à caractère personnel à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit / contrat), le traitement sera, par principe, soumis à analyse d'impact.

560 Règl. (UE) 2016/ 679, art. 35, § 7, b.

561 Règl. (UE) 2016/679, art. 35, § 7, d.

562 Règl. (UE) 2016/679 art.23.

563 A titre d'exemple il est nécessaire de mettre en place des mesures de sécurité physique des locaux: Limiter l'accès aux locaux ; Ne pas stocker ou archiver des dossiers ou documents contenant des données à caractère personnel dans des bureaux accessibles à tous ; Installer des alarmes.

564 Il est notamment conseillé d'authentifier les utilisateurs : mettre en place un mot de passe de minimum 8 caractères contenant une majuscule, une minuscule, un chiffre et un caractère spécial ; ne pas le partager ; ne pas le noter en clair sur une feuille ; éviter de le préenregistrer ; le changer régulièrement. gérer les habilitations et sensibiliser les utilisateurs : déterminer les personnes qui sont habilitées à accéder aux données à caractère personnel ; supprimer les permissions d'accès obsolètes ; rédiger une charte informatique et l'annexer au règlement intérieur lorsqu'il en existe un ; sécuriser l'informatique mobile : prévoir des moyens de chiffrement pour les ordinateurs portables et les unités de stockage amovibles (clés USB, CD, DVD...), éviter d'y stocker des données à caractère personnel sensibles des clients ; sauvegarder et prévoir la continuité d'activité : mettre en place des sauvegardes régulières, stocker les supports de sauvegarde dans un endroit sûr, etc.

565 Règl. (UE) 2016/679 art. 31.

566 Règl. (UE) 2016/679 consid. 85 et art. 33, § 1.

systèmes de traitement de données et l'existence de mesures d'urgence[568]. Si le responsable de traitement et le sous-traitant traitent des données à caractère personnel ne respectant pas les dispositions du RGPD ils encourent des amendes administratives très élevées. Les autorités de contrôle peuvent notamment : prononcer un avertissement ; mettre en demeure l'entreprise ; limiter temporairement ou définitivement un traitement ; suspendre les flux de données ; ordonner de satisfaire aux demandes d'exercice des droits des personnes ; ordonner la rectification, la limitation ou l'effacement des données. S'agissant des nouveaux outils de conformité qui peuvent être utilisés par les entreprises, l'autorité peut retirer la certification délivrée ou ordonner à l'organisme de certification de retirer la certification.

83 Les sanctions administratives. En vertu du droit de l'Union, l'article 83 du RGPD autorise les autorités de contrôle des États membres à imposer des amendes administratives en cas d'infraction au règlement. Le niveau des amendes et les circonstances prises en compte par les autorités nationales pour décider d'imposer une amende, ainsi que les plafonds maximaux de cette amende, sont également prévus à l'article 83. Le régime de sanction est donc harmonisé dans l'UE. Les amendes peuvent s'élever, selon la catégorie de l'infraction, de 10 ou 20 millions d'euros, ou, dans le cas d'une entreprise, de 2% jusqu'à 4% du chiffre d'affaires annuel mondial, le montant le plus élevé étant retenu. Ce montant doit être rapporté au fait que, pour les traitements transnationaux, la sanction sera conjointement adoptée entre l'ensemble des autorités concernées, donc potentiellement pour le territoire de toute l'Union européenne. Dans ce cas, une seule et même décision de sanction est décidée par plusieurs autorités de contrôle. Lorsqu'elles déterminent le type et le niveau d'amende à imposer, les autorités de contrôle doivent prendre en compte une série de facteurs. Par exemple, elles doivent dûment prendre en compte la nature, la gravité et la durée de l'infraction, les catégories de données. Lorsqu'un contrôleur ou un transformateur a pris des mesures pour atténuer les dommages subis par les personnes concernées, cela devrait également être pris en considération. De même, le degré de coopération avec l'autorité de surveillance à la suite de l'infraction et la manière dont l'autorité de contrôle a eu connaissance de l'infraction (par exemple, violée) sont d'autres facteurs importants guidant les autorités de surveillance dans leur décision[569]. Au-delà de la possibilité d'imposer des amendes administratives, les autorités de contrôle disposent d'un large éventail d'autres pouvoirs correctifs. Les pouvoirs « correctifs » des autorités de contrôle sont définis à l'article 58 du RGPD. Elles vont de l'émission d'ordres, avertissements et à l'imposition d'interdictions temporaires ou même permanentes des activités de traitement. Ce sont les ingrédients de la recette avec laquelle l'Union européenne, à travers le nouveau règlement, veut obtenir le respect des données personnelles et un gage de confiance dans l'économie numérique.

567 Règl. (UE) 2016/679consid. 75, 85 et 156 et art. 25, § 1, 32, § 1, a et 89, § 1.

568 Règl. (UE) 2016/679Art. 32.

569 Article 29 Working Party (2017), « Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679 », WP 253, 3 October 2017.

CONCLUSION DU CHAPITRE I

Un examen du régime de protection en la matière fait apparaître que la protection des données à caractère personnel s'est développée à partir du droit à la vie privée, consacré par l'article 8 de la CEDH de 1950. Dans un second temps, la protection des données à caractère personnel a été reconnue pour la première fois comme un droit distinct dans la Convention 108 du Conseil d'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108).

Seulement une dizaine d'années plus tard a été adopté un texte contraignant relatif aux données personnelles au sein de l'Union européenne. L'enjeu économique représenté par la circulation des données personnelles étant considérable, c'est d'abord pour assurer la réalisation du marché intérieur que les autorités de l'Union européenne ont fixé des règles. Le cadre juridique de l'Union européenne n'est pas général. La directive n° 95/46 CE, qui est entrée en vigueur en 1995, a été élaborée pour encadrer l'utilisation des données personnelles dans les États membres dans l'ex-premier pilier. C'est en effet sur la perspective économique et celle du marché intérieur[570] par l'aveu même de la Commission que la directive a trouvé son fondement juridique[571]. Ce n'est qu'après l'adoption de la Charte des droits fondamentaux de l'Union européenne, laquelle consacre spécifiquement et de manière autonome le droit à la protection des données personnelles dans son article 8, que le second objectif originellement présenté (la protection des droits et libertés fondamentaux des individus) a été ramené à sa juste place.

Suite à l'adoption de la directive 95/46, la réglementation communautaire s'est développée. L'Union européenne a non seulement adopté le règlement n° 45/2001 CE pour encadrer l'utilisation des données personnelles par les institutions communautaires elles-mêmes mais elle a progressivement réglementé l'utilisation des données personnelles dans les États membres dans les anciens deuxièmes et troisièmes piliers. Elle a notamment adopté la directive « *e-privacy* » pour encadrer l'échange des données dans les services de communications électroniques et une décision-cadre en matière de coopération judiciaire et policière. Malgré la volonté d'harmoniser le cadre légal et de protéger au mieux les données personnelles des individus, le constat est sans appel : la mise en application de la directive n'a pas permis à l'Union européenne l'instauration d'un système unitaire et harmonisé. Les différences dans l'application de la directive 95/46 ont mené à la création d'un contexte d'insécurité juridique, posant un frein à la libre circulation des données personnelles au sein de l'Union. Les disparités d'interprétation et d'application présentent donc un risque réel quant à la poursuite des activités économiques à l'échelle communautaire. A l'heure où la protection des données personnelles et de la vie privée fait la une des journaux chaque semaine et où la multiplication des cas

570 Dans la rédaction initiale de 1990, cette proposition avait pour objet « la protection des personnes à l'égard du traitement des données à caractère personnel », COM (90) 314 final SYN 287 et 288, 18 septembre 1990 mais la rédaction de 1992 complète ce titre par une référence à « la libre circulation de ces données » car ce texte a pour but d'assurer le fonctionnement du marché intérieur » COM (92) 422 final SYN 287, 15 octobre 1992. La base légale de l'intervention de l'Union européenne est ainsi l'ex. article 100 A, paragraphe 1er du Traité de Rome relatif à la réalisation du marché intérieur. D'ailleurs la Commission a elle-même reconnu que, d'un point de vue juridique, elle repose seulement sur l'objectif économique de réalisation du marché intérieur COM (2003) 265 final, 15 mai 2003, « Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE) ».

571 Voy. Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE), *C.O.M.* (2003) 265 final, p. 4.

majeurs de fuite de données personnelles met en péril des entreprises internationales de renom et des milliers de consommateurs, la protection des données personnelles des individus constitue un enjeu primordial, tant pour le secteur public que pour le secteur privé. L'ensemble de ces réglementations font d'ailleurs aujourd'hui l'objet d'un processus de modernisation entamé en 2010 pour répondre aux évolutions technologiques mais aussi sociales et économiques. Le nouveau règlement général sur la protection des données 679/2016 (RGPD) a été adopté dans l'optique de mettre en place un cadre solide et cohérent de protection permettant à l'économie numérique de se développer au sein du marché intérieur. Néanmoins on y retrouve le double objectif présent dans la directive 95/46 c'est-à-dire renforcer le marché unique et garantir les droits fondamentaux. La mise en œuvre du règlement européen sera l'enjeu déterminant des prochaines années. Ce texte modernise le cadre juridique tout en restant fidèle aux grands principes de la directive 95/46. Il rééquilibre les règles du jeu en renforçant l'individu, il dessine un véritable modèle européen du numérique, facteur de confiance et potentiellement d'attractivité. L'enjeu pour l'Union européenne est de montrer qu'elle est capable de faire vivre ce modèle européen qui relève de son identité.

CHAPITRE II. LE RÉGIME DE PROTECTION DANS L'ELSJ

84 La tension existant entre impératifs de sécurité et protection des données personnelles. Les données échangées dans l'espace de liberté, sécurité et de justice sont souvent des données sensibles dont le traitement peut porter atteinte à la vie privée. Le chapitre veut analyser les pratiques sécuritaires contemporaines et leurs impacts sur les citoyens de l'Union. Cela nous invite à repenser les régimes des droits fondamentaux en vigueur, notamment au regard de la tension existant entre impératifs de sécurité et protection de la vie privée et des données personnelles. Le droit à la protection des données à caractère personnel dans ce domaine a une importance particulière mais subit aussi des limitations qu'il conviendra d'identifier et éventuellement de justifier. L'objet du présent chapitre sera d'analyser le fonctionnement des différents mécanismes existants permettant l'échange d'informations dans le cadre de l'Espace de liberté, de sécurité et de justice de l'Union européenne (en matière d'asile, d'immigration et aussi dans la coopération policière et judiciaire en matière pénale) afin de vérifier si l'on assiste à un déplacement du curseur vers plus de sécurité au détriment de l'exigence de liberté Au sein de l'UE, la protection des données dans le secteur de la police et de la justice pénale est réglementée dans le cadre du traitement national et transfrontalier par les autorités de police et de justice pénale des États membres et des acteurs de l'UE[572]. Alors que le traité de Maastricht était resté vague quant aux objectifs du troisième pilier, le traité d'Amsterdam propose un véritable projet européen avec l'objectif ambitieux « *d'offrir aux citoyens un niveau élevé de protection dans un espace de liberté, de sécurité et de justice* ». Toutefois, c'est à la suite du sommet de Tampere[573] (et des attentats du 11 septembre 2001) que la plupart des décisions-cadres relatives au droit pénal matériel sont adoptées[574]. Le système repose sur la création de fichiers de données personnelles, informations indispensables en matière de lutte contre le terrorisme, formes graves de criminalité et d'immigration illégale[575]. Or, la difficulté est de trouver un équilibre entre sécurité et protection des données personnelles afin de ne pas se retrouver dans une société surveillée et liberticide. En effet, l'allocution « sécurité et ordre public », entraîne souvent l'application de mesures limitant l'exercice de certains droits

572 Une distinction importante entre le droit de l'Europe et le droit de l'UE est que le droit du Conseil de l'Europe, contrairement au droit de l'UE, s'applique également au domaine de la sécurité nationale. Cela signifie que les parties contractantes doivent rester dans les attributions de l'article 8 de la CEDH, même pour des activités liées à la sécurité nationale. Plusieurs arrêts de la Cour européenne des droits de l'homme concernent les activités de l'État dans les domaines sensibles du droit et de la pratique de la sécurité nationale.

573 Au « programme de Tampere » succède le « programme de La Haye » adopté par le Conseil européen de Bruxelles les 4 et 5 novembre 2004 (voy. les conclusions, doc. ST 14292 2004 INIT, du 05/11/2004, p. 11 et s.). Le « programme de Stockholm » adopté par le Conseil européen des 10 et 11 décembre 2009 (doc. ST 6 2009 INIT, du 11/12/2009, p. 9 et s.) pour la période 2010-2014. Le Conseil européen des 26 et 27 juin 2014 (a adopté des orientations stratégiques pour la période 2015-2020 (doc. ST 79 2014 INIT, du 27/06/2014). Quoique ces orientations n'utilisent plus le terme de «programme», elles sont parfois qualifiées de « programme de Rome ».

574 R. SCHUTZE, *From dual to cooperative federalism : the changing structure of the european law,* Oxford University Press, 2009, p. 1123-1124.

575 V. GAUTRON, « Usage et mésusages des fichiers de police: la sécurité contre la sûreté? », AJ pénal, 2010, p. 266.

fondamentaux [576] . La sûreté constitue un concept ancien qui a pu justifier des mesures restrictives des droits et libertés au nom de la sécurité ; Thomas Hobbes a théorisé l'importance de la sécurité dans le « contrat social », décrite comme un « attribut de l'État »[577]. Comme il a été souligné, la sécurité n'est pas envisagée comme un droit subjectif en soi, mais plutôt comme une notion autonome entrant en relation avec d'autres normes de rang constitutionnel sur un plan strictement fonctionnel[578]. Ainsi le concept de sécurité appartient à toutes les traditions constitutionnelles contemporaines, mais le sens qui lui est attribué n'est pas univoque. Ce concept est appréhendé tantôt comme un droit subjectif des individus à l'intégrité physique, tantôt comme une des missions régaliennes de l'État. De plus, la notion de sécurité se rapproche à celle plus large d'ordre public. Toutefois, l'ordre public n'est pas défini par le droit positif comme constituant un droit subjectif. On parle alors d'objectif de valeur constitutionnelle.[579], Les objectifs de valeur constitutionnelle constitueraient, sur le plan matériel, des « conditions d'effectivité des droits et des libertés » qui ne peuvent être méconnus par le législateur. Leur portée normative serait, toutefois, limitée dans la mesure où il n'impose qu'une obligation de moyens aux pouvoirs publics et donc disposant d'un rang inférieur aux droits fondamentaux[580]. Par conséquent, l'existence d'un « droit à la sécurité » à défaut d'encadrement, peut entraîner des dérives et des risques. Ainsi la sécurité et la liberté entretiennent un lien étroit avec la protection des données personnelles puisqu'elles sont essentielles au travail des autorités répressive, mais comme le disait Benjamin Franklin « Ceux qui sont prêts à abandonner une liberté essentielle en échange d'un peu de sécurité ne méritent ni la liberté, ni la sécurité » [581]. Au contraire, d'autres ont vu dans la sûreté « beaucoup plus qu'une liberté particulière ayant un objet déterminé […] elle est, plus largement, la garantie de la sécurité juridique de l'individu face au pouvoir. La sûreté constitue donc la protection avancée de toutes les libertés : c'est elle qui permet leur exercice paisible ».[582] Ce débat philosophique oppose classiquement les tenants

576 Voy. V. MITSILEGAS, « The Value of Privacy in an Era of Security: Embedding Constitutional Limits on Preemptive Surveillance », *Internal political sociology*, vol. 8, (1) 2014, p.104-108.

577 T. HOBBES, *Léviathan. Traité de la matière, de la forme et du pouvoir ecclésiastique et civil*, (1651), Université du Québec, Chicoutimi, http://classiques.uqac.ca/classiques/hobbes_thomas/leviathan/leviathan.html.

578 E. DENNINGE, « Stato di prevenzione e diritti dell'uomo », cit. 93, cit. in M. RUOTOLO, *La sicurezza nel gioco del bilanciamento, , Astrid Rassegna* (revue de droit constitutionnel online), 2009, p. 32.

579 Cela est confirmé par le Conseil constitutionnel en 1982 et en 1985. Dans la décision n° 82-141 DC du 27 juillet 1982, le Conseil constitutionnel a estimé qu'il « appartient au législateur de concilier (…) l'exercice de la liberté de communication telle qu'elle résulte de l'article 11 de la Déclaration des droits de l'homme (…) et les objectifs de valeur constitutionnelle que sont la sauvegarde de l'ordre public » (consid.5). Celui-ci a précisé ultérieurement, dans la décision n° 85-187 DC du 25 janvier 1985, qu' « en vertu de l'article 34 de la Constitution la loi fixe les règles concernant les garanties fondamentales accordées aux citoyens pour l'exercice des libertés publiques ; que dans le cadre de cette mission, il appartient au législateur d'opérer la conciliation nécessaire entre le respect des libertés et la sauvegarde de l'ordre public sans lequel l'exercice des libertés ne saurait être assuré » (consid. 3).

580 P. DE MONTALIVE, « Les objectifs de valeur constitutionnelle », Cahiers du Conseil constitutionnel n° 20, Juin 2006, disponibles à l'adresse : https://www.conseil-constitutionnel.fr/nouveaux-cahiers-du-conseil-constitutionnel/les-objectifs-de-valeur-constitutionnelle

581 B. FRANKLIN, il a exprimé une telle idée lors d'un débat devant le Congrès continental à Philadelphie en 1775 à propos des négociations avec l'Angleterre".

582 J. RIVERO, *Le régime des principales libertés, Les Libertés publiques, t. 2*, Paris, PUF, coll. « Thémis », 2003, p. 21.

des libertés fondamentales, aux défenseurs de toujours plus de sécurité, pour lesquels des sacrifices doivent être consentis pour assurer la sécurité[583]. L'Union européenne a fait le choix de placer la relation entre sécurité et liberté sous l'ongle du respect des droits fondamentaux[584]. Ceci signifie concevoir l'ELSJ comme « un espace unique de protection des droits fondamentaux », au sein duquel « le respect de la personne et de la dignité humaine (…) constitue une valeur essentielle » [585] . Toutefois la protection de la vie privée et son développement sous forme d'une protection spécifique de données personnelles, apparaît dans les faits comme très formelle et peu efficace[586]. Le régime de protection des données dans l'UE a été profondément influencé par l'ancienne structure en piliers de l'UE, qui a été abolie par le Traité de Lisbonne.[587] Cette ancienne division en pilier reste source de grandes incertitudes et de lacunes, un cadre juridique global sur la protection des données à caractère personnel fait toujours défaut[588]. Or, l'UE a dû élaborer une législation spécifique pour assurer la protection des données traitées dans le champ couvert par l'ELSJ puisque les États avaient mis en place différents systèmes de coopération transfrontière entre les autorités compétentes [589] . La décision-cadre 2008/977/ JAI [590] , constitue le premier instrument [591] applicable dans les

---

583 A. TURK, P. PLAZZA, « La difficile quête d'un équilibre entre impératifs de sécurité publique et protection de la vie privée », *Cultures et Conflits, Fichage et Listing*, hiver 2009, n° 76, p. 124.

584 Le droit à la vie privée dans les pays d'Europe continentale comme l'Allemagne et la France ont une place centrale, alors que les pays de tradition anglo-saxonne, comme l'Angleterre et les États-Unis, l'abordent avec beaucoup plus de souplesse.

585 Voy. conclusions du Conseil européen des 10 et 11 décembre 2009, doc. EUCO 6/09, § 27.

586 M. FOESSEL, « La sécurité : paradigme pour un monde désenchanté », Esprit, aout-septembre 2006, p. 194.

587 Le principal objectif de l'ancien premier pilier de l'UE, à savoir l'ancien pilier communautaire, est de garantir la libre circulation des données à caractère personnel entre les États membres, dans le fonctionnement du marché intérieur, tout en protégeant les droits fondamentaux des personnes physiques et en particulier leur droit au respect de la vie privée dans le cadre du traitement des données à caractère personnel.

588 Étant donné que la directive 95/46 ne s'applique pas aux traitements mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire ni aux traitement qui ont pour objet la sécurité publique, la défense, la sureté de l'État et les activités relevant du domaine pénale.

589 Concernant la protection des données à caractère personnel dans le contexte du titre VI TUE (ledit pilier III), voy. par exemple, la Convention d'application de l'accord de Schengen de 1990 comprenant des dispositions spécifiques sur la protection des données applicables au Système d'Information Schengen, JO L 239, 22.9.2000, p. 19; la Convention Europol de 1995 et, entre autres, les règles relatives à la transmission de données à caractère personnel par Europol à des états et des instances tierces, JO C 316, 27.11.1995, p. 2 ; la décision instituant Eurojust de 2002, JO L 63, 6.3.2002, p. 1 et les dispositions du règlement intérieur d'Eurojust relatives au traitement et à la protection des données à caractère personnel, JO C 68, 19.3.2005, p. 1; la Convention sur l'emploi de l'informatique dans le domaine des douanes de 1995, y compris les dispositions relatives à protection des données à caractère personnel applicables au système d'information des douanes, JO C 316, 27.11.1995, p. 34 ; et la Convention relative à l'entraide judiciaire en matière pénale entre les états membres de l'Union européenne de 2000, notamment article 23, JO C 197, 12.7.2000, p. 1 et 15.

590 Décision-cadre relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale, JOUE 30 déc. 2008, L 350/60. Elle sera bientôt remplacée par la directive sur la protection des données relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquête ou de poursuite ou d'exécution de sanctions pénales, et à la libre circulation de ces données

591 Dans le domaine appartenant à l'ex-troisième pilier (en matière de coopération judiciaire et pénale), il n' y a pas de texte général régissant les traitements de données à caractère personnel. Dès 2005, la Commission avait proposé un projet de décision-cadre mais il n'a pas été adopté. De nombreux mécanismes de coopération ont été mis en place entre les États et il existe plusieurs traitements de données mais chacun fonctionne avec ses règles propres : décision JAI Europol, Système

échanges transfrontaliers de données à caractère personnel dans le cadre de la coopération policière et judiciaire[592]. Il est intéressant de voir comment l'Union européenne a mis en place son régime de protection des données personnelles dans l'ELSJ et a su placer le curseur entre sécurité et respect des libertés (section I). Toutefois, contrairement à la période précédente marquée par le souci de protéger le droit fondamental à la protection des données personnelles la nouvelle priorité de l'Union européenne semble celle de renforcer la sécurité dans le contexte de menace terroriste. Le cadre juridique préexistant a alors montré ses fragilités et ses lacunes ce qui a justifié une réforme du cadre juridique (section II).

d'Information Schengen, système d'information des douanes. Des mécanismes plus généraux de coopération en matière policière et pénale ont été prévus par la décision JAI 2008/615 visant à intégrer le Traité Prüm dans le cadre juridique de l'UE ainsi que par la décision-cadre 2008_977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale.

592 Voy. E. SANFRUTOS CANO, *The End of the Pillars? A Single EU Legal Order After Lisbon*, in Law And Outsiders 67, Cian Murphy et al. eds., 2011 (explaining the evolving rules for the adoption of legislation in the field of JHA, which required unanimity in the Council until the entry into force of the Lisbon Treaty in 2009 and are now subject instead to normal voting rules).

Section I. L'approche européenne entre protection des droits fondamentaux et sécurité publique

85 Les enjeux démocratiques de l'utilisation des fichiers. L'activité de police et l'activité judiciaire représentent des domaines au cœur de la souveraineté nationale. Le risque notamment pour les domaines couverts par l'ancien troisième pilier peut être résumé à ce qui a été appelé « *the rise of the culture of control* »[593]. Avant que l'Union européenne se dote d'un texte en la matière, diverses disciplines nationales trouvaient application. Elles reposaient pour une large mesure sur les principes et sur les définitions de la Convention de Strasbourg n. 108/1981 en tant que standard minimum [594] , et d'autres instruments spécifiques, comme le système d'information Schengen (SIS et SIS II)[595], le système sur les visas (VIS)[596] ou les base de données gérés par Europol[597] et Eurojust[598] ou encore celles encadrés par le traité de Prüm[599]. Par conséquent, la difficulté était l'aboutissement des niveaux de protection différents selon les États membres. C'est seulement avec le Traité de Lisbonne que le cadre juridique dans le domaine de la coopération policière et judiciaire en matière pénale s'est considérablement développée afin de construire un « Espace de liberté, sécurité et justice » (ELSJ).

---

593 K. NUOTIO, « Security and Criminallaw: A difficult Relationship », *in* M.FICHERA et J. KREMER (dir.), Law and Security in Europe : Reconsidering the Security Constitution, Intersentia, 2013, pp. 197-217, sp. 215.

594 Voy. Convention 108, Art. 6. En ce qui concerne la police et la justice pénale, au niveau européen, la Convention modernisée 108 couvre tous les domaines du traitement des données à caractère personnel et ses dispositions visent à réglementer le traitement des données à caractère personnel en général. Par conséquent, la Convention modernisée 108 s'applique à la protection des données dans le domaine de la police et de la justice pénale. Le traitement des données génétiques, des données personnelles relatives aux infractions, aux procédures pénales et aux condamnations et toutes mesures de sécurité connexes, les données biométriques qui identifient de manière unique une personne, ainsi que toute donnée personnelle sensible, ne sont autorisés que lorsque des garanties appropriées existent le traitement de ces données peut porter atteinte aux intérêts, aux droits et aux libertés fondamentales du sujet de données; notamment le risque de discrimination. La recommandation de la police adoptée par le Conseil de l'Europe en 1987 oriente les États membres du Conseil de l'Europe sur la manière dont ils devraient donner effet aux principes de la Convention 108 dans le contexte du traitement des données à caractère personnel par les autorités de police. Voy. Council of Europe, Committee of Ministers (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector, 17 September 1987. D'ailleurs, les activités criminelles utilisant et affectant de plus en plus les systèmes de traitement électronique des données, de nouvelles dispositions pénales sont nécessaires pour relever ce défi. Le CdE a donc adopté un instrument juridique international - la Convention sur la cybercriminalité, également connue sous le nom de Convention de Budapest - pour aborder la question des crimes commis contre et au moyen de réseaux électroniques. Voy. Council of Europe, Committee of Ministers (2001), Convention on Cybercrime, CETS No. 185, Budapest, 23 November 2001, entered into force on 1 July 2004.

595 Le Système d'information Schengen (SIS) est un système informatique mis en place en application de l'accord de Schengen, du 14 juin 1985 dans le cadre de la réalisation de l'espace Schengen. Il constitue l'une des mesures dites compensatoires à la libre circulation prévue par l'Accord et la Convention Schengen. Ces mesures compensatoires ont été adoptées en vue d'assurer un niveau de protection au moins équivalent à celui existant avant l'abolition des frontières. Le SIS permet aux autorités responsables des États Schengen d'échanger des informations pour le contrôle des personnes et des objets aux frontières ainsi que pour la délivrance de visas et de permis de séjour.

596 Règlement (CE) no 767/2008 du Parlement européen et du Conseil du 9 juillet 2008 concernant le système d'information sur les visas (VIS) et l'échange de données entre les États membres sur les visas de court séjour (règlement VIS).

597 Décision 2009/371/JAI du Conseil, 6 avril 2009 instituant l'office européen de police (Europol).

598 Décision 2002/187/JAI du Conseil, du 28 février 2002, modifiée par la décision 2003/659/JAI et 2009/426/JAI du Conseil, du 16 décembre 2008.

599 Décision 2008/615/JAI du Conseil du 23 juin 2008.

Le traité de Lisbonne marque un saut qualitatif d'une coopération pénale interétatique à une intégration pénale supra-étatique[600]. Les principaux développements en matière de coopération ont été en effet précédés par des accords, conclus extérieurement à l'Union, entre groupes d'États disposés à céder partie de leur souveraineté pour combattre la criminalité. C'est le cas notamment de la Convention de Schengen et du Traité de Prüm601, ces accords ont été progressivement incorporés dans l'architecture de l'Union[602]. Les premières vraies initiatives autonomes de la part de l'Union européenne sont arrivées successivement au programme de La Haye en 2004, qui a souligné l'importance et la nécessité d'une action intégrée en matière de coopération de police [603] établie sur le « principe de disponibilité »[604] dans le but de faire circuler librement les données personnelles entre services répressifs dans l'espace couvert par l'ex-troisième pilier. Cette « mutualisation, à l'échelle communautaire, des informations des données des traitements nationaux » [605] était la première pierre de la construction d'une protection des données personnelles circulant sans frontières. D'ailleurs la proposition d'une décision-cadre[606] voulait apporter une réponse aux difformités mise en place par le principe de disponibilités. C'est seulement en 2008 que la décision-cadre 2008/977/JAI a posé un socle

---

600 Le droit de punir est depuis longtemps confronté à l'internationalisation que M. MASSÉ définit comme un « mouvement par lequel le droit pénal franchit les frontières et s'affranchit de la souveraineté des États », ce qui souligne « une mutation de la discipline par redéfinition de ses moyens et par déplacement de la source du droit de punir », voy. M. MASSÉ, *L'internationalité et le droit pénal,* Revue Lamy Droit des affaires, 2002, n°46, pp. 67-71 ; et du même auteur, *Des figures asymétriques de l'internationalisation du droit pénal, RSC,* 2006, n°4, pp. 755-766. Voy. également M. HENZELIN, R. ROTH, « Le droit pénal à l'épreuve de l'internationalisation », Revue internationale de droiot comparé, 2003, p.719-720.

601 Le traité de Prüm était un accord international de coopération policière signé en 2005 par l'Autriche, la Belgique, la France, l'Allemagne, le Luxembourg, les Pays-Bas et l'Espagne. Il s'agit d'un exemple important de coopération transfrontalière caractérisé par l'échange de données détenue au niveau national et incorporé dans le droit communautaire en 2008 grâce à la décision du Conseil 2008/651/JAI. La décision prévoit l'accès automatisé aux profils ADN, données d'empreintes digitales et certaines données nationales relatives à l'immatriculation des véhicules; la transmission d'informations pour prévenir des infractions terroristes. Les bases de données mises à disposition par la décision Prüm sont entièrement régies par le droit national, mais l'échange de données est en outre régi par la décision, dont la compatibilité avec la directive sur la protection des données des autorités policières et judiciaires devra être évaluée. Les autorités compétentes en matière de surveillance de ces flux de données sont les autorités nationales de surveillance de la protection des données.

602 Les conclusions du Conseil européen de Tampere d'octobre 1999 avaient souligné la nécessité d'approfondir l'échange d'informations en matière répressive entre les pays de l'Union européenne. Le principe de disponibilité des données avait été présenté dans le programme de la Haye en 2004 et visait à permettre aux agents répressifs d'un État un accès direct aux données détenues par d'autres états. Le Traité de Prüm du 2è mai 2005 relatif à l'approfondissement de la coopération transfrontalière, en vue de combattre le terrorisme et la criminalité et la migration illégale (entre la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche) avait fixé les règles de cet échange des données mais les états ont ensuite pris conscience de la nécessité d'intégrer les dispositions de ce traité dans le cadre juridique de l'UE.
La décision Prüm vise à aider les États membres signataires à améliorer le partage d'informations dans le but de prévenir et de combattre la criminalité dans trois domaines: le terrorisme, la criminalité transfrontalière et la migration illégale. À cette fin, la décision énonce des dispositions concernant

603Voy. http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=uriserv%3Al16002

604 Il faut l'entendre comme la possibilité, pour les services répressifs d'un État membre qui a besoin de certaines informations dans l'exercice de ses fonctions, de les obtenir d'un autre État membre qui les détient. L'État membre sollicité serait tenu de communiquer les informations requises, sauf refus dûment motivé.

605 J.M. DELARUE, « L'Europe des fichiers, Dialogue des juges, des policiers, des autorités administratives indépendantes », *in Le dialogue des juges, Mélanges en l'honneur du Président Bruno Genevois*, Dalloz, 2009, p. 276.

606 Voy. la Proposition de décision-cadre du Conseil relative à l'échange d'informations en vertu du principe de disponibilité, COM(2005)490,

commun[607] . Le Contrôleur européen de la protection des données (CEPD) avait d'ailleurs souligné que « l'applicabilité de la décision-cadre au traitement national des données est une condition essentielle afin, non seulement d'assurer un niveau de protection suffisant des données à caractère personnel, mais aussi de permettre une collaboration efficace entre les services répressifs »[608]. Toutefois l'harmonisation apportée par la décision-cadre n'a pas su édifier un régime de protection efficace puisqu'elle ne s'appliquait pas aux traitements nationaux. De plus, la Décision-cadre ne se substituait pas aux régimes spécifiques déjà prévus[609]. Dès sa création elle se présentait comme un instrument insuffisant pour assurer une protection complète et efficace dans le cadre de l'ELSJ.

Toutefois, des avancées ont été mises en place par l'entrée en vigueur du Traité de Lisbonne[610]et des nouvelles priorités ont été mis en lumière par le programme de Stockholm[611]. Depuis l'expiration du programme de Stockholm,[612] les actions concrètes de l'Union dans ce domaine reposent sur les orientations stratégiques définies par le Sommet européen de juin 2014[613]. Contrairement à la période précédente, marquée par le souci de renforcer la sécurité dans le contexte de menace terroriste, la nouvelle priorité est en revanche de développer le cadre juridique de la protection des droits fondamentaux, en particulier de la vie privée et des données personnelles[614] . Dans l'espace pénal européen la difficulté repose sur le fait de conjuguer liberté, sûreté et justice. L'étude du présent chapitre veut évaluer les problèmes pour le droit à la protection des données personnelles que pose l'exploitation des bases de données (§1) ainsi que le rôle joué par les Agences européennes dans l'échange des données (§2). Il conviendra

---

607 Décision-cadre 2008/977/JAI du Conseil du 27 novembre 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale

608 Voy. le troisième avis du CEPD relatif au projet de décision-cadre, 27 avril 2007, JOUE C 139 du 23 juin 2007.

609 Tels que EUROPOL, EUROJUST, le SIS, et le traité de Prüm.

610 Tant du point de vue de la protection des droits fondamentaux que du point de vue institutionnel avec la disparition de la division en piliers. Cela a des conséquences significatives concernant le contrôle démocratique et signifie la généralisation de la procédure législative « ordinaire », c'est-à-dire un Parlement Européen jouant pleinement son rôle de colégislateur mais aussi des conséquences concernant le contrôle juridictionnel. Voy. sur ce point V. CONSTANTINESCO, *Le processus de décision : vers une nouvelle gouvernance ?*, Europe, juillet 2008, dossier 8, § 5. V. également H. LABAYE, *L'espace de liberté, sécurité et justice : la nouvelle frontière ?, Europe*, juillet 2008, dossier 10, § 9.

611 Voy. Conclusions du Conseil européen, EUCO 6/09 du 11 décembre 2009.

612 Le programme de Stockholm fournit une feuille de route pour le travail de l'Union européenne (UE) dans le domaine de la justice, de la liberté et de la sécurité pour la période 2010-2014. Sur la lancée des résultats obtenus dans le cadre des programmes de Tampere et de La Haye, il vise à relever les défis futurs et à renforcer le domaine de la justice, de la liberté et de la sécurité au moyen d'actions qui mettent l'accent sur les intérêts et les besoins des citoyens.

613 Lors de sa réunion à Bruxelles le 27 juin 2014, le Conseil européen a défini cinq grandes priorités qui guideront les travaux de l'UE au cours des cinq prochaines années. Ces priorités sont présentées dans un document intitulé « Programme stratégique pour l'Union à l'ère du changement ». Ce programme stratégique sera utilisé pour planifier les travaux du Conseil européen.

614 COM (2009262/4,) point 2.3.

de se demander si l'on assiste à un déplacement du curseur vers plus de sécurité au détriment de l'exigence du respect des droits fondamentaux[615].

§1. L'identification de différentes formes d'échange de données dans l'ELSJ

86 Le contrôle dans l'espace européen et dans la sécurisation des frontières extérieures de l'Union. L'élaboration d'immenses bases de données est devenue l'objet principal de la politique de sécurité au sein de l'Union européenne. L'accroissement illimité des bases de données pose des problèmes quant aux droits des personnes concernées, notamment les techniques de fichage, les systèmes de surveillance, l'incorporation de plusieurs données et leurs interconnexions avec d'autres bases de données peuvent devenir un moyen d'anticipation des comportements « à risque ». Une analyse au niveau européen de ces bases de données sera présentée pour vérifier si la protection des droits est effective. Le Traité de Lisbonne a institué une nouvelle base juridique pour la protection des données personnelles[616]. La compétence prévue par l'art. 16 du TFUE est une compétence concourante de l'Union avec les États membres dans tout l'espace de liberté, sûreté et justice (coopération en matière d'immigration, coopération civile et pénale). D'ailleurs, dans ce secteur pourront être prévues des règles spécifiques, comme prévu dans la Déclaration 21 jointe au Traité de Lisbonne. La seconde base juridique concerne le secteur de la politique étrangère et de sûreté commune dans lequel le TFUE prévoit seulement l'adoption d'une décision *ad hoc* du Conseil[617]. Le droit à la protection

---

615 Dans l'affaire Wijsenbee du 19 septembre 1999, C-378/97, La Cour de justice examine la compatibilité avec le droit communautaire applicable d'une loi nationale réglementant les vérifications d'identité opérées sur des citoyens lors du franchissement des frontières. En l'état du droit communautaire applicable au moment des faits, l'absence de ces règles d'harmonisation permettait donc, selon la Cour, aux États membres, de procéder à des contrôles d'identité aux frontières intérieures de la Communauté afin d'établir si la personne concernée est un ressortissant communautaire et dispose donc du droit à la libre circulation sur le territoire des États membres, ces derniers demeurant compétents pour sanctionner la violation d'une telle obligation. La Cour précise que les sanctions prévues par la législation nationale doivent être comparables à celles appliquées à des infractions nationales similaires et ne pas être disproportionnées, sous peine de constituer une entrave à la liberté de circulation.

616 Au titre de l'ancien « troisième pilier» (coopération policière et judiciaire en matière pénale), le Parlement européen était uniquement consulté. Son rôle a été renforcé par le traité de Lisbonne, qui introduit plus d'efficacité, de responsabilité et de légitimité dans l'espace de liberté, de sécurité et de justice (ELSJ). Le traité de Lisbonne a généralisé (à quelques exceptions près) la méthode communautaire, basée sur la procédure de codécision (appelée maintenant « procédure législative ordinaire») entre le Parlement et le Conseil (où l'unanimité a été remplacée par le vote à la majorité). L'ancienne structure en piliers a disparu. En ce qui concerne les accords internationaux, une nouvelle procédure a été introduite, la procédure d'approbation. L'abolition de l'ancien « troisième pilier» a conduit à l'harmonisation des instruments législatifs. Au lieu de décisions-cadres, de décisions et de conventions, même dans le domaine du droit pénal, l'Union adopte les instruments normaux de l'Union européenne (règlements, directives et décisions). Le rôle de la Cour de justice a également été renforcé par le traité de Lisbonne: les procédures ordinaires de renvoi préjudiciel et les procédures d'infraction engagées par la Commission s'appliquent. Des dispositions de transition étaient valables jusqu'au 1er décembre 2014 pour les actes qui étaient déjà en vigueur dans les domaines de la coopération policière et judiciaire en matière pénale. Les États membres peuvent toujours proposer des mesures législatives, mais une initiative exige à présent le soutien d'un quart des États membres. Des mesures spéciales sont prévues en ce qui concerne la coopération renforcée, les dérogations et ce que l'on appelle le «frein de secours». La charte des droits fondamentaux de l'Union est intégrée dans le traité de Lisbonne et a un caractère juridiquement contraignant pour l'Union européenne (et ses institutions et ses organes) et les États membres dans la mise en œuvre du droit de l'Union.

617 Voy. art. 39 TUE: « Conformément à l'article 16 du traité sur le fonctionnement de l'Union européenne et par dérogation à son paragraphe 2, le Conseil adopte une décision fixant les règles relatives à la protection des personnes physiques à l'égard

des données a trouvé son apogée avec la Charte des droits fondamentaux[618] ; dans l'après Lisbonne, la consolidation de l'ELSJ a changé le cadre institutionnel en étendant l'action de l'Union européenne au-delà du domaine du marché Intérieur. Avant d'analyser les systèmes d'information présents au sein de l'Union européenne, il est intéressant de souligner qu'il n'existe pas une notion harmonisée d'*information* au sein des États membres[619]. Par exemple la langue italienne ne distingue pas entre une information générique et une information relevant des systèmes d'échange des données, en revanche dans la langue française existe le terme *renseignement* qui introduit une notion liée au caractère secret de l'information. Au-delà de l'échange de données entre les États membres et de la création d'autorités européennes spécialisées dans la lutte contre la criminalité organisée transfrontalière, plusieurs systèmes d'information conjoints ont été établis, tel que le Système d'information Schengen, le système d'information sur les visas[620], Eurodac[621], Eurosur[622]. Dans la première et moins développée phase de coopération, l'échange des données émanait d'une demande de l'autorité de l'État vers un autre État. Ledit système a été remplacé par le principe de « disponibilité » selon lequel une information détenue par l'un des services répressifs d'un État membre peut profiter à l'ensemble des services des autres États membres. Comme l'indique la Commission « le partage de l'information entre autorités répressives est essentiel en vue de lutter contre le terrorisme et de mener des enquêtes relatives à la criminalité transfrontière de manière efficace »[623].Toutefois, le renforcement de la dimension sécuritaire de l'Union doit se réaliser

---

du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du présent chapitre, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes ».

618 Voy. Report from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions, 2010 Report on the Application of the EU Charter of Fundamental Rights, Brussels, 30.3.2011, COM(2011) 160 final, p. 6.

619 D. BIGO, *L'Europe des polices et de la sécurité intérieure*, Editions Complexe, Coll. Espace international, Bruxelles, 1992, p. 153 ; D. BIGO, « Du discours sur la menace et de ses ambiguïtés », Cahiers de la Sécurité Intérieure, n° 14, 1993, p. 141; D. BIGO, « Polices en réseau, l'expérience européenne », *Revue française de science politique*, 1997, p. 227-232.

620 Le système d'information sur les visas (VIS) est un système d'échange de données sur les visas entre les États Schengen. La mise en œuvre du VIS constitue un élément clé de la politique commune en matière de visas qui, associée à d'autres politiques, permet à l'Union européenne d'établir un espace de liberté, de sécurité et de justice. Concernant la protection des données personnelles Seul le personnel dûment autorisé des autorités compétentes sera habilité à saisir, à modifier, à effacer ou à consulter les données du VIS.

621 Le système Eurodac permet aux pays de l'Union européenne (UE) de participer à l'identification des demandeurs d'asile et de personnes ayant été appréhendées dans le contexte d'un franchissement irrégulier d'une frontière extérieure de l'Union. En comparant les empreintes, les pays de l'UE peuvent vérifier si un demandeur d'asile ou un ressortissant étranger se trouvant illégalement sur son territoire a déjà formulé une demande dans un autre pays de l'UE ou si un demandeur d'asile est entré irrégulièrement sur le territoire de l'Union. Il se compose d'une unité centrale gérée par la Commission européenne, d'une base de données centrale informatisée d'empreintes digitales et de moyens électroniques de transmission entre les pays de l'UE et la base de données centrale.

622 Le système européen de surveillance des frontières (EUROSUR) devrait aider les États membres à acquérir une parfaite connaissance de la situation à leurs frontières extérieures. La « connaissance de la situation» mesure la capacité des autorités à détecter les mouvements transfrontaliers et à motiver les mesures de contrôle.

623 Voy. La communication de la Commission au Conseil et au Parlement européen du 10 mai 2005, Journal officiel C236 du 24/09/2005.

dans le respect des droits de la personne[624]. Cela a été affirmé tant par la Cour de justice que par la CourEDH « en principe quelconque traitement effectué par un tiers est apte à constituer préjudice aux tels droits »[625]. Encore plus une récolte à grande échelle des données personnelles porte le risque de ne pas respecter l'intégrité et l'exactitude dans l'enregistrement dans les bases des données. De plus une si rapide et générale circulation des données peut porter préjudice aux droits fondamentaux[626]. Cela constitue le noyau dur de la question qui concerne l'équilibre entre droits fondamentaux[627], et l'amélioration de l'efficacité de l'échange de données ne doit pas se faire au détriment des droits fondamentaux et c'est principalement la question de la protection des données à caractère personnel qui se pose. Les droits fondamentaux sont ainsi protégés tant par l'Union européenne que par le Conseil d'Europe à travers la prévision des droits correspondants selon laquelle lorsque la Charte contient des droits correspondants à ceux de la CEDH, leur portée est la même[628]. Le cadre juridique devient alors une interconnexion et une convergence de solutions européennes, une osmose et un « *multilevel protection of human rights* »[629]. Si le contrôle sur la base légale et sur la légitimité du but poursuivi a été analysé dans le passé, la censure des deux juges se concentre aujourd'hui sur l'étendue de la marge d'appréciation des autorités publiques dans leur ingérence[630] . La Cour a eu l'occasion de préciser ainsi le principe selon lequel les données doivent être utilisées pour les finalité établies lors de leur récolte[631]. Dans un système fragile constitué d'une multitude de textes applicables

---

624Voy. Sur les principes les article 6-7, 12, 14 et 22 de la directive 95/46/CE, Voy. Également les conclusions de l l'Avv. général Mengozzi, aff. C-291/12, Schwarz, point 39.

625 CJUE, aff.C-291/12, Schwarz, 17 octobre 2013, § 25 ; CEDH 4 décembre 2008, S. et Marper c.Royaume-Uni, n° 30562/04 et 30566/04, point 86; et du 18 avril 2013, M.K. c. France, n. 19522/09, point 29, selon laquelle « La Cour rappelle que la conservation, dans un fichier des autorités nationales, des empreintes digitales d'un individu identifié ou identifiable constitue une ingérence dans le droit au respect de la vie privée". Encore sur les fichiers, l'affaire du 26 mars 1987, Laender c. Suède, n. 9248/81; du 16 février 2000, Amann c. Suisse,. n. 27798/95; et du 4 mai 2000, Rotaru c. Roumanie, ric. n. 28341.

626 L'échange de renseignements d'un base données à l'autre et le croisement entre elles peuvent avoir un impact sur le droit à la vie privée; ainsi le passage de renseignements de la part de l'intelligence, à la police et au système douanier, comporte le risque de contredire les principes du procès équitable et de contrevenir au principe du respect des finalités pour lesquelles les données ont été recueillis ;

627 Voy. la jurisprudence de la Cour de justice: 18 décembre 2007, aff. C-137/05, Irlande c. Conseil de l'Union européenne (sur les règles en matière de caractéristiques de sûreté des bases de données et sur les éléments biométriques y contenu de passeports et documents de voyage) ; 16 décembre 2008, aff. C-524/06, Huber (sur le critère de nécessité du traitement des données personnelles); 26 octobre 2010, aff. C-482/08, Royaume-Uni et Irlande du Nord (en matière d'accès au système d'information des visa-VIS); 17 octobre 2013, aff. C-291/12, Schwarz (en matière de légitimité de l'obligation d'obtention d'empreintes digitales pour la délivrance du passeport); Actuellement il y a des renvois préjudiciels (aff. C- de 446 à 449/12) en matière d'utilisation des données biométriques recueillies à travers le passeport et d'autres documents de voyage.

628 Art. 52, n. 3, Charte des droits fondamentaux de l'UE.

629 M. CARTABIA, « The multilevel protection of fundamental rights in Europe: the European Pluralism and the need for a judicial dialogue », in C. CASONATO(a cura di), *The protection of fundamental rights in Europe: lessons from Canada*, Quaderni del Dipartimento di Scienze Giuridiche, Università degli Studi di Trento, 2003, p. 399. Voy.également G. BRONZINI et V. PICONE, *Le giurisprudenze europee in movimento. Luci e ombre nel processo di costruzione di uno jus commune*, in Quest. Giust., 2007 (1), p. 131.

630 CEDH, S. e Marper c. Regno Unito, cit., point 97 (anche se la Corte riscontra che le norme sono formulate «in termini piuttosto generici» e si prestano «a una interpretazione eccessivamente larga»: punto 99) e punto 100; et CJUE, Schecke GbR e Eifert, cit., point 35, 38 et 45, ainsi la CJ a déclaré qu'il y avait une correcte marge d'appréciation de la part des règles communautaire relatives à la récolte et stockage des données nécessaires au relâchement du passeport biometrique.

631 CJUE, sentenza Schwarz, cit., § 61.

et de plusieurs bases de données l'apport de la jurisprudence est nécessaire pour effectuer la juste mise en balance entre droits fondamentaux et droit à la sûreté. Les règles de l'UE en matière de bases des données sont récentes, ainsi il manque une jurisprudence de la Cour de justice qui puisse montrer quel équilibre est réalisé entre les exigences de sécurité et celles de protection de la vie privée et des données personnelles. Dans ce domaine la Cour de justice ne manque pas de s'inspirer à la jurisprudence de la CEDH. L'importance de cette dernière a été expressément reconnue par la Cour de justice dans l'affaire *Österreich Rundfunk*[632]. De façon emblématique, la Cour de justice s'est prononcée sur la surveillance d'État dans l'arrêt *Digital Rights Ireland*[633]. L'arrêt « *Digital Rights Ireland* » portait sur la question de la validité de la directive 2006/54/CE imposant une conservation des données de télécommunication pendant une durée déterminée. Dans cet arrêt la Cour de justice a rappelé que l'accès des autorités publiques aux données personnelles collectées et traitées pour une finalité initiale différente de la leur peut constituer un motif légitime. Toutefois, cet accès ne saurait être universel, indiscriminé et inconditionnel[634]. La directive 2006/24/CE a été invalidée notamment en raison de l'absence de critères objectifs permettant de délimiter l'accès des autorités compétentes aux métadonnées (données de communication, sans le contenu des communications) dont elle imposait la conservation aux opérateurs de services de télécommunication. Or, de tels critères auraient dû être définis afin de garantir qu'un tel accès ne soit possible qu'en lien avec l'objectif légitimement poursuivi de lutte contre les infractions graves et la criminalité[635]. Ainsi, la CJUE rappelle, tout comme la CEDH, que la surveillance d'État doit elle aussi obéir au principe de limitation des finalités. La Cour de justice a donc joué un rôle important dans la fixation d'un cadre restreignant les politiques de conservation des données de communication. Il est possible de distinguer la création des fichiers en matière d'asile et d'immigration (A) (ce sont les bases de données SIS et VIS) et la création des fichiers dans le cadre de la coopération policière, notamment Eurodac (B). Ces fichiers structurent le système communautaire de contrôle de migrations et de coopération policière. Lesdits systèmes d'information font l'objet d'un contrôle par des agences européennes. En effet, l'art. 16 TFUE permet au législateur de fixer les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union[636], et à la libre circulation de ces données ; de plus le respect de ces règles est soumis au contrôle des autorités indépendantes et des agences européennes[637].

---

632 CJCE, Österreich Rundfunk, aff. C-465/00, C-138/01 et C- 139/01, 20 mai 2003.

633 CJUE, Digital Rights Europe, aff. C-293/12 et C-594/12, 8 avril 2015.

634 CJUE, Digital Rights Europe, préec.§ 54 à 60.

635 CJUE, Digital Rights Europe, préec.§ 60.

636 M. VAN DE KERCHOVE, « Le principe de subsidiarité », in *Le droit pénal au lendemain du traité de Lisbonne, Société de législation comparée*, Paris, 2012, p. 41.

637 Il est important ici de souligner le maintien du schéma existant, à savoir une dispersion institutionnelle et la coexistence de plusieurs autorités au plan européen et au plan national.

A. Les systèmes d'information en matière d'asile et d'immigration

87 Des bases de données spécifiques. L'entrée et le séjour de ressortissants étrangers sur un territoire national est un domaine hautement sensible, sur lequel les États européens maintiennent aujourd'hui un grand nombre de prérogatives souveraines. Depuis les années 1980 cependant, ils ont développé une importante coopération en matière de liberté de circulation, de contrôle aux frontières, d'asile et d'immigration. La politique européenne de l'asile et de l'immigration repose tout d'abord sur le principe de liberté de circulation des personnes au sein des 26 pays membres de l'espace Schengen. Intégré au cadre juridique de l'Union européenne par le traité d'Amsterdam en 1997, « l'acquis Schengen » permet aux individus, « quelle que soit leur nationalité », de ne pas faire l'objet de contrôles lorsqu'ils franchissent les frontières internes de l'espace (art. 3 TUE). L'article 67 TFUE précise également que l'Union européenne « développe une politique commune en matière d'asile, d'immigration et de contrôle des frontières extérieures qui est fondée sur la solidarité entre États membres ». Bien que le contrôle et la surveillance des frontières extérieures restent principalement de la responsabilité des États membres, l'Union européenne appuie leur action à travers plusieurs instruments communs. Depuis le Conseil européen de Laeken (2001), l'Union européenne cherche à établir un système intégré de gestion des frontières extérieures, afin de lutter notamment contre le terrorisme, l'immigration illégale et la traite des êtres humains. Cette orientation a abouti à la mise en place de systèmes comme le SIS, le VIS ou Eurosur, et à la création d'agences telles que Frontex.

1) Le système d'espace Schengen (SIS)

88 Un fichier commun aux États membres. Les attentats de 2001 ainsi que ceux de Londres et de Madrid de 2004 et 2005 ont provoqué une évolution de la conception de la coopération policière. Il est apparu nécessaire de renforcer le fichier SIS (Système d'espace Schengen), mis en place en 1995, dans le cadre des Accords de Schengen[638]. Il s'agit d'un fichier commun aux États membres de l'espace Schengen, alimenté par les agents des services de police et les autorités judiciaires nationales et qui centralise les données relatives aux personnes et aux véhicules ou objets recherchés[639].

638 Le système d'information Schengen (SIS) est une base commune de données sur les personnes recherchées ou portées disparues, les biens perdus ou volés, ainsi que les interdictions d'entrée. Elle est régulièrement utilisée par les forces de l'ordre des membres de l'espace Schengen, notamment pour vérifier qu'une personne qui tente d'entrer dans l'espace Schengen ne s'est pas déjà vu refuser l'entrée. Opérationnel depuis le 9 avril 2013, le SIS de 2e génération (SIS II) collecte également des données biométriques.

639 Notamment des données concernant personnes recherchées ou disparues, placées sous surveillance, arrêtées aux fins d'extradition, personnes non admises dans l'espace Schengen. Il s'agit de données relatives au nom, les signes physiques particuliers, date et lieu de naissance, nationalité.

Il est prévu que les données soient conservées pendant trois ans renouvelables. Le SIS est composé d'un site central C-SIS et par un site par pays, le N-SIS, l'ensemble de C-SIS et N-SIS constitue le SIS. En 2006 le SIS de deuxième génération, le SISII a été établi[640], il a désormais vocation à stocker des données biométriques (empreintes digitales et photographies et les copies de mandat d'arrêt européen). L'impact sur la protection des données personnelles est particulièrement fort du fait du volume de données qu'il gère et des acteurs pouvant y accéder (Europol, Eurojust, les parquets nationaux) et enfin de la création d'une plateforme d'interconnexion avec le système d'informations sur les visas (VIS)[641]. De plus le SIS pose problème au regard du principe de finalité, il cumule les finalités de protection de la sécurité publique et de contrôle de l'immigration. Ainsi les données contenues dans le SIS peuvent faire l'objet d'un traitement ultérieur en matière d'immigration et elles peuvent être liées à Eurodac, système qui stocke les empreintes digitales des demandeurs d'asile et au VIS. Les règles visant à protéger les données personnelles sont encadrées par le règlement n °1978/2006 sur l'établissement du SIS ainsi que par la décision 2007/533/JAI. Ces deux instruments font référence à la directive 95/46 ainsi qu'au règlement 45/2001 comme cadre juridique général. Vu la catégorie des données contenues dans le SISII il est établi un contrôle au niveau de l'État membre ainsi qu'un contrôle au niveau européen [642] . De plus, depuis avril 2013, la responsabilité du contrôle de la protection des données pour le Système SISII a été transférée de l'autorité de contrôle commune Schengen vers le Contrôleur européen à la protection des données personnelles (ci-après « CEDP »), ce nouveau système permet une coordination entre les autorités de contrôle nationales et le CEDP. D'ailleurs le CEDP a contribué à l'amélioration du SIS intervenant avec nombreuses recommandations[643]. Pour renforcer le cadre juridique de l'espace Schengen, le système est à nouveau objet d'amélioration, grâce à la proposition « Frontières intelligentes », qui devra prévoir un système d'entrées - sorties et un programme d'enregistrement des voyageurs pour l'espace Schengen[644]. Cette proposition a fait l'objet de critiques de la part du G29 lequel estime cette proposition insuffisamment justifiée au regard des principes de nécessité et de proportionnalité[645]. La licéité du traitement des données

---

640 Règlement n° 1987/2006 du Parlement européen et du Conseil du 20 décembre 2006 sur l'établissement, le fonctionnement et l'utilisation du Système d'information Schengen de deuxième génération. Voy. aussi la décision 2007/533/jai du Conseil du 12 juin 2007 sur l'établissement, le fonctionnement et l'utilisation du Système d'information Schengen de deuxième génération.

641 Voy. sur ce point les inquiétudes du CEDP, Avis 2006/C91/11 publié au JOUE le 19/4/2006 et la position de P. Hustinx dans son article, « Data Protection and Schengen Governance », (Conférence « Upholding Freedom of Movement : an Improved Schengen Governance », Parlement européen, Bruxelles, 8 février 2012).

642 L'autorité nationale de contrôle est chargée de contrôler en toute indépendance la licéité du traitement des données dans le cadre du SISII sur leur territoire et leur transmission. D'ailleurs au niveau européen la création d'une autorité de contrôle commune (ACC) garantissait le contrôle sur les accès au SIS mais depuis avril 2013 (mise en service de SISII) le CEDP a hérité ses fonctions.

643 Notamment sur la sécurité des données, l'interdiction ou la limitation apporté à l'interopérabilité des systèmes, au nom du principe de finalité limitée etc.

644 Le 28 février 2013 la Commission a présenté une proposition dite Smart Borders, l'objectif est de contrôler automatiquement la durée du séjour maximum (de la durée de 90 jours de citoyens de pays extérieurs de l'espace Schengen) grâce aux données sur les voyageurs et leurs données biométriques. Concernant le système d'enregistrement des voyageurs (fréquents, par exemple hommes d'affaires) il s'appuierait sur un système de numéros d'identification et sur des données biométriques.

645 Voy. Opinion 05/2013 on Smart Borders, juin 2013.

personnelles dans le système d'information SIS est illustrée par l'affaire *Dalea c. France*[646]. Dans cette affaire, le requérant s'est vu refuser un visa touristique pour la France, car les autorités avaient indiqué dans le SIS que son entrée devait être refusée. Le requérant a cherché en vain à accéder à ses données devant la CNIL et en dernier recours devant le Conseil d'État. La CEDH dans son raisonnement a conclu que le recours du requérant au titre de l'article 8 était irrecevable car le signalement du requérant dans le SIS était prévu par la loi française, poursuivant le but légitime de protéger la sécurité nationale et il existait des mesures suffisantes pour le protéger contre des décisions arbitraires. De plus le requérant n'avait pas montré en quoi il avait subi préjudice de son impossibilité d'entrer dans l'espace Schengen, la Cour avait estimé que l'ingérence dans son droit au respect de la vie privée était proportionnée. En 2016, la Commission européenne a réalisé une évaluation du SIS[647] montrant que des mécanismes nationaux ont été mis en place pour permettre aux personnes concernées d'accéder, de corriger et de supprimer leurs données personnelles dans le SIS II ou d'obtenir une compensation liée à des données inexactes. Pour améliorer l'efficience et l'efficacité du SIS II, la Commission européenne a présenté trois propositions de règlements: un règlement concernant l'établissement, le fonctionnement et l'utilisation du SIS dans le domaine des contrôles aux frontières, qui abrogera le règlement SIS II ; un règlement sur la création, le fonctionnement et l'utilisation du SIS dans le domaine de la coopération policière et de la coopération judiciaire en matière pénale, qui abrogera notamment la décision SIS II ; et un règlement sur l'utilisation du SIS pour le retour des ressortissants de pays tiers en séjour irrégulier. Les propositions permettent le traitement d'autres catégories de données biométriques en plus des photographies et des empreintes digitales, qui font déjà partie du régime actuel du SIS II. Les empreintes faciales, les empreintes palmaires et les profils ADN seront également stockés dans la base de données SIS. En outre, alors que le règlement SIS II et la décision SIS II prévoyaient la possibilité de rechercher avec une empreinte digitale une personne, les propositions rendent cette recherche obligatoire si l'identité de la personne ne peut être établie autrement. Les images faciales, les photographies et les empreintes palmaires seront utilisées pour rechercher le système et identifier les personnes, lorsque cela deviendra techniquement possible. Les nouvelles règles sur les attributs biométriques présentent des risques particuliers pour les droits des individus. Dans son avis[648], le CEDP a relevé que les données biométriques sont très sensibles et que leur introduction dans une base de données à grande échelle devrait reposer sur une évaluation fondée sur des preuves de la nécessité de les inclure dans le SIS. En d'autres termes, la nécessité de traiter les nouvelles données devrait être démontrée. Le CEPD a également estimé qu'il était nécessaire de préciser davantage le type d'informations pouvant être incluses dans le profil ADN. Le profil ADN pouvant inclure des informations sensibles (l'exemple le plus notable étant les problèmes de santé révélateurs d'informations), les profils ADN stockés dans le SIS doivent contenir : « uniquement les informations minimales strictement nécessaires à l'identification des personnes disparues et exclure explicitement l'information sanitaire, l'origine raciale et toute autre information

---

646 CEDH, Dalea c. France, req. n° 964/07, 2 février 2010.

647 Voy. SIS II SCG, *The Schengen Information System. A guide for exercising the right of access.*

648 EDPS, « Opinion on the new legal basis of the Schengen Information System », Opinion 7/2017, 2 May 2017.

sensible ». Les propositions établissent toutefois des garanties supplémentaires pour limiter la collecte et le traitement ultérieur des données à ce qui est strictement nécessaire et opérationnel, et l'accès est limité aux personnes ayant un besoin opérationnel de traiter les données personnelles.

2) Le système d'information sur les visas (VIS)

89 La protection des frontières extérieures. Le système commun d'identification des données relatives aux visas a été créée en 2004, par la décision du Conseil[649], permettant aux États Schengen d'échanger des données sur les visas par l'intermédiaire d'un système qui connecte les consulats des États Schengen situés dans des pays non membres de l'Union avec les points externes de passage des frontières de tous les États Schengen. Le VIS a pour but la mise en œuvre d'une politique commune des visas en simplifiant l'examen des demandes de visa et les contrôles aux frontières extérieures tout en contribuant à la prévention des menaces dirigées contre la sécurité intérieure des États membres. Concrètement le VIS est une base de données qui regroupe les empreintes digitales des demandeurs d'asile. Il permet notamment de contrôler, aux points de passage des frontières extérieures, la véritable identité d'une personne qui détient un visa biométrique. Il comprend les données du demandeur, l'accès est permis aux seules autorités en charge des visas des États membres et seulement sous certaines conditions les autorités nationales de police et Europol peuvent demander l'accès aux données saisi dans le VIS dans le but de prévenir et de détecter des actes de terrorisme et infractions pénales [650.] Le système permet un échange entre États Schengen de demandes de visa afin d'éviter le *visa shopping* et de lutter contre la fraude. Il est aussi un instrument pour appliquer le règlement Dublin II et III pour la détermination du pays de l'UE responsable de l'examen d'une demande d'asile. Les données qui en font partie concernent les données biographiques (identité, histoire des visas accordés et refus) et biométriques. Des critiques ont été soulevées par le CEDP et le G29 quant au caractère incomplet de ce système puisqu'il faut consulter d'autres bases de données pour avoir l'ensemble des informations concernant la personne[651]. Concernant l'accès aux données, peuvent y accéder, le personnel autorisé, l'Office européen d'Europol et les services de police nationaux, ce qui semble contraire au principe de finalité qui devrait cantonner l'usage du VIS à des objectifs liés à la politique commune des visas[652]. Chaque État membre est responsable de la licéité du traitement, de l'utilisation des données et de la sécurité du traitement, le temps de conservation est fixé à cinq ans. En principe le transfert des données

649 Décision 2004/512/CE du Conseil, JO L213 du 15/06/2004, règlement 767/2008, JO L218 du 13/08/2008, décision 2008/633/ JAI du Conseil JO L218 du 13/08/2008.

650 Le cadre juridique du VIS se fonde sur la décision 2004/512/CE du Conseil du ! juin 2004, sur la décision n°2008/633/JAI du Conseil du 23 juin 2008 et sur le règlement n°767/2008 du 9 Juillet 2008 et sur le règlement 810/2009 du 13 juillet 2009.

651 Voy. CEDP, Avis, 2006/C321/14, JOUE du 29 décembre 2006, p. 40 et l'avis du G29 3/2007, WP

134 Adopté le 1er mars 2007, p. 7.

652 CEDP, Avis 2006/C 97/03, p. 7.

du VIS vers des pays tiers sont interdits mais des dérogations peuvent avoir lieu lorsque l'information est nécessaire pour lutter et prévenir le terrorisme ou d'autres infractions graves. Toutefois le VIS pêche comme le SIS par ses finalités multiples.

B. Le système d'information en matière de coopération policière

90 Le système Eurodac. Afin de lutter contre la criminalité et le terrorisme, on a assisté à la prolifération des plusieurs systèmes d'informations. Le système Eurodac a été créé en 2000[653] pour comparer les empreintes digitales aux fins de l'application de la Convention Dublin sur l'examen des demandes d'asile [654] afin de déterminer lequel des États membres doit être considéré responsable d'une demande d'asile déposée dans l'Union[655]. Dans le fichier Eurodac sont stockées les empreintes digitales des personnes demandant l'asile dans un État membre, des personnes appréhendées lors du franchissement irrégulier des frontières extérieures de l'Union et des personnes se trouvant en situation de séjour irrégulier.
Les pays de l'UE peuvent ainsi vérifier si un demandeur d'asile se trouve illégalement sur son territoire ou s'il a déjà formulé une demande d'asile dans un autre État de l'UE afin de déterminer quel État membre est compétent pour examiner la demande et éviter *l'asylum shopping*. Pour éviter tout abus, les données ainsi récoltées sont conservées pour une durée de 18 mois et sont effacées de la base une fois obtenu le titre de séjour. Concernant l'accès à la base Eurodac on peut constater une évolution en plus, alors que le règlement Eurodac de 2000 respectait le principe de finalité admettant la consultation afin de mettre en œuvre la politique commune en matière d'asile, le nouveau règlement n°603/2013 permet l'accès des autorités nationales et d'Europol à la base Eurodac pour prévenir et détecter des infractions pénales graves. Le risque de dérive et de discriminations a été soulevé par la CEDP[656].
L'avis du CEPD concernant la proposition modifiée de règlement Eurodac se fait largement l'écho d'inquiétudes. Un point crucial dans la proposition de la Commission est l'ajout au système Eurodac, qui permet la comparaison des empreintes digitales des demandeurs d'asile aux fins de l'application efficace du règlement de Dublin (établissant les critères et mécanismes de détermination de l'État membre responsable de l'examen d'une demande d'asile présentée dans l'un des États membres par un ressortissant d'un pays tiers), d'une disposition permettant à l'avenir aux autorités répressives d'accéder aux données Eurodac, aux fins de prévention et de détection des infractions terroristes et autres infractions pénales graves ainsi que des enquêtes en la matière. S'il paraît évident qu'un tel mécanisme peut s'avérer utile dans la lutte

653 Créée par le règlement n° 2725/2000 du Conseil du 11 décembre 2000, le règlement n° 407/2002 a fixé les modalités d'application. Le nouveau règlement Eurodac n° 603/2013 est entré en vigueur le 20 juillet 2015.

654 Règlement n° 2725/2000 du 11 décembre 2000 concernant la création du système Eurodac pour la comparaison des empreintes digitales aux fins d'application de la convention Dublin.

655 Mise en place en 2003, la base de données Eurodac collecte les empreintes digitales des demandeurs d'asile, afin de déterminer l'État membre responsable de l'examen d'une demande.

656 V. l'Avis du CEDP 2009/C 229/02 ; l'avis 2010 C/92/01 ; 2011/C/101/03 sur la proposition de modifiée de règlement du Parlement européen et du Conseil concernant la création du système Eurodac pour la comparaison des empreintes digitales

contre la criminalité, il s'agit néanmoins incontestablement d'une « intrusion grave dans les droits d'un groupe de personnes vulnérable en quête de protection »[223], comme le relève le CEDP. Cette disposition peut apparaître en outre comme discriminatoire, ou stigmatisante à tout le moins, dans la mesure où des demandeurs d'asile pourraient ainsi être identifiés grâce aux données Eurodac, si une empreinte digitale est relevée sur le lieu d'un délit, alors que d'autres personnes y échapperont parce que ce type de données n'est pas disponible pour tous les autres groupes de la société, la question se pose de savoir si, s'agissant de cet argument, l'équilibre est véritablement rompu dans la balance entre protection des droits fondamentaux et sauvegarde de la sûreté. Face à la multiplication des bases de données, il existe des erreurs et dérives. Une des questions essentielles est celle de l'authentification des personnes habilitées à accéder aux données, ainsi que les moyens de lutter contre les accès illégaux. Il s'agit de garantir en premier lieu la sécurité technique des bases de données personnelles, qui est à la charge des États, un ultérieur risque est lié à l'interopérabilité des bases de données, le paradoxe consiste dans le fait que pour fonctionner efficacement, les bases de données doivent être interopérables, ce qui renforce leur fragilité, par le recours aux mêmes normes de sécurité[657].

En mai 2016, la Commission a présenté une proposition relative à une nouvelle refonte du règlement Eurodac, dans le cadre d'une réforme visant à améliorer le fonctionnement du régime d'asile européen commun [658] . La refonte proposée est importante car elle étendra considérablement la portée de la base de données initiale Eurodac. Eurodac a été initialement créé pour soutenir la mise en œuvre du « *Common European Asylum System* » (CEAS), en fournissant des preuves d'empreintes digitales pour permettre de déterminer quel État membre est responsable de l'examen d'une demande d'asile déposée dans l'Union. La refonte proposée étendra la base de données pour faciliter le retour des migrants en situation irrégulière. Les autorités nationales pourront consulter la base de données pour identifier les ressortissants de pays tiers qui séjournent irrégulièrement dans l'Union ou qui sont entrés irrégulièrement dans l'Union, afin d'obtenir des preuves pour aider les États membres à renvoyer ces personnes. De plus, alors que le régime juridique actuellement en vigueur ne requiert que la collecte et le stockage des empreintes digitales, la proposition introduit la collecte d'images faciales individuelles, qui constitue un autre type de données biométriques.

La proposition abaisserait également l'âge minimum des enfants dont les données biométriques peuvent être collectées - à six ans au lieu de quatorze ans –, ce qui correspond à l'âge minimum prévu par le règlement de 2013. La portée élargie de la proposition signifie qu'elle constituera une ingérence dans les droits à la vie privée et à la protection des données d'un plus grand nombre de personnes susceptibles d'être incluses dans la base de données.

---

657 Face à l'évolution extrêmement rapide des technologies de sécurité, dans le contexte sécuritaire actuel et au regard des exigences liées à la coopération policière et judiciaire pénale européenne, les systèmes de protection mis en place peuvent aboutir à leur contournement par une série de pratiques.

658 Voy. European Commission, Proposal for a Regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast), COM (2016) final, 4 May 2016.

Pour contrebalancer cette interférence, la proposition et les amendements proposés par la commission LIBE du Parlement européen[659], cherchent à renforcer les exigences en matière de protection des données

Les trois fichiers, SIS, VIS, Eurodac, sont des instruments pour la mise en place d'une police administrative spéciale « qui ambitionne de sauvegarder l'ordre public par un contrôle de l'accès au territoire et un encadrement du séjour des ressortissants étrangers » [660] . Il faut remarquer que les fichiers sont censés être européens mais les États sont les seuls à juger de l'opportunité de l'inscription d'un signalement dans la base de données puisqu'il n'existe pas de ligne directrice présidant au choix des entrées. De plus les fichiers migratoires sont de plus en plus systématiques et massifs, cela se traduit par une extension de leurs finalités et le fait qu'ils deviennent des outils d'enquête policière. Or, le respect des règles est fondamental pour empêcher que les techniques de fichage ne placent les individus en surveillance continue. Ainsi le respect de ces règles est soumis au contrôle des autorités indépendantes et des agences européennes.

En plus d'améliorer les fonctionnalités des trois principaux systèmes d'information – SIS II, VIS et Eurodac – la Commission a proposé la création d'un quatrième système de gestion centralisée des frontières à l'adresse des ressortissants de pays tiers : le système d'entrée-sortie (SEE), qui devrait être mis en œuvre d'ici 2020[661].

§2. Le traitement des données personnelles par les agences européennes

91 Le respect des droits des personnes dans la lutte contre la criminalité. L'espace Schengen ayant été créé pour la première fois dans le cadre d'un accord international indépendant du droit de l'UE, le système d'information Schengen (SIS) élaboré à partir d'accords multilatéraux a ensuite été intégré au droit de l'UE. Le système d'information sur les visas (VIS), Eurodac, Eurosur et le système d'information des douanes (CIS) ont été créés en tant qu'instruments régis par le droit de l'Union. Lesdits systèmes d'information communs ont été mis en place pour faciliter la coopération et l'échange de données entre autorités nationales et européennes compétentes à des fins spécifiques dans les domaines de la protection des frontières, de l'immigration, de l'asile et des douanes. Au-delà de ces systèmes d'informations, des autorités européennes spécialisées dans la lutte contre la criminalité transfrontalière ont été

659 Voy. European Parliament, « Report on the proposal for a regulation of the European Parliament and of the Council on the establishment of 'Eurodac' for the comparison of fingerprints for the effective application of [Regulation (EU) No. 604/2013 establishing the criteria and mechanisms for determining the Member State responsible for examining an application for international protection lodged in one of the Member States by a third-country national or a stateless person], for identifying an illegally staying third-country national or stateless person and on requests for the comparison with Eurodac data by Member States' law enforcement authorities and Europol for law enforcement purposes (recast) », PE597.620v03-00, 9 June2017.

660 V. TCHEN, *Droits des étrangers*, Ellipses, 2006, p. 7-24.

661 European Commission (2016), Proposal for a Regulation of the European Parliament and of the Council establishing an Entry/Exit System (EES) to register entry and exit data and refusal of entry data of third country nationals crossing the external borders of the Member States of the European Unionand determining the conditions for access to the EES for law enforcement purposes and amending Regulation (EC) No. 767/2008 and Regulation (EU) No. 1077/2011, COM(2016) 194 final, Brussels, 6 April 2016.

créées, telles qu'Europol, Eurojust et le Parquet européen. En effet, l'élimination progressive de contrôles aux frontières au sein de l'Union a facilité la libre circulation des citoyens européens, mais a également permis aux criminels d'agir plus facilement au niveau transnational. Afin de relever le défi de lutte contre la criminalité transfrontalière, l'espace de liberté, de sécurité et de justice comprend des mesures visant à promouvoir la coopération policière et judiciaire en matière pénale. Des mesures spécifiques ont été adoptées pour lutter contre la criminalité transnationale et veiller à ce que les droits des victimes, des suspects et des détenus soient protégés dans l'Union. Les agences de l'Union européenne jouent un rôle crucial dans le soutien à la coopération opérationnelle. Elles participent, en effet, à l'évaluation des menaces communes pour la sécurité, contribuent à la définition des priorités communes pour l'action opérationnelle et facilitent la coopération et les poursuites transfrontières. Avant de présenter les traitements de données personnelles mis en œuvre au sein de l'UE, il est nécessaire d'étudier les modalités et fonctionnement des agences qui traitent les données. Nous verrons dans un premier temps l'organisation de l'Agence Europol A) dans un second temps nous analyserons l'agence Eurojust B) et Frontex C).

A. Le traitement de données personnelles par Europol

92 Une réponse aux menaces criminelles. Les réseaux criminels et terroristes à grande échelle constituent une menace importante pour la sécurité intérieure de l'Union ainsi que pour la sécurité de ses citoyens. Cette menace montre que les groupes criminels diversifient de plus en plus leurs activités (« polycriminalité »), et que ces dernières revêtent un caractère de plus en plus transfrontalier[662]. Il convient, dès lors, que les autorités répressives nationales coopèrent plus étroitement avec leurs homologues des autres États membres[663]. Dans ce contexte, il est nécessaire de donner à Europol les moyens de mieux soutenir les États membres en matière de prévention de la criminalité ainsi que d'analyses et d'enquêtes criminelles à l'échelle de l'Union. S'agissant de la coopération policière (art. 87 et 88 TFUE), on pense évidemment à Europol[664], mais également à l'intensification de l'échange de données notamment aux données PNR[665] mettant à l'épreuve le droit au respect à la vie privée et le droit à la protection de ses données personnelles protégés par la Charte. Europol, l'office européen de police, créé en

662 S. BRAMMERTZ, S. DE VREESE, J. THYS, *La collaboration policière transfrontalière*, Bruxelles, Politeia, 1993, p. 173-192.

663 S. BRAMMERTZ, « La coopération policière en Europe et dans l'Euroregio Meuse-Rhin », *Déviance et Société*, 1992, vol. 16, n° 2, p ; 219-229.

664 A. BOUMEDIENNE-THIERY., D. COHN-BENDIT, *Europol, excroissance opaque de l'Union européennee*, Le Monde, 20 octobre 1999.

665 Voy. la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JO L 119 du 4/5/2016, p. 132-149 ; également l'avis rendu par la Cour relatif à l'accord PNR avec le Canada, CJUE, (Grande chambre), 26 juillet 2017, Avis 1/15 rendu en vertu de l'article 218, paragraphe 11, TFUE.

1998[666] et sur décision du Conseil en 2009[667], devient une agence communautaire. Son statut juridique actuel en tant qu'institution de l'UE repose sur le règlement relatif à l'Agence de coopération de l'Union européenne en matière de répression (règlement Europol)[668]. Le but d'Europol est d'aider à prévenir et à enquêter sur le crime organisé, le terrorisme et d'autres formes d'infractions énumérées à l'annexe I du règlement Europol, qui touchent plusieurs États membres. Son objectif est d'aider les services répressifs des États membres à prévenir et à combattre le crime organisé, le terrorisme et d'autres formes de criminalité grave affectant au moins deux États membres. Europol a d'emblée été conçu comme un lieu de centralisation et d'échange d'informations. Implanté à la Haye, il dispose aussi d'unités nationales Europol (ci-après UNE) dans chaque états membre. Europol et UNE peuvent saisir et récupérer des données du système d'information Europol crée pour fournir des données des personnes suspectées ou condamnées pour une infraction pénale relevant de la compétence d'Europol ou des personnes à l'égard desquelles il existe des éléments de fait indiquant qu'elles s'apprêtent à commettre de telles infractions. Récemment, le Centre européen de lutte contre la cybercriminalité a été créé à Europol le 1 janvier 2013 [669] , il s'agit d'une plateforme communautaire relative à la cybercriminalité. En termes de coopération policière, l'importance d'Europol doit être soulignée, à la fois en termes d'échange et d'analyse d'informations et en termes de support opérationnel. L'approbation par le Conseil, le 4 décembre 2015, d'un texte de compromis sur un projet[670] de règlement relatif à Europol émanant de la Commission devrait contribuer à améliorer la coopération policière entre États car Europol devrait avoir plus de moyens pour agir comme « le centre névralgique de l'échange d'informations entre les services répressifs des États membres »[671]. Les règles générales applicables à ce système sont précisées dans la décision 2009/371/JAI et les données qu'il contient sont celles relatives : aux personnes

---

666 La Convention créant Europol sur la base du Traité de Maastricht (créant le troisième pilier) fut approuvée le 26 juillet 1995 et après ratification par les États membres entra en vigueur le 1er octobre 1998. Conformément à la logique du troisième pilier, Europol bien que crée par un acte de la communauté, n'était pas une institution européenne, mais une organisation internationale directement financé par les États membres, et disposant d'une réglementation autonome par rapport au droit communautaire.

667 Décision du Conseil 2009/371/JAI du 6 avril 2009.

668 Voy. Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ 2016 L 135, p. 53. Voy. considérant 5 du Règlement: « Le présent règlement vise à modifier et à étendre les dispositions de la décision 2009/371/JAI ainsi que des décisions du Conseil 2009/934/JAI (1), 2009/935/JAI (2), 2009/936/JAI (3) et 2009/968/JAI (4) portant application de la décision 2009/371/JAI. Étant donné que les modifications à apporter à ces décisions sont significatives tant par leur nombre que par leur nature, il convient, dans un souci de clarté, de remplacer intégralement ces décisions pour les États membres liés par le présent règlement. Europol instituée par le présent règlement devrait remplacer Europol qui avait été institué par la décision 2009/371/JAI, qui, par conséquent, devrait être abrogée, et en assumer les fonctions".

669 Voy.. Avis du 29 juin 2012 du CEDP, sur l'institution du Centre européen de lutte contre la cybercriminalité.

670 http://www.gdr-elsj.eu/wp-content/uploads/2016/01/Proposition-Europol.pdf.

671 Europol a été créé en 1998, l'office européen de police dispose d'unités nationales dans chaque État membre. Son objectif est de contribuer à la prévention du crime organisé, du terrorisme et d'autres formes de criminalité grave, ainsi qu'aux enquêtes affectant au moins deux États membres. Le système d'information Europol est une base de données qui permet aux États membres d'échanger des renseignements en matière criminelle portant sur des personnes suspectés ou condamnées ou des personnes à l'égard desquelles il existe des éléments de fait indiquant qu'elles s'apprêtent à commettre des infractions pénales. Les activités criminelles utilisent de plus en plus les systèmes électroniques pour commettre les infractions. Pour cette raison au sein d'Europol a été créé le 1er janvier 2013 le centre européen de la lutte contre la cybercriminalité.

soupçonnées d'avoir commis une infraction relevant de la compétence d'Europol[672] ou déjà condamnées pour une telle infraction ; pour lesquelles il existe des indices concrets ou des bonnes raisons de croire qu'elles commettront de telles infractions[673]. Il s'agit de données limitées qui ne peuvent être conservées que pendant une durée nécessaire, ce qui doit faire l'objet d'une évaluation tous les trois ans. Au niveau des États membres, l'autorité de contrôle nationale surveille le traitement des données à caractère personnel traitées par Europol. Le CEDP est chargé de surveiller et de garantir la protection des droits et libertés fondamentales des personnes physiques en ce qui concerne le traitement des données à caractère personnel par Europol et de conseiller Europol et les personnes concernées sur toutes les questions relatives au traitement des données à caractère personnel. À cette fin, le CEDP agit en tant qu'organe d'enquête et de plainte et travaille en étroite coopération avec les autorités nationales de contrôle[674]. De plus un comité de coopération a été créé avec une fonction consultative. Il est composé d'un représentant de l'autorité de contrôle nationale de chaque État membre et du CEDP.

Concernant les droits, chaque individu a le droit d'accès à toutes données à caractère personnel qu'Europol peut détenir, en plus d'un droit de demander que ces données à caractère personnel soient vérifiées, rectifiées ou supprimées. Le droit d'accès s'exerce à l'initiative des personnes physiques concernées, auprès de l'État membre de son choix, qui doit saisir sans délai Europol lequel aura trois mois pour répondre[675]. Le refus des demandes d'accès peut résider dans le fait de protéger la sécurité et l'ordre public des États membres, dans la nécessité de ne pas compromettre une enquête ou de protéger les droits et libertés d'un tiers. Toute personne qui n'est pas satisfaite d'une décision d'Europol concernant l'exercice de ces droits peut former un recours devant la Cour de justice[676].

Toute personne qui a subi un préjudice du fait d'un traitement illégal a le droit de recevoir une indemnisation pour le préjudice subi, soit par Europol, soit par l'État membre responsable, en introduisant un recours devant la CJUE dans le premier cas ou devant la juridiction nationale compétente dans le deuxième cas[677]. Concernant le transfert des données Europol peut, sous certaines conditions, transférer des données à caractère personnel à un organe de l'Union ou à une autorité d'un pays tiers ou à une organisation internationale[678]. Des difficultés demeurent dans le cadre des transferts aux pays tiers, notamment dans le cadre de l'accord *Swift*[679]. En

672 Mais l'infraction est définie au regard du droit national applicable.

673 Articles 11à 13 de la Décision 2009/371/JAI précitée.

674 Voy. Art. 43 et 44.

675 Le G29 déjà en 2005 à l'occasion d'un avant-projet du texte de la décision 2009/371/JAI avait exprimé des inquiétudes notamment à l'égard du caractère particulièrement large de ces dérogations au principe d'information du sujet du traitement de données.

676 Voy. Art. 48.

677 Conformément à l'article 340 du traité sur le fonctionnement de l'Union européenne.

678 Voy. Art. 24 et 25.

679 L'accord TFTP dit accord Swift a été approuvé par le Parlement européen le 7 juillet 2010 et il vise à donner une base juridique à une situation de fait découverte grâce au scandale Swift en 2006 par le New York Times. Les États-Unis espionnaient les données Swift (Society for Worldwide Interbank Financial Telecommunication) et toutes les transactions

particulier, les requêtes adressées à Europol par les autorités américaines pour demander le transfert de données étaient générales, abstraites et trop peu spécifiques pour permettre une évaluation adéquate de la nécessité de transmission des données demandées[680]. Le G29 et le Parlement européen ont également exprimé leurs préoccupations, notamment sur l'impossibilité de contrôler la durée de conservation des données après leur transmission vers les États-Unis, ou encore la limitation des traitements ultérieurs aux finalité pour lesquelles les données avaient été collectées. Le CEDP a soulevé des critiques, il relève que les règles existant avant la décision 2009/371/JAI étaient plus protectrices car les données conservées faisant l'objet d'une évaluation tous les ans[681]. De plus dans son avis, il souligne que le principe de finalité n'est pas respecté puisque l'Agence peut traiter les données et seulement dans un deuxième temps évaluer leurs utilités. Ainsi Europol traite, analyse, stocke des données, échange et partage des renseignements et facilité des enquêtes policières mais son apport se prolonge dans le cadre des relations extérieures. En effet, l'Union européenne a conclu des accords d'échange d'information avec des États tiers, l'accord *Passenger Name Record* (PNR) avec les États-Unis, le Canada et l'Australie et l'accord *Swift* conclu avec les États-Unis concernant le transfert de données financières entre l'UE et les USA. Ces accords ont permis aux autorités répressives des États parties d'une part de déceler les liens existants entre certains passagers et des actes ou activités liés au terrorisme et d'autres part une mise en réseau des banques de données policières des États membres.

Le Centre européen de lutte contre le terrorisme a été créé en janvier 2016 pour fournir un soutien opérationnel aux États membres dans le cadre d'enquêtes liées à des infractions terroristes. Il vérifie les données opérationnelles en direct par rapport aux données qu'Europol possède déjà, apportant rapidement des pistes financières, et analyse tous les détails d'enquête disponibles pour aider à compiler une image structurée d'un réseau terroriste[682]. Le Centre européen de lutte contre le trafic de migrants a été créé en février 2016, à la suite d'une réunion du Conseil en novembre 2015, pour aider les États membres à cibler et à démanteler les réseaux criminels impliqués dans le trafic de migrants. Il agit comme un centre d'information soutenant les bureaux régionaux de la force opérationnelle de l'UE à Catane (Italie) et au Pirée (Grèce), qui aident les autorités nationales dans plusieurs domaines, notamment le partage de renseignements, les enquêtes pénales et les poursuites pénales. Au-delà des critiques et des lacunes, il est possible de noter qu'Europol même pendant la première phase intergouvernementale a toujours été sensible à la question relative à la protection des données personnelles. Par ailleurs, la communautarisation d'Europol en 2009 a sûrement eu le mérite de

financières internationales dans le cadre de leur programme de lutte contre le terrorisme. L'accord TFTP donne aux autorités américaines l'accès aux données bancaires européennes stockées chez Swift.

680 Cependant un avis de l'ACC plus récent montre des avancements notamment dans la justification des requêtes mais continue à porter une appréciation négative sur le respect du principe de proportionnalité concernant le volume massif et régulier de transfert de données de l'UE vers les États-Unis concernant des personnes non suspectes. Voy. ACC Europol 8 avril 2013, TFTP Agreement Inspection Report.

681 Voy. Sur ce point l'avis 2007/C du 27 octobre 2007 du CEDP sur la proposition du Conseil portant création de l'Office européen de police (Europol) COM (2006) 817, JOUE C 225/03.

682 Voy. Le rapport sur le terrorisme en Europe disponible à l'adresse : https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report

faire converger le droit européen en matière de protection des données entre les différents piliers[683].

B. Le traitement des données par Eurojust

93 La protection des données dans le domaine de la coopération judiciaire. Crée en 2002, Eurojust[684] est l'organe chargé de promouvoir la coopération judiciaire dans les enquêtes et poursuites des crimes graves touchant au moins deux États membres. Les fonctions d'Eurojust sont exercées par des juges ou des membres du ministère public désignés par chaque État. Eurojust peut traiter des données à caractère personnel pour autant que cela soit nécessaire à la réalisation de ses objectifs. Eurojust répond aux demandes d'assistances émanant des autorités nationales compétentes des États membres. En retour, Eurojust peut demander aux États membres d'entreprendre des enquêtes ou des poursuites. Les données qui font l'objet du traitement par Eurojust sont uniquement celles relatives aux personnes suspectées d'avoir commis un délit ou condamnées pour un délit mais aussi aux victimes et aux témoins[685]. L'accès aux données est permis seulement aux membres des autorités nationales ainsi qu'au personnel Eurojust. Eurojust prend des mesures pour assurer la protection des données correspondant au moins à celle qui résulte de l'application des principes de la convention 108 du Conseil de l'Europe [686] . Les principes de licéité et de loyauté et de proportionnalité et nécessité du traitement doivent être respectées, toute personne a droit d'accès aux données et peut demander la rectification ou l'effacement si les données ne correspondent pas à la réalité. Toutefois des limites au droit d'accès peuvent se vérifier afin d'éviter de compromettre l'enquête. Un organe de contrôle commun (OCC) indépendant est établi pour contrôler les activités d'Eurojust et tous les trois ans est prévue une vérification[687]. Comme pour Europol toute personne qui n'est pas satisfaite d'une décision d'Europol concernant l'exercice de ses droits peut former un recours devant le comité des recours de l'OCC. Les décisions de l'OCC sont définitives et contraignantes à l'égard d'Eurojust. En revanche si une erreur de droit ou de fait commise par Eurojust a constitué un préjudice, la partie lésée peut former uniquement un recours devant le tribunal compétent de l'État membre dans lequel résulte le préjudice. La Commission européenne a présenté une proposition de règlement visant à réformer Eurojust en juillet 2013. Cette proposition était accompagnée d'une proposition visant à créer un bureau du Procureur européen dans le but de lutter contre les infractions pénales portant atteinte aux intérêts

---

[683] C. CHEVALLIER-GOVERS, *De la coopération à l'intégration policière dans l'Union européenne*, Bruxelles, Bruylant, 1999, p. 250.

684 Institué par la décision du Conseil 2002/187/JAI et amendé par la décision du Conseil 2009/426/JAI du 16 décembre 2008. En 2013 la Commission européenne a adopté des mesures législatives instituant le parquet européen et réformant Eurojust. Voy. L'avis du CEDP du 5 mars 2014.

685 Les données qui peuvent faire l'objet d'un traitement concernent : le nom, date, lieu de naissance, nationalité, coordonnées, profils ADN, empreintes, photographies etc. La liste est donc très étendue mais ces données peuvent être traités que dans le cadre précisément défini d'une enquête.

686 Art. 14 à 24 de la décision.

687 Art. 23 de la décision.

financiers de l'UE[688]. Le Parquet européen sera mis en place dans le cadre de la procédure de coopération renforcée, qui permettra à au moins neuf États membres d'établir une coopération avancée dans un domaine relevant des structures de l'Union, sans la participation des autres pays de l'Union. La République tchèque, l'Estonie, la Finlande, la France, l'Allemagne, la Grèce, la Lettonie, la Lituanie, le Luxembourg, le Portugal, la Roumanie, la Slovénie, la Slovaquie et l'Espagne ont tous adhéré à la coopération renforcée. L'Autriche et l'Italie ont exprimé leur intention d'adhérer. Le Parquet européen sera compétent pour enquêter et poursuivre les fraudes et autres délits de l'Union portant atteinte aux intérêts financiers de l'Union, dans le but de coordonner efficacement les enquêtes et les poursuites dans les différents ordres juridiques nationaux et d'améliorer l'utilisation des ressources et l'échange d'informations au niveau européen. La proposition prévoit des garanties strictes pour garantir les droits des personnes impliquées dans les enquêtes du Parquet européen, conformément à la législation nationale, au droit de l'Union et à la Charte des droits fondamentaux de l'Union européenne. Les mesures d'investigation qui concernent principalement les droits fondamentaux nécessiteront une autorisation préalable d'un tribunal national. Les enquêtes du Parquet feront l'objet d'un contrôle juridictionnel par les tribunaux nationaux. Le règlement sur la protection des données des institutions de l'union[689] s'appliquera au traitement des données personnelles administratives effectuées par le Parquet européen. Pour le traitement de données à caractère personnel liées à des questions opérationnelles, telles qu'Europol, le Parquet européen disposera d'un régime de protection des données autonome similaire à celui qui régit les activités d'Europol et d'Eurojust. Les règles de protection des données du Procureur sont donc presqu'identiques aux règles de la directive sur la protection des données pour les autorités de police et de justice pénale. Selon la proposition relative à la création du Parquet européen, le traitement des données à caractère personnel doit respecter les principes de licéité et proportionnalité, de limitation de la finalité, de minimisation des données, d'intégrité et de confidentialité. La proposition prévoit également les principes de sécurité du traitement et de responsabilité, exigeant que le Parquet européen mette en œuvre des mesures techniques et organisationnelles appropriées pour assurer un niveau de sécurité approprié aux risques posés par le traitement, l'évaluation préalable au traitement. Par exemple, le traitement impliquant l'utilisation de nouvelles technologies est susceptible d'entraîner un risque élevé pour les droits des individus. Enfin, la proposition prévoit la désignation d'un responsable de la protection des données par le collège, qui doit être dûment associé à toutes les questions relatives à la protection des données à caractère personnel et veiller au respect des dispositions de la législation sur la protection des données.

688 European Commission (2013), « Proposal for a Council Regulation on the establishment of the European Public Prosecutor's Office », COM(2013) 534 final, Brussels, 17 July 2013, Art. 26 (4).

689 Regulation (EC) No. 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the institutions and bodies of the Community and on the free movement of such data, OJ 2001 L 8.

C. Le traitement des données par Frontex

94 La protection des données personnelles dans la gestion des frontières externes de l'Union. L'agence Frontex (Agence européenne pour la gestion de la coopération opérationnelle aux frontières extérieures des États membres de l'Union européenne) a été créée en 2004[690]. Elle coordonne les activités des garde-frontières externes de l'Union et aide les États membres dans la mise en œuvre des règles communautaires relatives aux frontières extérieures. L'agence dispose d'un système qui est susceptible de contenir des données à caractère personnel. Ce système a été critiqué par le CEDP puisqu'il ne contient aucune règle précise sur la protection des données ni des garanties des droits des personnes concernées[691]. L'étude concernant les fichiers et le rôle joué par les agences européennes dans le cadre de l'ELSJ a montré que ce domaine manque de transparence et d'unité. De plus, l'ensemble des systèmes élaborés dans l'ELSJ ne saurait pas respecter le principe de proportionnalité par rapport au but à atteindre. En effet, s'agissant de la question des délais de conservation en particulier, l'imprécision des formules employées par les différents textes, qui accordent une marge discrétionnaire considérable aux autorités concernées, montrent qu'une réforme du système est nécessaire. Ainsi le Traité de Lisbonne en instaurant une base juridique unique, l'art. 16, permet au législateur de fixer les règles relatives à la protection des personnes physiques à l'égard de leur traitement des données par les institutions, organes et organismes de l'Union, ainsi que les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Or, la Charte des droits fondamentaux a renforcé l'importance du droit à la protection des données ; ainsi l'art. 68 de la Charte prévoit que la protection des données constitue une liberté essentielle des individus. On peut espérer que la Cour de justice sera saisie de recours concernant les bases de données puisque à ce jour elle ne l'a toujours fait. Cela s'explique par la considération que la compétence de la Cour de justice se trouve limitée par exemple par les actes juridiques européens en matière des droits de la personne faisant l'objet d'un fichage puisque la prééminence est aux autorités nationales de contrôle et au juge national. C'est surtout la CourEDH qui a joué un rôle très important concernant les bases de données. Elle a reconnu notamment le droit d'information et d'accès aux personne faisant l'objet d'un fichage. Ainsi, une réforme concernant le droit à la protection des données personnelles dans le cadre de l'ELSJ a été nécessaire pour créer un système cohérent et assurer une protection efficace.

690 Créée par le Règlement CE n° 2007/2004 du Conseil du 26 octobre 2004.

691 Voy. Avis CEDP 2010 C 375/01, JOUE du 30 décembre 2010.

Section II. La réforme dans l'ELSJ

95 L'apparente antinomie entre sécurité publique et protection des données personnelles utilisée à des fins répressives. L'intervention du législateur européen pour assurer la protection des données personnelles lorsqu'elles sont utilisées à des fins répressives est relativement récente. C'est seulement avec l'art 16 du Traité de Lisbonne consacrant dans son paragraphe 2 la compétence du législateur communautaire pour l'adoption de règles en matière de protection des données personnelles qu'un cadre juridique harmonisé a vu le jour. Cette compétence du législateur communautaire est fondée sur la reconnaissance d'un droit à la protection des données personnelles, consacré comme droit fondamental par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, qui est ainsi reconnue dans toutes les matières, même pour la coopération judiciaire en matière pénale et la coopération policière. Ainsi la révision de la décision cadre n° 2008/977 JAI à travers l'adoption d'une directive relative à la protection des données personnelles en matière de justice et de police constitue un acte législatif examiné à travers la procédure de codécision. Dans sa communication de janvier 2012[692], la Commission a proposé de remplacer la décision-cadre par une directive pour encadrer le traitement des données personnelles par les autorités compétentes dans le but de prévenir et détecter les infractions pénales, d'enquêter, de poursuivre ou d'exécuter des sanctions pénales[693]. Dans la présente section, une analyse de la réforme nous amènera à nous interroger sur le fait de savoir si l'Union a réussi à éliminer l'antinomie entre sécurité publique et protection des données personnelles utilisée à des fins répressives. La reforme cherche à « protéger les libertés et droits fondamentaux des personnes physiques, et notamment leur droit à la protection des données à caractère personnel, et assurer l'échange de ces données entre autorités compétentes au sein de l'Union »[694]. D'ailleurs le CEPD a reconnu les avancées de cette réforme pour la protection des données au sein de l'Union européenne, mais déplore que les règles relatives à la police et à la justice soient inadaptées[695]. Cependant, une réforme a été nécessaire car vingt-sept autorités répressives différentes ne peuvent coopérer efficacement sans un degré minimum d'harmonisation des règles relatives à la coopération policière et judiciaire en matière pénale.

L'étude de la réforme veut vérifier la cohérence entre la protection offerte au niveau de l'ex-premier pilier et au niveau de l'ELSJ. Il est nécessaire tout d'abord d'examiner les lacunes de

---

692 Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données COM (2012) 10 final - 2012/0010 (COD).

693 Commission européenne, Communication relative à la protection de la vie privée dans un monde en réseau, Un cadre européen relatif à la protection des données, adapté aux défis du 21e siècle, COM (2012) 9 final, Bruxelles, le 25 janvier 2012, p. 4.

694 Commission européenne, Proposition de directive du Parlement européen et du Conseil, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, COM (2012) 10 final, Bruxelles, le 25 janvier 2012, p. 7.

695 Voy. le président du CEDP, P. Hustinx, Newsletter du CEPD, n°31, 28 janvier 2012, p. 3.

la décision-cadre (§1) pour passer à l'analyse du nouveau cadre juridique et vérifier si l'Union européenne a su élaborer et affirmer sa propre conception de protection des données personnelles en matière pénale et faire cohabiter sécurité publique et droit fondamental à la protection des données (§2).

§1. Les limites du cadre juridique préexistant

96 L'ancienne division en piliers. Avant l'entrée en vigueur du Traité de Lisbonne, la législation relative à la protection des données dans l'espace de liberté, de sécurité et de justice (ELSJ) était divisée entre le premier pilier (protection des données collectées à des fins privées et commerciales, en utilisant la méthode communautaire) et le troisième pilier (protection des données collectées à des fins répressives, au niveau intergouvernemental). En conséquence, les processus décisionnels applicables à chacun de ces deux domaines suivaient des règles différentes[696]. Cela a entrainé tant une confusion quant à la base juridique applicable (A) quant à l'application des règles car lacunaires (B).

A. Des difficultés découlant de la base juridique

97 L'apport de la jurisprudence de la Cour de justice. Une expression des problèmes découlant de l'ancienne division en piliers pour le régime de protection des données de l'UE est l'affaire *PNR* concernant les dossiers des passagers aériens[697]. L'affaire portait sur l'accord conclu entre les États-Unis et l'UE sur le transfert des données contenues dans les systèmes informatiques de réservation des compagnies aériennes assurant un service à destination ou au départ des États-Unis, désigné « *Passenger Name Records* » (ci-après données PNR). Suite à une décision d'adéquation adoptée par la Commission le 14 mai 2004 conformément à l'article 25 de la directive 95/46, le Conseil a adopté le 17 mai 2004 une décision concernant la conclusion de l'accord avec les États-Unis. Le Parlement européen a entamé une action devant la Cour demandant l'annulation de la décision d'adéquation de la Commission et de la décision du Conseil sur la conclusion de l'accord, en invoquant entre autres une violation des principes essentiels de la directive relative à la protection des données et du droit à la vie privée. La Cour de justice a annulé la décision d'adéquation au seul motif que son contenu ne relevait pas du champ d'application matériel de la directive 95/46 relative à la protection des données. Elle a

696 La structure en piliers a disparu dans le Traité de Lisbonne, qui renforce les bases nécessaires à l'élaboration d'un système de protection des données plus clair et plus efficace, tout en prévoyant de nouveaux pouvoirs pour le Parlement européen, celui-ci devenant colégislateur. L'article 16 du traité FUE dispose que le Parlement européen et le Conseil fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les Fiches techniques sur l'Union européenne institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union.

697 CJCE, Gr. Ch., Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes, affaires jointes C-317/04 et C-318/04, 30 mai 2006.

considéré que le transfert des données PNR constituait un traitement ayant pour objet «la sécurité publique et les activités de l'État relatives à des domaines du droit pénal » et que la décision d'adéquation ne pouvait donc être adoptée en vertu de cette directive. De même, la Cour de justice a annulé la décision du Conseil sur la conclusion de l'accord PNR avec les États-Unis, considérant que l'article 95 CE ne pouvait constituer une base juridique appropriée de la décision car il « vise le même transfert de données que la décision d'adéquation et donc des traitements de données qui sont exclus du champ d'application de la directive », et la Communauté n'avait donc pas la compétence pour conclure l'accord[698]. De plus, dans l'affaire *Irlande c. Parlement* européen et Conseil de l'Union européenne, la Cour de justice a été invitée à nouveau à se prononcer sur le problème de la division en piliers du régime communautaire de la protection des données[699]. Plus précisément, l'Irlande a demandé l'annulation de ladirective 2006/24/CE sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques au motif que l'article 95 CE n'était pas une base juridique appropriée pour cette mesure législative, car son objectif principal est de faciliter la recherche, la détection et la poursuite d'infractions pénales, y compris en matière de terrorisme et qu'elle aurait donc dû être adoptée dans le cadre du troisième pilier. Cependant, la Cour de justice a considéré que la directive a été adoptée sur le fondement d'une base juridique appropriée, étant donné que tant le but que le contenu de cet acte relèvent de l'article 95 CE. La Cour de justice a procédé à une distinction entre l'affaire *Irlande c. Parlement européen et Conseil de l'Union* européenne et *l'affaire PNR* car selon elle, la directive 2006/24 vise les activités des fournisseurs de services dans le marché intérieur et ne comporte aucune réglementation des activités des pouvoirs publics à des fins répressives comme cela était le cas dans l'affaire PNR. Toutefois, la Cour indique expressément que le recours formé par l'Irlande « porte uniquement sur le choix de la base juridique et non pas sur une éventuelle violation des droits fondamentaux découlant des ingérences dans l'exercice du droit au respect de la vie privée que la directive 2006/24 comporte »[700]. Ainsi la Cour s'exprime sur la base juridique mais non sur le fond de l'affaire. L'Union européenne disposait déjà d'une série d'instruments juridiques, pratiques et de soutien pour étayer un espace européen de sécurité intérieure. Les objectifs stratégiques fixés dans la stratégie de sécurité intérieure 2010-2014 restent valables et devraient être maintenus[701]. Le Traité de Lisbonne a donné à l'Union européenne des bases solides pour y parvenir, en renforçant le cadre juridique afin de conjuguer les efforts et de garantir la liberté et la sécurité, la libre circulation à l'intérieur de l'Union et une réaction efficace de celle-ci aux menaces transfrontières. Le traité a également permis de renforcer la protection des droits fondamentaux et le contrô le démocratique sur les politiques de l'Union en matière de sécurité intérieure et a fait du Parlement européen un colégislateur à part entière

698 E. GUILD et E. BROUWER, « The Political Life of Data - The ECJ decision on the PNR Agreement between the EU and the US », *Centre for European Policy Studies*, no 109, 2006.

699 CJCE, Irlande c. Parlement européen et Conseil de l'Union européenne, C-301/06, arr.t de Grande chambre du 10 février 2009.

700 CJCE, Irlande c. Parlement européen et Conseil de l'Union européenne, § 57.

701 Conclusions du Conseil du 25.2.2010 sur la stratégie de sécurité intérieure pour l'Union européenne : Vers un modèle européen de sécurité; COM (2014) 154 final du 11.3.2014.

dans le domaine de la coopération policière et judiciaire en matière pénale. Le contrô le juridictionnel de la Cour de justice de l'Union européenne et le rô le de gardienne des traités joué par la Commission y sont désormais pleinement effectifs. Toutefois, le cadre de profonde incertitude pour la protection des données personnelles, évoque le manque d'effectivité de la règlementation actuelle, en raison du morcellement progressif du cadre juridique et de l'insuffisante harmonisation dans les États membres.

B. Les difficultés découlant des lacunes de la décision-cadre 2008/977 JAI

98 Un manque d'efficacité. Concernant l'étude des dispositions de la décision-cadre, il est possible de constater un grand nombre de lacunes. Tout d'abord, concernant le principe de finalité, l'article 3 § 1 de la décision-cadre précise que les données à caractère personnel peuvent être collectées par les autorités compétentes « uniquement pour des finalités déterminées, explicites et licites et traitées uniquement pour les finalités pour lesquelles elles ont été collectées ». Le traitement des données pour une autre finalité est permis, mais seulement dans la mesure où il n'est pas incompatible avec la finalité pour laquelle les données ont été collectées. Telle disposition aurait dû respecter le principe de proportionnalité et de stricte nécessité comme le suggérait dans son avis le CEPD[702], dans la logique de l'article 8 de la CEDH[703] et 8 de la Charte des droits fondamentaux. Or, ce critère figurait dans le texte de la proposition de la Commission, mais a disparu du texte final de la décision-cadre[704]. D'ailleurs, le CEDP souhaitait une distinction entre données relatives aux faits non confirmées et données relatives à des renseignements[705]. Un autre élément de flou concerne les données sensibles : la décision-cadre ne contient aucune disposition spécifique relative à la protection des données biométriques et des profils ADN, l'article 6 permet le traitement des données sensibles à condition que soit prévu par une loi, alors que dans la proposition de la Commission le traitement devait être prévu par la loi et être nécessaire à l'accomplissement des buts légitimes de l'autorité concernée aux fins de prévention et de détection des infractions pénales, et d'enquêtes et de poursuites en la matière, ou bien la personne concernée devait avoir consenti au traitement. Un élément qui montre le manque d'efficacité de la décision-cadre concerne le transfert vers des États tiers. Le texte prévoit le consentement préalable de l'État auprès duquel les données ont été collectées, cependant si le transfert de données « est essentiel pour prévenir un danger immédiat et sérieux pour la sécurité publique d'un État membre ou d'un État tiers ou pour les intérêts essentiels d'un État membre et que l'accord préalable ne peut pas être obtenu

---

702 V. le § 65 du premier avis du CEPD, du 19 décembre 2005, JOUE C 047 du 25 fév. 2006, p. 27-47.

703 Voy., par exemple, notre commentaire de l'arrêt *Marper c. Royaume-Uni* du 4 décembre 2008, relative à la durée de conservation (indéfinie) de données à caractère sensible (données biométriques et profils ADN) de personnes qui avaient été acquittées ou relaxées de leurs poursuites pénales.

704 COM (2005)475 final, 4 oct. 2005, voy. l'article 11.

705 V. le § 32 du premier avis du CEPD, du 19 décembre 2005, JOUE C 047 du 25 fév. 2006, p. 27-47.

en temps utile »[706] il est possible de déroger au consentement préalable. Il en résulte que dans un contexte de lutte contre le terrorisme une telle dérogation devient en réalité la règle. L'autre condition pour le transfert de données (sur l'exemple de l'art. 25 de la directive 95/46) est le niveau de protection « adéquat » du pays destinataire. Toutefois l'existence d'un niveau de protection adéquat est constituée par une décision de l'autorité de contrôle nationale, comme conséquence il peut y avoir une différence de traitement en fonction de l'origine des données. Une réforme du cadre juridique visant à assurer une meilleure protection des données, a été donc nécessaire. Ainsi à ce cadre juridique, a été rapproché de n'avoir pas su mettre fin au morcellement législatif constaté en ce domaine, à cause du choix de sa base juridique car elle coexiste avec de nombreuses règles spécifiques, adoptées au fur et à mesure de la création de divers mécanismes de coopération comme le Système d'Information Schengen (SIS) pour l'espace Schengen, le VIS en matière de visas, EUROPOL etc. [707]. Ainsi les dispositions de la décision-cadre 2008/977 JAI n'assuraient pas un niveau élevé de protection pour les données personnelles.

§2. Le nouveau cadre juridique

99 La refonte du cadre juridique dans l'ELSJ. Une réforme était nécessaire car le champ d'application de la Décision-cadre 2008/977/JAI était trop limité puisqu'elle s'appliquait uniquement aux traitements transfrontières de données conférant une très grande marge de manœuvre aux États pour transposer ses dispositions[708]. Elle ignorait toute norme commune pour les échanges avec les pays tiers, entretenant un flou quant à une nécessaire distinction entre les différentes catégories de personnes concernées, telles que les suspects, les criminels, les témoins et les victimes, pour assurer une protection effective et adéquate. Le paquet de réforme présenté par la Commission en 2012[709] contenait un projet de directive pour encadrer les traitements dans les domaines répressifs et de prévention de la criminalité, traitements qui étaient exclu du champ d'application du projet de règlement générale. Il lui est aussi reproché de n'avoir pas su mettre fin au morcellement législatif en ce domaine, car elle coexiste avec de nombreuses règles spécifiques, C'est la raison pour laquelle la décision cadre a fait l'objet de nombreuses critiques[710]. Toutefois il faut rappeler qu'il y a eu des avancées avec le Traité de

---

706 V. article 13 § 2 de la décision-cadre.

707 V. la liste complète des instruments dans l'annexe document SEC (2012)72.

708 Le risque c'est d'avoir deux systèmes de protection des données dans une même enquête. Cela menacerait non seulement la protection du citoyen mais compliquerait également le travail policier ou judiciaire. Voy. Par exemple la position très sévère du Controleur Européen de la Protection des données (CEPD) dans son avis du 27 avril 2007. Voy. aussi le commentaire »La protection des données dans l'ELSJ, work in progress" Rev.trim. dr. Eur. Juillet-septembre 2009 n° 3 pp. 775-790.

709 Le projet de réforme se situe dans le prolongement d'une consultation publique lancée en 2009 visant à obtenir des contributions relatives aux nouveaux défis en matière de protection des données personnelles et à l'amélioration du cadre juridique au sein de l'Union européenne. Ce projet repose sur l'article 16 du traité sur le fonctionnement de l'Union européenne, qui est la nouvelle base juridique, introduite par le traité de Lisbonne, pour l'adoption de règles en matière de protection des données.

Lisbonne, tout d'abord à côté la proclamation de la valeur juridique contraignante de la Charte des droits fondamentaux, elle a introduit dans son art. 16 du TFUE le droit d'assurer la protection des données personnelles, en instituant une base juridique pour l'intervention de l'Union dans la matière. De plus, la suppression de la structure en pilier a reconduit la coopération de police sous des procédures décisionnelles typiques de l'ancien premier pilier, en préfigurant aussi la possibilité d'une action plus incisive et, en même temps, de contrôles démocratiques plus stricts. Ainsi sur la base de l'art.16 TFUE[711], les textes de base en matière de protection des données, la directive 95/46/CE pour le marché intérieur et la décision-cadre 2008/977/JAI pour l'ELSJ ont toutes les deux été réformées et remplacées par deux instruments distincts[712]. Toutefois, la directive qui a succédé à la décision-cadre ne semble pas apporter de réponses satisfaisantes aux objections majeures qui avaient été soulevées (A). D'abord elle ne réunit pas les multiples règlementations spécifiques évoquées, [713] laissant des législations morcelées et elle manque de clarté dans sa rédaction[714], ainsi l'hétérogénéité législative semble destinée à perdurer vu la proposition d'un texte distinct du règlement général. En effet, suivant cette vague de réforme, dans le programme de Stockholm « une Europe ouverte et sûre qui sert et protège les citoyens », la Commission a été invitée à présenter une proposition concernant l'utilisation des données PNR aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité, ainsi que des enquêtes et des poursuites en la matière[715]. Ainsi a été adoptée la directive 681/2016[716] relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité (B).

710 Voy. Par exemple la position très sévère du Contrôleur Européen de la Protection des Données dans son avis du 27 avril 2007, J.O.U.E. C 139/1, 23 juin 2007.

711 L'art. 16 du Traité de Lisbonne consacre dans son paragraphe 2 la compétence du législateur communautaire pour l'adoption de règles en matière de protection des données personnelles. Cette compétence du législateur communautaire fondée sur la reconnaissance d'un droit à la protection des données personnelles, consacré comme droit fondamental par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, est ainsi reconnue dans toutes les matières, même pour la coopération judiciaire en matière pénale et la coopération policière.

712 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquê tes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/ JAI du Conseil; et le Règlement (UE) 679/16.

713 Le CEDP souhaité une réglementation nettement plus complète et plus uniforme qui remplacerait également les dispositions spéciales toujours en vigueur des différents régimes du 3ème pilier. Voy. « la proposition visant à créer un marché intérieur de l'UE pour les secteur de communications électroniques : champ de tension entre protection des données, neutralité du réseau et liberté économique », 4ème rencontre de Bonn sur la réglementation, Centre de recherche sur l'intégration européenne, Bonn, 13 janvier 2014.

714 Voy. Par ex. la rédaction du principe de limitation de la finalité, ou les pouvoirs indûment limités des autorités de contrôle, ou les conditions pour les transferts vers des pays tiers.

715 JO C 115 du 4.5.2010, p. 1.

716 Sur le fondement de l'art. 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a) du TFUE.

A. La directive 680/2016 relative à la protection des données à caractère personnel traitées à des fins pénales

100 Une réforme partielle. À la directive relative à la protection des données à caractère personnel traitées à des fins pénales[717] se substitue la décision-cadre 2008/977/JAI. Elle trouve son fondement juridique dans l'article 16§2 du TFUE. Elle vise à faciliter l'échange de données entre les autorités compétentes [718] et définit les règles et principes généraux relatifs à la protection des données à la coopération policière et judiciaire en matière pénale. Le champ d'application de la directive est plus large que celui de la décision-cadre qu'elle abroge, elle s'applique à la fois aux traitements transnationaux et nationaux de données à caractère personnel par les autorités policières et judiciaires, alors que la décision-cadre s'appliquait seulement aux échanges transnationaux. Le traitement des données doit donc contribuer à la réalisation de l'espace de sécurité liberté et justice, alors qu'en principe, en coopération judiciaire pénale internationale, les droits fondamentaux et leur protection apparaissent toujours comme une limite à l'efficacité de la répression.[719] Le directive continue de porter sur les activités de prévention, d'enquête, de détection et de poursuite de crimes déjà couvertes par la décision-cadre [720] et énonce les principes régissant le traitement des données à caractère personnel, elle oblige les États membres à établir une distinction entre les données personnelles de différentes catégories de personnes concernées. La Directive reprend les principes du Règlement 679 à commencer par les définitions d'intéressé, de donnée personnel, traitement, titulaire du traitement etc.… La directive prévoit aussi que, le transfert vers des pays tiers ne peut avoir lieu que s'ils sont nécessaires à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales.

Elle contient, cependant, des dispositions spécifiques sur la responsabilité du responsable et sur ses obligations en matière de transparence et de droit d'accès. Parmi les institutions qui ont participé à la réforme, le G29 a exprimé son avis critique car la directive a un caractère plutôt sémantique que substantiel[721], contrairement à l'abrogation de la directive 95/46 remplacée par le règlement, qui constitue un développement de la matière qui aura un impact sur la vie des citoyens [722] . La doctrine a également critiqué le choix de la Commission d'élaborer deux

---

717 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/ JAI du Conseil.

718 Directive (UE) 2016/680, considérant 93.

719 V.G. TAUPIAC NOUVEL, *De la protection des données personnelles à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en coopération pénale européenne. La fragmentation de l'Espace de liberté sécurité et de Justice*, Journée d'étude européennes du GDR CNRS ELSJ, Lyon III, 14 et 15 juin 2012.

720 Directive (UE) 2016/680, art. 1er, § 1.

721 Voy. Avis n. 1/2013 du 26 février 2013 (doc. web n. 2980389) e les avis n. 1/2012 et 8/2012 (doc. web nn. 2572831 et 2133818).

instruments séparés pour la coopération pénale et pour la protection des données en général. Elle a souligné le risque que les deux instruments de la réforme, subissent une évolution différente d'autant plus qu'à la lumière de l'interaction croissante entre le secteur privé et les autorités de police, le choix d'un instrument autonome dans le champ de la coopération pénale apparaît critiquable. En effet, de nos jours les bases de données privées peuvent être cédées aux agences gouvernantes[723]. D'ailleurs le CEDP a lui aussi critiqué le choix de la Commission, il aurait souhaité un unique règlement pour les deux domaines avec la possibilité d'intégrer les dispositions de caractère générale avec des règles *ad hoc*. Déjà lors de l'élaboration du projet de directive, le CEDP estimait qu'elle ne satisfaisait pas l'exigence d'un haut niveau de protection des données car elle laissait subsister l'ensemble des actes spécifiques existants au niveau européen (décision JAI 2008/615, Europol, Eurojust). Il estimait aussi que les règles de transfert des données entre opérateurs publics entre eux ou entre opérateurs privés n'étaient pas claires ainsi que les règles gouvernant les transferts internationaux[724]. Le Groupe de l'article 29 a partagé certaines critiques en particulier sur le choix de deux instruments législatifs (directive et règlement), il estime ainsi que certaines dispositions sont lacunaires, notamment celles portant sur la durée de la conservation et celles sur la limitation d'accès[725]. L'esprit de la Directive semble chercher un équilibre entre le respect de la vie privée et des données personnelles et la sécurité des citoyens. Elle semble la meilleure réponse possible à ceux qui, dans les derniers mois, sur la base des faits de Paris, de Bruxelles et de Berlin, semblaient convaincus que la vie privée devait céder le pas à la sûreté. Le traitement automatisé de données personnelles sera prohibé s'il menace de compromettre l'identité personnelle d'un citoyen, une attention particulière sera attribuée à la sécurité des systèmes qui recueillent les données et une obligation de dénoncer aux Autorités de contrôle chaque violation des bases des données et, surtout, une plus ample coopération entre les autorités de contrôle nationales.

La directive affirme le droit à la protection des données à caractère personnel et les principes fondamentaux qui devraient couvrir le traitement des données, en suivant de près les règles et principes énoncés dans le règlement général sur la protection des données. Les droits des individus et les obligations imposées aux contrôleurs - par exemple en matière de sécurité des données, de protection des données par conception et par défaut et de notification des violations de données - ressemblent aux droits et obligations du règlement général sur la protection des données. La directive prend également en compte et tente de résoudre les graves problèmes technologiques émergents qui peuvent avoir un impact particulièrement lourd sur les individus, tels que l'utilisation de techniques de profilage par les autorités chargées de l'application de la loi. En principe, les décisions fondées uniquement sur le traitement automatisé, y compris le profilage, doivent être interdites. En outre, elles ne doivent pas être fondées sur des données sensibles. Ces principes sont soumis à certaines exceptions prévues dans la directive. La directive contient également des règles pour assurer la responsabilité des contrôleurs. Ils

722 F. GILBERT, *EU Data Protection Overhaul, New Draft Regulation*, in *The Computer & Internet Lawyer*, March 2012, Vol 29 No 3.

723 P. DE HERT, V. PAPAKONSTANTINOU, « The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals », in *Computer Law & Security Review* 28, 2012, p.130- 142.

724 Voy. L'avis du CEDP du 7 mai 2012, n° 305, sur le paquet de mesures pour une réforme de la protection des données.

725 Voy. l'Avis 01/2012 G29, WP 191, relatif aux propositions de réforme de la protection des données adopté le 23 mars 2012, p. 29 et s.

doivent désigner un responsable de la protection des données chargé de contrôler le respect des règles de protection des données, d'informer et de conseiller l'entité et les employés chargés du traitement de leurs obligations et de coopérer avec l'autorité de surveillance. Le traitement des données à caractère personnel dans le secteur de la police et de la justice pénale est désormais soumis à la surveillance d'autorités de supervision indépendantes. Le régime juridique général de protection des données et le régime spécial de protection des données pour les services répressifs et pénaux doivent tous deux satisfaire aux exigences de la Charte des droits fondamentaux de l'Union.

B. La directive PNR relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité

101 Surveillance et politique anti-terrorisme. Les limitations provisoires des libertés fondamentales peuvent être légitimée par l'existence d'une situation susceptible de troubler l'ordre social et dans les cas plus extrêmes, mettre en danger les institutions publiques[726]. Or, les évènements de nature terroriste en Europe ont entraîné une double réaction. Dans un premier temps, les pouvoirs publics ont mis en place des mesures aptes à répondre promptement au danger en cours et à faire face aux circonstances exceptionnelles du cas d'espèce. Dans un deuxième temps, elles ont élaboré de nouveaux dispositifs juridiques aptes à intervenir sur le plan préventif à long terme[727]. L'idée de la Directive PNR[728] est née dans le but d'harmoniser la politique de lutte contre le terrorisme au niveau de l'Union européenne après les attentats de Paris en janvier 2015. D'ailleurs, l'utilisation des PNR était déjà réglementée dans certains États membres comme le Royaume-Uni, toutefois au niveau européen les instruments existants ne permettaient pas aux autorités répressives d'identifier des suspects « inconnus »[729] de la même manière qu'une analyse des données PNR le ferait[730]. En effet, l'évaluation des données

---

726 F. NATOLI, « Sécurité et ordre public : deux notions à relation variable. Comparaison franco-italienne », *La Revue des droits de l'homme*. Disponible à l'adresse : http://revdh.revues.org/2905 ; DOI : 10.4000/revdh.2905

727 B. ACKERMAN, *The Emergency Constitution*, The Yale Law Journal, 2004. Disponible à l'adresse : http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1120&context=fss_papers

728 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JO L 119 du 4/5/2016, p. 132-149 ; également l'avis rendu par la Cour relatif à l'accord PNR avec le Canada, CJUE, (Grande chambre), 26 juillet 2017, Avis 1/15 rendu en vertu de l'article 218, paragraphe 11, TFUE.

729 Il y a au niveau européen des instruments comme la directive sur les informations préalables sur les passagers (API), le système d'information Schengen (SIS) et le système d'information Schengen de deuxième génération (SIS II) mais ils ne permettent pas aux autorités répressives d'identifier des suspects « inconnus » qui ne sont pas fichés.

730 La directive PNR de l'UE s'applique aux vols internationaux à destination et en provenance de l'UE, mais également aux vols intra-UE si un État membre en décide ainsi les données des dossiers passagers (Passenger Name Record - PNR) contiennent plusieurs types d'informations, telles que les dates de voyage, l'itinéraire de voyage, les informations de contact, l'agence de voyages où le vol a été réservé, les moyens de paiement utilisés, le numéro de siège et les informations sur les bagages. aider les autorités chargées de l'application de la loi à identifier les suspects connus ou potentiels et à effectuer des évaluations en fonction des habitudes de déplacement et d'autres indicateurs généralement associés aux activités criminelles. Une analyse des données PNR permet également un suivi rétrospectif des itinéraires et des contacts des personnes soupçonnées d'avoir participé à des activités criminelles, ce qui peut permettre aux autorités répressives d'identifier les réseaux criminels.

PNR permet d'identifier des personnes qui n'étaient pas soupçonnées de participation à des infractions terroristes ou à des formes graves de criminalité avant cette évaluation et qui devraient être soumises à un examen plus approfondi par les autorités compétentes. Il appartiendra ensuite aux États membres d'alerter d'autres pays, si nécessaire. Ils pourront aussi demander des données PNR à d'autres, de leur propre initiative, dans le cadre d'une enquête. Concernant le champ d'application, la directive s'appliquera aux « vols extra-UE » et contraindra les compagnies aériennes à fournir aux autorités nationales les données des passagers pour tous les vols à partir d'un pays tiers vers l'UE et inversement. Cependant, les États membres pourront étendre cette application aux « vols intra-UE », à condition d'en informer la Commission européenne. Concernant les finalités possibles, dans les annexes de la Directive, les différentes infractions sont listées[731] de façon à limiter le traitement des données PNR pour la prévention et la détection d'infractions terroristes et d'infractions graves, ainsi que la réalisation d'enquêtes et de poursuites en la matière. Afin de gérer les données PNR, des Unités de renseignements sur les passagers devront être créées par les États membres et seront chargées de les conserver pendant une période de cinq ans. Ces dernières seront non masquées durant les six premiers mois. En ce qui concerne les garanties, la directive interdit la collecte et l'analyse de « données sensibles » (origine ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, orientation sexuelle). De plus, les unités nationales de renseignements sur les passagers devront nommer un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties correspondantes ; l'accès à l'ensemble des données PNR devrait uniquement être octroyé dans des conditions très strictes et limitées après la période de conservation initiale ; tout traitement des données PNR devrait être journalisé ou faire l'objet d'une trace documentaire. Il faut souligner aussi que les nouveaux instruments juridiques dans l'ELSJ ne mettent pas en place un organe commun comme le G29, introduit par la directive 95/46/CE et renforcé par le règlement 679/16. Ce qui souligne encore une fois le niveau de garanties insuffisantes dans le cadre juridique relevant de l'ex-troisième pilier. Ce niveau insuffisant peut s'expliquer à travers les spécificités propres à l'ELSJ, permettant l'*opt-out* de certains États membres, le contrôle du principe de subsidiarité et la clause du frein d'urgence prévue à l'art. 83§3[732]. La compétence pénale conserve donc certaines caractéristiques intergouvernementales qui témoignent du profond attachement des États membres à ne pas être totalement dépossédés de leur pouvoir de punir. Le droit pénal reste en effet étroitement lié à la société nationale.

731 La liste inclut par exemple, incluant par exemple la traite d'êtres humains, la participation à une organisation criminelle, la cybercriminalité, la pédopornographie, ainsi que le trafic d'armes, de munitions et d'explosifs.

732 La clause dite du « frein d'urgence » de l'article 83§3 prévoit que lorsqu'un membre du Conseil estime qu'un projet de directive pénale porte « atteinte aux aspects fondamentaux de son système de justice pénale », il peut bloquer la procédure législative Art. 83§3 : « Lorsqu'un membre du Conseil estime qu'un projet de directive visée au paragraphe 1 ou 2 porterait atteinte aux aspects fondamentaux de son système de justice pénale, il peut demander que le Conseil européen soit saisi. Dans ce cas, la procédure législative ordinaire est suspendue. Après discussion, et en cas de consensus, le Conseil européen, dans un délai de quatre mois à compter de cette suspension, renvoie le projet au Conseil, ce qui met fin à la suspension de la procédure législative ordinaire ».

CONCLUSION DU CHAPITRE II

Le chapitre a montré que l'Union européenne est parvenue à élaborer sa propre conception de la protection des données en matière pénale, et se poursuit en confrontant cette conception à son application concrète, tant pour la coopération policière et judiciaire en matière pénale que pour la lutte contre le financement du terrorisme.

Le traitement des données par les autorités de police pouvant avoir un impact significatif sur les personnes concernées, des règles détaillées de protection des données pour le traitement des données à caractère personnel dans ce domaine sont particulièrement nécessaires. Des instruments juridiques spécifiques régissent la protection des données dans le cadre de la coopération transfrontalière entre la police et les services de répression, en particulier dans la lutte contre le terrorisme et la criminalité transfrontalière. Des règles spéciales de protection des données existent pour l'Office européen de police (Europol), l'unité de coopération judiciaire européenne (Eurojust) et le nouveau bureau du Procureur européen, qui sont des organes de l'Union chargés d'aider et de promouvoir les services répressifs transfrontaliers.

Des règles spéciales de protection des données existent également pour les systèmes d'information communs mis en place au niveau de l'Union pour les échanges d'informations transfrontaliers entre les autorités policières et judiciaires compétentes. Des exemples importants sont le système d'information Schengen II (SIS II), le système d'information sur les visas (VIS) et Eurodac, un système centralisé contenant les empreintes digitales des ressortissants de pays tiers et des apatrides demandeurs d'asile.

La division en piliers antérieure au traité de Lisbonne a généré une complexité et une multitude de régimes juridiques applicables. On trouve autant de systèmes de protection des données personnelles que d'instruments de collectes des informations. D'ailleurs, la principale limitation à laquelle se heurte actuellement l'Union résulte de l'ancienne architecture en piliers[733]. La « depillarisation »[734] du système avec le Traité de Lisbonne n'a pas mis un terme à cette fragmentation de la réglementation juridique comme le met bien en exergue le processus de révision des différentes réglementations. La directive n° 95/46 CE adoptée dans le cadre du premier pilier est remplacée par le règlement 679/16, et la décision-cadre 2008/977 dans le troisième pilier est remplacée par la directive 680/16. L'adoption d'instruments spéciaux est donc nécessaire pour parvenir à la clarté et à l'équilibre entre la protection des données et d'autres intérêts légitimes et pour relever des défis particulièrement pertinents dans des secteurs spécifiques. C'est le cas des règles régissant le traitement des données à caractère personnel par les autorités répressives.

L'instrument normatif utilisé, une directive, montre bien la marge de manœuvre plus importante laissée aux États dans ce secteur de la coopération pénale et judiciaire. Les États n'entendent

---

733 Bien que la protection des données soit très poussée dans l'ancien premier pilier de l'UE, le régime de protection des données établi dans l'ancien troisième pilier ne peut être jugé satisfaisant. Et pourtant, l'ancien troisième pilier englobe des domaines comme la coopération policière, la lutte contre le terrorisme et les questions de droit pénal où la protection des données revêt une importance cruciale.

734 O. COSTA, P. MAGNETTE, *Au-delà du traité de Lisbonne, quelles perspectives pour l'intégration pour l'intégration européenne ?*, Disponible à l'adresse : https://hal.archives-ouvertes.fr/halshs-00326443

pas renoncer à la définition des règles dans ces secteurs touchant directement à leur souveraineté.

Lorsqu'une autorité compétente traite des données à caractère personnel à des fins de prévention, d'enquête, de détection ou de poursuite d'infractions pénales, la directive 2016/680 s'appliquera. Lorsque les autorités compétentes traitent des données à caractère personnel à des fins autres que celles mentionnées ci-dessus, le régime général du règlement général sur la protection des données s'appliquera. Contrairement à son prédécesseur (décision-cadre 2008/977 / JAI du Conseil), le champ d'application de la directive 2016/680 s'étend aux traitements nationaux de données à caractère personnel par les autorités répressives et ne se limite pas aux échanges de ces données entre États membres. En outre, la directive cherche à atteindre un équilibre entre les droits des individus et les objectifs légitimes du traitement lié à la sécurité.

L'Union européenne a choisi d'exploiter les potentialités des nouvelles technologies de l'information et de la communication pour développer un modèle de sécurité intérieure fondé sur l'élaboration d'un modèle global pour l'échange d'informations qui privilégie la prévention et l'anticipation. Si le niveau de menace terroriste élevé justifié incontestablement d'adapter et de moderniser les outils de détection des risques, des garanties fortes ont été prévues.

Dans ce contexte, le rôle de la Cour de justice n'a jamais été aussi important. Elle s'érige comme l'ultime recours face à cette fuite en avant sécuritaire et comme gardienne de l'identité et des valeurs démocratiques européennes.

CONCLUSION DU TITRE I

Les résultats de la recherche du présent Titre permettent de constater que, en conformité avec l'expérience historique et avec la tradition juridique de nombreux États membres, l'Union européenne a édifié le droit à la protection des données personnelles comme un droit fondamental. Le Titre I a illustré en particulier que ce droit s'est construit et a évolué à partir d'une *summa divisio* entre marché intérieur et ELSJ due à l'ancienne structure en piliers. Né de l'expérience du Conseil de l'Europe et de la jurisprudence de la Cour européenne des droits de l'homme, le droit à la protection des données personnelles a été mis en œuvre par les dispositions de la Directive 95/46/CE afin de garantir le bon fonctionnement du marché intérieur grâce à la libre circulation des données. Seulement dans un second temps ce droit a fait l'objet d'une protection spécifique, en tant que droit fondamental, avec l'inscription dans l'art. 8 de la Charte des droits fondamentaux, élevée par le Traité de Lisbonne au rang de droit primaire. Le problème de la directive 95/46/ CE est qu'elle ne s'applique pas, par définition, aux activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité UE (l'ancien troisième pilier, l'ELSJ aujourd'hui), ni aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal. D'ailleurs, le traité d'Amsterdam a fait de la réalisation d'un espace de liberté, de sécurité et de justice l'un des objectifs majeurs de l'Union européenne. Cet objectif politique s'est traduit par la mise en œuvre progressive d'une politique européenne de sécurité intérieure et à des dispositifs de contrôle visant à surveiller la mobilité intérieure et à empêcher les déplacements jugés illégitimes ou indésirables. Le développement des technologies et des pratiques de surveillance crée des formes de contrôle social. Le défi est d'assurer que le respect des droits fondamentaux et la sécurité ne soient pas des notions contradictoires, mais des objectifs politiques cohérents et complémentaires[735]. L'approche de l'Union repose sur les valeurs démocratiques, dont le principe de l'État de droit et le respect des droits inscrits dans la Charte des droits fondamentaux. Ainsi toutes mesures de sécurité doivent satisfaire les principes de nécessité, de proportionnalité et de légalité et prévoir les garanties appropriées de recours juridictionnel[736]. Le constat est le passage d'une logique liée au développement du marché intérieur à une logique constitutionnelle. Ainsi la Cour de justice a tracé le socle de cette « révolution » et le législateur est intervenu avec une réforme garantissant la protection d'un droit fondamental de l'individu. L'utilisation croissante des fichiers à des fins de sécurité illustre la politique de l'Union européenne en matière d'immigration et d'asile mais également dans le cadre de la coopération policière. Il faut alors se poser la question de la conciliation entre sécurité et libertés individuelles. Le constat est qu'il reste des lacunes comme le démontre le cadre juridique toujours morcelé qui reprend l'ancienne division en pilier. Le résultat de la réforme dans l'ELSJ semble loin d'être à la hauteur de celui atteint dans le cadre communautaire. La

735 Voy. l'arrêt de la CJUE, aff. jointes C-293/12 et C-594/12, 8 avril 2014, § 42.

736 Voy. Article 52, paragraphe 1, de la Charte des droits fondamentaux.

« depillarisation » du système avec le Traité de Lisbonne n'a pas mis un terme à cette fragmentation de la réglementation juridique comme le met bien en exergue le processus de révision des différentes réglementations. En effet, la refonte de la législation en matière de protection des données personnelles (à travers l'élaboration du règlement 679/16 et de la directive 680/16 maintient la *summa divisio* entre marché intérieur et ELSJ. Le cadre juridique a été complété par la directive 2016/681/UE sur l'utilisation des données PNR pour la prévention, détection, enquête et poursuite d'infractions terroristes et de crimes graves. Cette directive prévoit l'obligation pour les transporteurs aériens de transmettre des données PNR aux autorités compétentes et établit des garanties strictes de protection des données pour le traitement et la collecte de ces données.

Si le niveau de menace terroriste élevé justifie incontestablement d'adapter et de moderniser les outils de détection des risques, des garanties fortes doivent être prévues. Malgré ces contestations, la législation de l'Union européenne apparaît comme l'instrument légitime pour établir les équilibres nécessaires à l'utilisation des données personnelles. De plus, la Cour de justice assure le juste équilibre entre le droit fondamental à la protection des données personnelles et l'accès des autorités nationales (sous certaines conditions aux informations) pour des finalités de prévention, détection, enquête et poursuite d'infractions terroristes et de crimes graves[737].

737 À la suite de l'arrêt Digital Rights Ireland, la CJUE a été saisie de deux autres affaires concernant l'obligation générale imposée en Suède et au Royaume-Uni aux fournisseurs de services de communications électroniques de conserver les données de télécommunication. Dans l'affaire Tele2 Sverige et Home Department c. Tom Watson ea, la CJUE a déclaré que la législation nationale qui prescrit la conservation générale et indiscriminée des données sans exiger aucune relation entre les données à conserver et une menace pour la sécurité publique, sans préciser toutes conditions par exemple : délai de conservation, zone géographique, groupe de personnes susceptibles d'être impliquées dans une infraction grave, dépasse les limites du strict nécessaire et ne peut être considéré comme justifié dans une société démocratique, comme l'exige la directive 2002/58 / CE, lue à la lumière de la Charte des droits fondamentaux del'UE.

TITRE II. LA PROJECTION INTERNATIONALE DU STANDARD EUROPÉEN DE PROTECTION

102 Les données personnelles comme moyen d'exportation de valeur de l'Union. L'ampleur de la collecte et du partage de données à caractère personnel a augmenté de manière exponentielle grâce à l'évolution des technologies. La révolution numérique redessine les frontières entre le marché intérieur et le marché numérique caractérisé par l'absence de frontières. Le pouvoir de marché[738] des données personnelles a été perçu par les autorités et la jurisprudence communautaire à travers une législation encadrant les échanges de données et de nombreuses décisions.

Ainsi les technologies permettent tant aux entreprises privées qu'aux autorités publiques d'utiliser les données à caractère personnel comme jamais auparavant. Le présent Titre est dédié à l'analyse de la « dimension externe » de la protection des données personnelles. Il est proposé d'évaluer les principes, les instruments normatifs et le raisonnement jurisprudentiel à travers lesquels l'Union européenne cherche à assurer un niveau élevé de protection aux données personnelles sortant de son territoire[739]. Ainsi les données personnelles non seulement font l'objet d'une protection spécifique à l'intérieur de ses frontières mais également lorsqu'elles sont transférées vers des États tiers. Il faut alors se pencher sur le mécanisme juridique qui permet d'assurer une protection « adéquate » dans des pays qui n'ont pas la même sensibilité que l'Union européenne vis-à-vis de la protection accordée aux données à caractère personnel. En effet, la protection des données personnelles constitue, pour l'ordre juridique européen, un droit fondamental. Or, cette conception est l'expression d'une expérience historique-juridique et d'une sensibilité culturelle typiquement européenne très différentes des traditions juridiques d'autres démocraties occidentales comme les États-Unis[740]. Ainsi au sein de l'Union[741], la protection des données à caractère personnel est un droit fondamental, proclamé, garanti et sanctionné. L'article 8 de la Charte des droits fondamentaux de l'Union, désormais élevé au rang de droit primaire grâce au Traité de Lisbonne, consacre le droit de toute personne à la protection de ses données à caractère personnel[742]. Ainsi ces différentes approches ont mené à

738 On peut définir le pouvoir de marché comme « l'aptitude d'une entreprise à l'emporter sur ses concurrents, ainsi qu'à contracter, de manière rentable avec ses partenaires » Voy. A. DECOCQ et G. DECOCQ, « Droit de la concurrence, droit interne et droit de l'Union européenne », *LGDJ*, 6e éd. 2014, n° 84, p. 111.

739 Voy. dans ce sens : J. ROCHFELD, E. GATTONE, *Quel avenir pour la protection des données à caractère personnel en Europe ?*, Dalloz, 2018, p.2788

740 Si l'on considère que les États-Unis n'ont pas connu des formes de dictature, il n'y a pas de doutes que l'expérience des régimes nazis et fascistes du XXe siècle a contribué à renforcer l'intensité avec laquelle, en Europe, est ressentie la nécessité d'une protection de la vie privée. De plus, le traitement des données personnelles « sensibles » à des fins politiques (si l'on pense à la race, les croyances religieuses, l'appartenance syndicale, ainsi que l'orientation sexuelle) comme outil pour la mise en œuvre d'une politique répressive et raciste a représenté une pratique générale dans un certain nombre de régimes autoritaires européens.

741 Il convient de citer aussi la protection des données personnelles offerte dans le cadre du Conseil de l'Europe : c'est le juge qui, au fil de sa jurisprudence, a donné consistance au droit à la protection des données à caractère personnel, derivé dans le droit au respect de la vie privée garanti expressément par l'article 8 de la Convention européenne des droits de l'homme. La Convention 108 du 28 janvier 1981 (également en cours de refonte), a été le premier instrument international spécifiquement consacrée à « la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ».

un « conflit transatlantique » sur le plan économique qui s'est aggravé par une différente hiérarchisation des priorités dans le débat entre sécurité et liberté et l'adoption par les États-Unis de législations priorisant la lutte contre le terrorisme. En effet dans ces dernières années, le phénomène du transfert international des données personnelles n'est plus exclusivement lié à des raisons de nature commerciale, mais, de plus en plus, à des exigences de sécurité publique[743]. Or, les enjeux sécuritaires et anti-terroristes sont depuis la jurisprudence *Kadi*[744] un « objectif d'intérêt général de l'Union » tout comme l'est la lutte contre la criminalité grave afin de garantir la sécurité publique[745]. Cela a été confirmé par la Cour de justice dans l'affaire *Digital Rights* où elle a souligné que l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté[746]. Ainsi le transfert des données vers des pays tiers repose sur des intérêts tant de nature économique (Chapitre I) que sur des intérêts politiques de coopération internationale[747] dans la lutte contre la criminalité (Chapitre II).

742 Une protection efficace de ce droit fondamental exige que les données personnelles, qui présentent la particularité de pouvoir circuler avec une extrême facilité et de pouvoir sortir du territoire des États membres, doivent être protégées non seulement lorsqu'elles circulent à l'intérieur du territoire de l'Union, mais aussi lorsqu'elles sont transférées à l'étranger, vers des États tiers.

743 M.R. VAN WASSHOVA, « Data protection conflicts between the United States and the European Union in the war on terror: lessons learned from the existing system of financial information exchange », *in Case Western Journal of International Law*, 2007/2008, Vol. 39 Issue 1/2, p.827-865, 39p. Voy. Également M.BOTTA, M. V. DE AZEVEDO CUNHA, « La Protezione dei dati personali nelle relazioni tra USA e UE, le negoziazioni sul trasferimento dei PNR », in *Diritto dell'Informazione e dell'Informatica*, 2010, 2, p. 315

744 CJCE, Kadi et Al Barakaat International Foundation/Conseil et Commission, C 402/05 P et C 415/05.

745 CJCE, Tsakouridis, C 145/09.

746 CJUE, Digital Rights Ireland et Seitlinger, C-293/12 et 594/12, point 42. Voy. Également les articles 3 §2 TUE et 67 §3 TFUE qui donnent un fondement à la politique sécuritaire de l'Union.

747 Voy. sur ce point M. DONY, « La dimension externe de l'espace de liberté, de sécurité et de justice au lendemain de Lisbonne et de Stockholm : un bilan à mi-parcours », *éditions de l'Université de Bruxelles*, Institut d'Etudes Européennes - I.E.E.

CHAPITRE I. L'EXTRATERRITORIALITÉ DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES DANS LES RELATIONS COMMERCIALES

103 Les flux internationaux de données personnelles. Les échanges internationaux touchant l'ensemble des activités dépassant le cadre régional ou national, concernent de plus en plus les données personnelles. Ainsi elles font désormais l'objet d'un marché de plus en plus important avec le développement d'Internet [748] et sont devenues un « élément clé de l'économie numérique »[749] . Les données personnelles sont considérées par de nombreuses entreprises comme de véritables marchandises, utilisées et échangées, si l'on considère qu'aujourd'hui, toute stratégie d'entreprise place la connaissance du client au cœur de ses activités[750]. La libre circulation des données constitue alors un principe cardinal des échanges commerciaux, mais cela engendre des risques importants pour le respect de la vie privée du fait de la disparité des réglementations de la protection des données dans les pays tiers, voire du fait que nombreux responsables de traitement ou destinataires des données ne sont pas soumis à des règles de protection des données. Le manque d'harmonisation des règles peut conduire à un blocage préjudiciable à l'échange. Sur le plan international, dès les années 1980, la Convention 108[751] et l'élaboration des lignes directrices de l'OCDE (adoptées en 1980) ont voulu éviter ce risque de disparité en établissant des règles visant à encadrer les transferts de données tout en garantissant une protection adéquate. C'est en effet dans l'optique de la libre circulation des marchandises et de la construction du marché intérieur que l'Union européenne est intervenue en la matière[752] à travers le régime des transferts prévu dans la directive 95/46. Cette orientation a été également reprise par l'avocat général A. Tizzano, lequel soulignait que l'objectif primaire de la directive 95/46 était la libre circulation des données personnelles pour la réalisation du marché intérieur[753]. Cette interprétation n'a pas été suivie par la Cour de justice, elle a consacré

---

748 A. BELLEIL, *E-privacy. Le marché des données personnelles : protection de la vie privée à l'âge d'Internet*, Dunod, coll. Stratégies et management, 2001, p. 202.

749 F. ROCHELANDET, « Economie des données personnelles et de la vie privée », *La découverte*, coll. Repères, 2010, p. 125.

750 G. DESGENS-PASANAU « Informatique et Libertés : une équation à plusieurs inconnues », in J.-L. GIROT (dir.), *Le Harcèlement numérique*, Dalloz, coll. Présage, 2005, p. 75 et s. ; J. FRAYSSINET, *La traçabilité des personnes sur Internet » Droit & Patrimoine, Le mensuel, nº931* mai 2001*;* M. DUPUIS, *La vie privée à l'épreuve de l'Internet : quelques aspects nouveaux*, *RJPF*, 2001, n° 12, p. 6 et s.

751 La Convention STE n° 108 évoque dans le préambule « la nécessité de concilier les valeurs fondamentales du respect de la vie privée et la libre circulation de l'information entre les peuples ».

752 Dans sa rédaction initiale de 1990, la directive 95/46, avait pour objet « la protection des personnes à l'égard du traitement des données à caractère personnel », COM (90) 314 final SYN 287 et 288, 18 septembre 1990 mais la rédaction de 1992 complète ce titre par une référence à « la libre circulation de ces données » car ce texte a pour but d'assurer le fonctionnement du marché intérieur » COM (92) 422 final SYN 287, 15 octobre 1992. La base légale de l'intervention de l'Union européenne est ainsi l'ex. article 100 A, paragraphe 1er du Traité de Rome relatif à la réalisation du marché intérieur. D'ailleurs la Commission a elle-même reconnu que, d'un point de vue juridique, elle repose seulement sur l'objectif économique de réalisation du marché intérieur COM (2003) 265 final, 15 mai 2003, Premier rapport sur la mise en œuvre de la directive relative à la protection des données (95/46/CE).

la double finalité de la directive qui entend assurer la libre circulation des données personnelles[754], tout en garantissant un haut niveau de protection des droits fondamentaux[755]. Ainsi tant la Cour de justice que le législateur, conscients des défis des flux transfrontières de données personnelles, sont intervenus pour garantir le standard de protection européen aux échanges internationaux de données. La circulation des données n'est donc pas prohibée mais elle est encadrée et entourée des garanties.

Les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union et d'organisations internationales sont nécessaires au développement du commerce international et de la coopération internationale. L'augmentation de ces flux a créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données à caractère personnel. Le présent chapitre est dédié à l'analyse de la « dimension externe » de la protection des données personnelles. Il faut alors se pencher sur le mécanisme juridique qui permet d'assurer une protection « adéquate » aux données à caractère personnel transférées vers des pays qui n'ont pas la même sensibilité de l'Union européenne vis-à-vis de la protection accordée aux données à caractère personnel. En effet, la protection des données personnelles constitue, pour l'ordre juridique européen, un droit fondamental proclamé, garanti et sanctionné. Or cette conception est l'expression d'une expérience historique-juridique et d'une sensibilité culturelle typiquement européenne très différentes des traditions juridiques d'autres démocraties occidentales comme les États-Unis[756]. En ce qui concerne la zone Asie-Pacifique (APEC) c'est seulement en 2004 que des lignes directrices en matière de protection des données afin de faciliter le commerce transfrontalier ont été adoptés. Toutefois elles n'ont aucun caractère contraignent. Toutefois, en 2011 le Forum de coopération économique de l'APEC a finalisé un encadrement du transfert de données personnelles au sein de ses pays membres. Ces règles ne sont pas autant protectrices que les règles européennes mais se rapprochent des règles internes d'entreprise (BCR) européennes. À l'égard de l'espace africain francophone les chefs d'État réunis au sein de l'Organisation internationale de la francophonie en 2004 à Bucarest ont pris l'engagement de développer les règles communes sur le droit à la protection des données personnelles. Au sein de l'Union européenne[757] l'article 8 de la Charte des droits fondamentaux de l'Union, désormais élevé au rang de droit primaire grâce au Traité de Lisbonne, consacre le droit de toute personne à la protection de ses données à caractère personnel. Il existe par ailleurs

753 Voy. les Conclusion de l'Avocat général A. TIZZANO dans l'affaire Rechnungshof c. Österreichischer Rundfunk et autres, C-465/00, C-138/01 et C-139/01, 14 novembre 2002, § 53.

754 La libre circulation des données dans l'EEE résulte de la transposition de la directive 95/46 par les États membres qui a donné aux législations nationales une « protection équivalente ».

755 CJCE, 6 novembre 2003, Bodil Lindqvist, aff. C-101/01, Rec. I-12971, § 96.

756 Si l'on considère que les États-Unis n'ont pas connu des formes de dictature, il n'y a pas de doutes que l'expérience des régimes nazis fascistes du XXème siècle a contribué à renforcer l'intensité avec laquelle, en Europe, est ressenti la nécessité d'une protection de la vie privée. De plus, le traitement des données personnelles « sensibles » à des fins politiques (si l'on pense à la race, les croyances religieuses, l'appartenance syndicale, ainsi que l'orientation sexuelle) comme outil pour la mise en œuvre d'une politique répressive et raciste a représenté une pratique générale dans un certain nombre de régimes autoritaires européens.

757 Il convient de citer aussi la protection des données personnelles offerte dans le cadre du Conseil de l'Europe : c'est le juge qui, au fil de sa jurisprudence, a donné consistance au droit à la protection des données à caractère personnel, dérivé du droit au respect de la vie privée garanti expressément par l'article 8 de la Convention européenne des droits de l'homme. La Convention 108 du 28 janvier 1981 (également en cours de refonte), a été le premier instrument international spécifiquement consacrée à « la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ».

une législation substantielle en matière de protection des données, dont la directive 95/46/CE désormais remplacée par le nouveau règlement général 2016/679 a constitué le cœur. Une protection efficace de ce droit fondamental exige que les données personnelles, qui présentent la particularité de pouvoir circuler avec extrême facilité et de pouvoir sortir du territoire des États membres, doivent être protégées à l'intérieur du territoire de l'Union, mais aussi lorsqu'elles sont transférées à l'étranger, vers des États tiers. Le travail se propose, donc, de mettre en évidence les résultats obtenus grâce à une véritable politique législative étrangère de l'Union européenne[758], permettant à l'Union européenne de servir de modèle pour les pays tiers. Selon la doctrine, cette politique extérieure en matière de données personnelles est duale[759]. D'une part, elle s'explique par le caractère globalisé du marché numérique, rendant inutiles les initiatives de protection unilatérales des États, d'autre part il y a l'exigence d'un cadre juridique global en matière de circulation de données pour éviter une insécurité juridique et des difformités qui peuvent conduire à un blocage préjudiciable à l'échange économique. Cette politique étrangère visant à assurer un niveau élevé de protection aux données sortant des frontières de l'Union européenne est renforcée dans le passage de la Directive 95/46/CE au Règlement 2016/679. En effet, l'art. 4 de la Directive 95/46 prévoyait déjà qu'elle s'applique aux traitement effectués dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre mais également lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté[760]. Avec la refonte du cadre général, le Règlement 2016/ 679 étend le champ d'application territoriale. Ainsi la discipline communautaire s'applique à tout responsable du traitement et à tout sous-traitant proposant des biens ou des services aux personnes concernées situées dans l'Union européenne[761] et à tout traitement relatif au suivi du comportement d'une personne concernée dans l'UE[762]. Le responsable du traitement ou le sous-traitant (par exemple un fournisseur de nuages informatiques) peut donc être soumis au règlement sans pour autant être établi dans l'Union européenne[763] . Afin d'assurer une protection effective, d'abord la Directive 95/46/CE et ensuite le Règlement 2016/ 679, ont prévu des dispositions relatives au

---

758 Voy. la Thèse de L. FAVERO, *La dimension externe de la protection des données à caractère personnel dans le droit de l'Union eur*opéenne, Soutenue le 27-05-2013 à Strasbourg en cotutelle avec l'Università degli studi (Bologne, Italie), dans le cadre de École doctorale Droit, science politique et histoire (Strasbourg), en partenariat avec Centre d'études internationales et européennes (Strasbourg) (équipe de recherche Sous la direction de Fabienne Kauff-Gazin et de Lucia Serena Rossi).

759 P. PALLARO, « Rapporti Commerciali tra UE e Stati Terzi e la questione della tutela dei dati personali. Il difficile confronto UE-USA », in *Diritto del Commercio internazionale* 2000,03, p.753.

760 Voy. Art. 4. De la Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050.

761 Voy. Règl. (UE) 2016/ 679, art. 3, § 1.

762 Voy. Règl. (UE) 2016/679, art. 3, § 2. La notion de suivi du comportement implique « d'établir si les personnes physiques sont suivies sur Internet, ce qui comprend l'utilisation ultérieure éventuelle de techniques de traitement des données à caractère personnel qui consistent en un profilage d'une personne physique, afin notamment de prendre des décisions la concernant ou d'analyser ou de prédire ses préférences, ses comportements et ses dispositions d'esprit » (Règl. (UE) 2016/679, consid. 24).
763 Dans ce cas de figure, le responsable du traitement et le sous-traitant seront généralement tenus de donner un mandat écrit à un représentant européen.

transfert des données vers des pays tiers, contenant des règles tant substantielles que procédurales destinées à élever les standards internationaux de protection des données personnelles et empêcher leur utilisation illégale[764]. D'ailleurs, ces dispositions ont connu une importante contribution interprétative de la part du « Groupe pour la tutelle des personnes à l'égard du traitement des données personnelles », G29[765], et de la Cour de justice de l'Union européenne. L'esprit de la législation de l'Union européenne en matière de transfert des données est d'interdire le transfert des données lorsque l'État destinataire ne garantit pas un niveau « adéquat » de protection. Toutefois, ce niveau de protection « adéquat », s'est parfois transformé en exigence « d'équivalence », au point de faire parler « d'embargo » de données[766]. Dans cette optique la politique de l'Union européenne a obtenu des résultats surprenants, de nombreux pays (entre autres le Canada, la Suisse, le Japon et l'Australie) ont spontanément rapproché leurs propres législations nationales en matière de protection de données personnelles afin de s'aligner au *standard* de protection établi par la Directive 95/46/CE[767]. Cependant, d'autres pays comme les États-Unis, ont des approches et des conceptions différentes[768].

Ils existent des instruments juridiques permettant le transfert des données vers des pays tiers (section I) grâce auxquels l'Union européenne met en œuvre une politique étragère face aux intérêts économiques (section II).

Section I. Les instruments juridiques permettant le transfert des données personnelles vers des États tiers

764 Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données Journal officiel n° L 281 du 23/11/1995 p. 0031 – 0050. Voy. Art. 4. Voy. également considérant 56 de la directive 95/46 considérant que des flux transfrontaliers de données à caractère personnel sont nécessaires au développement du commerce international; que la protection des personnes garantie dans la Communauté par la présente directive ne s'oppose pas aux transferts de données à caractère personnel vers des pays tiers assurant un niveau de protection adéquat; que le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts; Considérant 57 : considérant, en revanche, que, lorsqu'un pays tiers n'offre pas un niveau de protection adéquat, le transfert de données à caractère personnel vers ce pays doit être interdit.

765 La nécessité d'une interprétation stricte des exceptions prévue à l'art. 26.1 de la directive 95/46 a été posée par le G29 dès 1998 dans son avis « Transferts de données vers les pays tiers : application des articles 24 et 25 de la directive relative à la protection des données ».

766 R. LOWTHER, « U.S. Privacy Regulations Dictated by EU Law: How the Healthcare Profession May be Regulated », in *Columbia Journal of Transnational Law*, 2003, 41 no2 435-54.

767 L. ZAGATO, « Il trasferimento di dati personali verso stati terzi: esiti (in parte sorprendenti) dell'unilateralismo giuridico CE », in *Dir. Comm. Internaz*. 2008, p.297.

768 Le régime de protection de la vie privée aux États-Unis ne repose pas, en fait, sur une loi générale, mais essentiellement sur la jurisprudence, sur les lois fédérales spécifiques, ainsi que sur l'autorégulation par les sociétés (self régulation). Voy. Sur ce point M. COPE HUIE; F. STEPHEN, D. HOGAN, « The right to privacy in personal data: the EU prods the US and controversy continues », in *Tulsa Journal of Comparative and International Law*, Spring 2002, Vol. 9 Issue 2, p391-469, 79p.

104 La définition de transfert. À l'ère de la globalisation des échanges, le traitement de données ne connait plus de frontières[769], cela comporte des risques importants pour le respect de la vie privée du fait de la disparité des réglementations entre les pays[770]. Il est donc nécessaire de disposer de règles permettant d'ancrer la protection des données personnelles au standard de protection le plus efficace. L'article 2, du Protocole additionnel à la Convention 108 pour la protection des personnes à l'égard du traitement des données, adopté en 2001, définit le flux international de données comme le « transfert de données vers un destinataire soumis à la juridiction d'un État ou d'une organisation qui n'est pas partie à la Convention 108 ». Cependant, le transfert hors Union européenne n'a pas été précisé ni dans la directive 95/46 ni dans le règlement 679/16. Dans le contexte d'Internet il n'est pas évident de déterminer s'il y a un transfert. La Cour de justice dans l'affaire *Bodil Lindqvist*[771] a considéré que le fait de poster un contenu sur un site Internet accessible depuis le monde entier ne constituait pas un transfert visé par l'article 25 de la directive 95/46. Elle relève l'absence d'automaticité dans l'envoi de l'information du serveur du site vers les utilisateurs du site. Ainsi la Cour en déduit qu'il n'y a pas de transfert car les utilisateurs doivent se connecter volontairement pour accéder au site et aux données personnelles contenues[772] et il n'y a pas de mise en relation directe entre l'émetteur et le destinataire de la donnée [773]. Par ailleurs, la Cour de justice a plus tard affirmé que « l'opération consistant à faire transférer des données à caractère personnel depuis un État membre vers un pays tiers constitue, en tant que tel, un traitement de données à caractère personnel au sens de l'article 2, sous b), de la directive 95/46 [...] effectué sur le territoire d'un État membre »[774]. Internet et la numérisation des biens et services ont transformé l'économie mondiale en facilitant la circulation des données dans le monde. Les échanges commerciaux reposent de plus en plus sur les flux de données personnelles et la confidentialité, la sécurité de ces données est devenue un facteur central de la confiance des consommateurs, mais également des entreprises désireuses d'un cadre à la fois sûr et compétitif. Ainsi les responsables de traitement et les sous-traitants peuvent transférer des données hors de l'Union européenne (UE) et de l'Espace Economique Européen (EEE) à condition d'assurer un niveau de protection des données adéquat. Ils doivent encadrer ces transferts en utilisant les différents outils juridiques.

769 Conseil de l'Europe, rapport de J.PH. WALTERAL, « Défis posés par les flux transfrontières de données à caractère personnel », 30 mai 2006.

770 Voy.. M. DINANT, *Les traitements invisibles sur Internet*, Disponible à l'adresse:http://www.droit.fundp.ac.be/crid/eclip/luxembourg.html. « Aujourd'hui, le simple fait d'allumer un ordinateur branché sur Internet met en route plusieurs processeurs qui exécutent subrepticement des centaines de programmes sans que l'utilisateur moyen en soit informé ni puisse avoir le moindre contrôle sérieux sur les données qui y sont traitées. » La crainte c'est que les opérateurs déplacent leurs activités dans des « paradis de données », c'est-à-dire dans des pays ayant une législation sur la protection des données moins stricte.

771 CJCE, Bodil Lindqvist, C-101/01, 6 novembre 2003.

772 Toutefois la solution dans l'affaire Bodil Lindqvist ne semble pas pouvoir s'appliquer aux cas où la finalité du site Internet serait de rendre accessibles des données et donc ne saurait être interprétée largement en dehors du cas d'espèce.

773 « Il n'existe pas de «transfert vers un pays tiers de données» au sens de l'article 25 de la directive 95/46 lorsqu'une personne qui se trouve dans un État membre inscrit sur une page Internet, stockée auprès de son fournisseur de services d'hébergement qui est établi dans ce même État ou un autre État membre, des données à caractère personnel, les rendant ainsi accessibles à toute personne qui se connecte à Internet, y compris des personnes se trouvant dans des pays tiers. » CJCE 6 novembre 2003 « Lindqvist » Aff. C-101/01, § 71.

774 CJUE, Schrems contre DPC, aff. C-362/14, 6 octobre 2015, § 45.

105 Les instruments juridiques encadrant le transfert. L'instrument juridique qui encadrait l'échange des données avec les États tiers, a longtemps été la directive 95/46 et son article 25 portant sur les principes applicables et l'article 26 posant les dérogations existantes permettant l'encadrement de ces transferts. Le RGPD [775]a repris ce schéma. Ainsi la Commission peut décider, avec effet dans l'ensemble de l'Union, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données (§1). En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant doivent prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties consistent dans la mise en œuvre d'instruments de droit privé et peuvent consister à recourir à des règles d'entreprise contraignantes, des clauses types de protection des données adoptées par la Commission, des clauses types de protection des données adoptées par une autorité de contrôle ou des clauses contractuelles autorisées par une autorité de contrôle (§2).

§1. La décision d'adéquation de la Commission européenne. Condition pour le transfert des données personnelles vers des États tiers

106 Une compétence exclusive de la Commission européenne. L'art. 45 du règlement 679/16 prévoit que le transfert vers des pays en dehors de l'Union européenne peut intervenir dans le respect d'exigences du niveau de protection « adéquat » du pays de destination. C'est la Commission européenne qui a la compétence d'établir si un pays respecte le principe de protection adéquat (A). De plus, c'est toujours la Commission européenne qui peut négocier un accord spécifique dans le cadre de règles sectorielles pour le transfert des données vers un État tiers (B). Cela illustre la mise en œuvre de la politique externe de l'Union européenne en matière de protection des données personnelles.

A. La décision « d'adéquation » de la Commission européenne

107 Une décision permettant d'échanger des données sans considération de frontières.

775 Afin d'assurer un haut niveau de protection des données transférées du territoire européen à des États tiers, les organismes souhaitant transférer des données peuvent recourir aux outils suivants : La décision d'adéquation (art. 45 du RGPD), qui constitue le premier outil juridique d'encadrement, dans la mesure où elle est prise sur la base d'un examen global de la législation en vigueur dans un État, sur un territoire ou applicable à un ou plusieurs secteurs déterminés au sein de cet État ; En l'absence d'une telle décision, des « garanties appropriées » (art. 46 du RGPD), constituées pour la majorité de décisions des autorités de contrôle et qui sont prises à la lumière des engagements des organismes concernés ; En l'absence de telles garanties appropriées, le transfert peut enfin être réalisé par dérogation à ces outils globaux d'encadrement, dans des situations particulières et des conditions spécifiques.

Le principe de protection « adéquat » était déjà présent dans l'ordre international[776] et a été repris au niveau de l'Union européenne et est aujourd'hui au cœur du système de transfert des données instauré par la Directive 95/46, comme dans le Règlement 679/2016[777]. L'article 25, paragraphe 1 de la Directive fixait comme principe que les É tats membres autorisent un transfert des données si le pays tiers assure un niveau de protection « adéquat ». Le paragraphe 2 précisait que le « caractère adéquat » doit s'apprécier au cas par cas, « au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ». En particulier, l'art. 25, § 4, de la directive 95/46 prévoyait que, « lorsque la Commission constate, conformément à la procédure prévue à l'article 31 § 2, qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du § 2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause ». Toutefois, en l'absence de protection adéquate au sens de l'article 25, paragraphe 2, la directive envisageait également à l'article 26, paragraphe2, la possibilité de mesures *ad hoc*, notamment à caractère contractuel, susceptibles d'offrir des garanties suffisantes pour que le transfert en question puisse s'effectuer. La directive ne détaillait pas la notion de niveau « adéquat », cependant le §2 de l'art. 25 précisait : « le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées »[778]. Ainsi avant tout transfert, l'objet de l'évaluation n'est pas seulement la législation de l'État tiers mais aussi les règles professionnelles et les mesures de sécurité qui y sont respectées. Selon la directive, devront faire objet d'évaluation les sources de rang législatif, mais également des sources de rang sublégislatif de caractère réglementaire et de même codes de conduite adoptés au sein d'une entreprise (règle de *self-regulation*). D'ailleurs le fait pour un État tiers d'adhérer à la Convention 108 est l'un des critères pris en compte pour établir le niveau de protection adéquat[779]. Le but de l'analyse sur l'adéquation est de tenir compte des différentes approches

776 Le Conseil de l'Europe et l'OCDE ont joué un rôle phare dans l'élaboration d'une réglementation internationale et dans l'harmonisation des législations nationales. Avec l'adoption de la directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, l'Union européenne a contribué à renforcer l'harmonisation des législations nationales des États membres et à créer un espace permettant d'échanger des données sans considération de frontières.

777 Le principe d'adéquation est maintenu dans le Règlement. Toutefois le règlement prévoit que le comité EDPest saisi par la Commission pour avis sur l'évaluation du niveau de protection adéquat assuré par un État tiers ou organisation internationales. Toutefois des nouvelles précisions ont été apporté afin de prendre mieux en compte le niveau de protection: ainsi il faut évaluer les pouvoirs de sanctions, l'effectivité des droits des personnes y compris le droit à réparation.

778 Sur la notion d'adéquation, voy. aussi Document de travail WP 12 sur les transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données, adopté par le Groupe de travail de l'article 29, le 24 juillet 1998, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp12fr.pdf.

779 La Convention 108 prescrit que ses principes doivent être inscrits dans le droit national et que des sanctions et des recours appropriés doivent être prévus en cas de violation de ces principes. Cela devrait suffire à garantir un niveau satisfaisant de respect des règles et des voies de recours appropriées aux personnes concernées en cas d'inobservation de ces règles d'un système visant à faire respecter les règles applicables à la protection des données. La Convention n'oblige pas cependant les parties contractantes à instaurer des dispositifs institutionnels permettant l'instruction des plaintes par une instance indépendante, bien que, dans la pratique, les pays qui l'ont ratifiée l'aient en général fait.

des États tiers en la matière sans créer de discriminations arbitraires ou injustifiées, ni constituer une entrave au commerce[780]. En général il y a aura un niveau de protection « adéquat » si d'une part, la personne concernée jouit des droits comme le droit à un recours et, d'autre part, si ceux qui traitent les données ont des obligations à respecter[781]. Cette notion d'exigence de « niveau de protection adéquat » n'est en effet pas définie de façon claire par la directive 95/46/CE. Elle n'implique pas un niveau de protection identique[782], mais « substantiellement équivalent »[783]. Le Règlement 679/16 encadre mieux la notion de protection « adéquate »[784]. La Commission européenne évalue le caractère adéquat de la protection offerte par le pays destinataire, sur la base des prescriptions relatives à la protection des données à caractère personnel qui figurent dans le document établi par le G29 et le Comité de l'article 31[785]. La décision de la Commission européenne constatant qu'un pays tiers assure un niveau de protection adéquat a pour effet de permettre le transfert, sans garanties supplémentaires, de données à caractère personnel depuis les 27 États membres de l'Union européenne et les trois États membres de l'EEE vers le pays

780 C. CHASSIGNEAU, « Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quis des *Safe Harbor* Principles), vie privée et interconnexions : vers un changement de paradigme ? », Conférence organisée par Programme international de coopération scientifique (CRDP/CECOJI), Ivry sur Seine, 5 juin 2003, p. 5.

781 L'article 44 du règlement 679/16 prévoit à son §2 : Lorsqu'elle évalue le caractère adéquat du niveau de protection, la Commission tient compte, en particulier, des éléments suivants: a) l'État de droit, le respect des droits de l'homme et des libertés fondamentales, la législation pertinente, tant générale que sectorielle, y compris en ce qui concerne la sécurité publique, la défense, la sécurité nationale et le droit pénal ainsi que l'accès des autorités publiques aux données à caractère personnel, de même que la mise en œuvre de ladite législation, les règles en matière de protection des données, les règles professionnelles et les mesures de sécurité, y compris les règles relatives au transfert ultérieur de données à caractère personnel vers un autre pays tiers ou à une autre organisation internationale qui sont respectées dans le pays tiers ou par l'organisation internationale en question, la jurisprudence, ainsi que les droits effectifs et opposables dont bénéficient les personnes concernées et les recours administratifs et judiciaires que peuvent effectivement introduire les personnes concernées dont les données à caractère personnel sont transférées; b) l'existence et le fonctionnement effectif d'une ou de plusieurs autorités de contrôle indépendantes dans le pays tiers, ou auxquelles une organisation internationale est soumise, chargées d'assurer le respect des règles en matière de protection des données et de les faire appliquer, y compris par des pouvoirs appropriés d'application desdites règles, d'assister et de conseiller les personnes concernées dans l'exercice de leurs droits et de coopérer avec les autorités de contrôle des États membres; et les engagements internationaux pris par le pays tiers ou l'organisation internationale en question, ou d'autres obligations découlant de conventions ou d'instruments juridiquement contraignants ainsi que de sa participation à des systèmes multilatéraux ou régionaux, en particulier en ce qui concerne la protection des données à caractère personnel.

782 CJUE, Schrems contre DPC, Aff. C-362/14, 6 octobre 2015, § 73.

783 CJUE, Schrems contre DPC, préec. Aff. C-362/14, §. 73.

784 Voy. considérant 104 du règlement 679/16 : La Commission, dans son évaluation d'un pays tiers, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l' État de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, ainsi que sa législation générale et sectorielle, y compris la législation sur la sécurité publique, la défense et la sécurité nationale ainsi que l'ordre public et le droit pénal. Lors de l'adoption, à l'égard d'un territoire ou d'un secteur déterminé dans un pays tiers, d'une décision d'adéquation, il y a lieu de tenir compte de critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier quand les données à caractère personnel sont traitées dans un ou plusieurs secteurs spécifiques. Plus particulièrement, le pays tiers devrait assurer un contrôle indépendant effectif de la protection des données et prévoir des mécanismes de coopération avec les autorités de protection des données des États membres, et les personnes concernées devraient se voy. octroyer des droits effectifs et opposables ainsi que des possibilités effectives de recours administratif et juridictionnel.

785 Voy. Avis G29 du 24 juillet 1998, L'analyse sérieuse du niveau de protection adéquat doit s'intéresser aux deux éléments fondamentaux suivants: le contenu des règles applicables et les moyens d'assurer leur application efficace. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/1998/wp12_fr.pdf

tiers concerné[786]. La Commission européenne fournit une liste de ces pays ainsi qu'un « contrat type » pour encadrer le transfert de données à caractère personnel vers des pays tiers n'assurant pas une protection adéquate. Ainsi, la Commission a établi plusieurs décisions d'adéquation[787] concernant la législation de l'Andorre, Argentine, Canada, Suisse, États-Unis[788] , Uruguay, Nouvelle Zélande, Israël[789]. l'Union et le Japon ont conclu, le 17 juillet, les négociations sur l'adéquation, venant compléter l'accord de partenariat économique. Les parties ont convenu de reconnaître comme «équivalents» leurs systèmes respectifs de protection des données, ce qui permettra aux données de circuler en toute sécurité entre l'UE et le Japon et donnera lieu à la création du plus grand espace au monde de flux de données en toute sécurité[790].

---

786 D'ailleurs cet article liste un nombre limité de cas dans lesquels une dérogation à l'exigence de protection adéquate pour les transferts vers des pays tiers peut s'appliquer. La première de ces dérogations couvre les cas où la personne concernée donne indubitablement son consentement au transfert envisagé. Il importe de garder à l'esprit de ce consentement, selon la définition qu'en donne l'article 2, point h), de la directive, il doit être libre, spécifique et informé. La deuxième et la troisième dérogations couvrent les transferts qui sont nécessaires soit à l'exécution d'un contrat entre la personne concernée et le responsable du traitement (ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée), soit à la conclusion ou à l'exécution d'un contrat conclu ou à conclure, dans l'intérêt de la personne concernée, entre le responsable du traitement et un tiers. La quatrième dérogation concerne les transferts nécessaires ou rendus juridiquement obligatoires pour la sauvegarde d'un intérêt public important. Cela peut couvrir certains transferts limités entre administrations publiques. La cinquième dérogation couvre les transferts nécessaires à la sauvegarde de l'intérêt vital de la personne concernée. Un exemple évident de ce type de transferts serait le transfert urgent d'un dossier médical vers un pays tiers dans lequel un touriste, soigné précédemment dans l'Union européenne, est victime d'un accident ou tombe gravement malade. La sixième et dernière dérogation concerne les transferts intervenant au départ de registres publics ouverts, en vertu de dispositions législatives, à la consultation du public, dans la mesure où les conditions requises pour cette consultation sont remplies dans le cas particulier. Ainsi lorsqu'un registre public dans un État membre peut être consulté par le public ou par des personnes pouvant justifier d'un intérê t légitime, une personne ayant le droit de le consulter puisse se voy. transmettre les informations demandées, mê me si elle se trouve en réalité dans un pays tiers et que la consultation implique en fait un transfert de données.

787 Les décisions relatives à la pertinence de la protection sont adoptées selon la « procédure de comité », qui comprend les étapes suivantes: la Commission présente une proposition; le groupe de travail « Article 29 » rend un avis; le comité de l'article 31 rend un avis adopté à la majorité qualifiée des États membres; le Parlement européen et le Conseil peuvent, à tout moment, demander à la Commission de maintenir, modifier ou retirer la décision d'adéquation au motif qu'elle excède les compétences d'exécution prévues par la Directive; et le collège des membres de la Commission adopte la décision.

788 Concernant la décision du 26 juillet 2000 (2000/520/CE), la Commission avait estimé que, dans le cadre du régime dit de la « sphère de sécurité (« *Safe Harbor* »), les États-Unis assurent un niveau adéquat de protection aux données personnelles transférées. Cependant suite à un renvoi préjudiciel, la Cour de justice a invalidé l'accord avec les États Unis. La Cour de justice a décidé dans l'affaire *Schrems* que tant qu'une décision de la Commission fondée sur l'article 25 paragraphe 6 est en vigueur, elle s'impose aux États membres, donc également aux autorités nationales de protection des données. Cependant, il est nécessaire qu'une telle autorité de contrôle puisse tout de même mener une enquête en cas de doute sur la mise en œuvre effective de cette décision, ou sur le niveau réel de protection des données dans le pays tiers visé. Et cette autorité doit disposer des moyens de recours suffisants si elle constate un manquement. Voy. CJUE 6 octobre 2015 « Schrems contre DPC » Aff. C-362/14, § 57.

789 La liste intégrale des décisions d'adéquation est consultable à l'adresse : http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_ex.htm. De plus la décision de la commission de 2001/497/CE modifié par la décision 2004/ 915 en 2004 instaurant des clauses contractuelles types relatives au transfert de données a été annulée par la Cour de justice en laissant beaucoup d'incertitudes.

790 Le 25 e sommet UE-Japon s'est tenu le 17 juillet à Tokyo. À l'issue du sommet, les dirigeants ont signé deux accords historiques, l'accord de partenariat stratégique et l'accord de partenariat économique, qui renforceront sensiblement les relations bilatérales. Věra Jourová, commissaire chargée de la justice, des consommateurs et de l'égalité des genres, a déclaré: «*Le Japon et l'UE sont déjà des partenaires stratégiques. Les données sont le carburant de l'économie mondiale et le présent accord permettra aux données de circuler en toute sécurité entre nous, au profit de nos citoyens comme de nos économies. Dans le même temps, nous réaffirmons notre attachement à des valeurs communes concernant la protection des données à caractère personnel. C'est la raison pour laquelle je suis entièrement convaincue qu'en travaillant ensemble, nous pouvons définir les normes mondiales en matière de protection des données et faire preuve de leadership commun dans ce domaine important .*». Voy. Communiquè de presse disponible à l'adresse : http://europa.eu/rapid/press-release_IP-18-4526_en.htm

Au titre du considérant 106 du RGPD, la Commission devrait évaluer le fonctionnement desdites décisions d'adéquation dans un délai raisonnable et communiquer toute conclusion pertinente au comité au sens du règlement (UE) n° 182/2011 du Parlement européen et du Conseil[791] établi en vertu durèglement, au Parlement européen et au Conseil. Toutefois, la liste des pays bénéficiant de « décisions d'adéquation » prises sous l'empire de la Directive 95/46, pourraient avec l'entrée en vigueur du Règlement 679/16 subir des modifications[792]. Ainsi cela conduira à terme à une évolution législative majeure chez chacun des pays bénéficiaires. Si les 27 pays membres de l'Union européenne doivent se mettre à niveau du fait de l'entrée en vigueur de la RGPD, il faudra que la Suisse, le Canada, Israël, l'Argentine, etc. fassent de même. Dans le cas échéant les transferts des données vers ces pays n'auront plus de « niveau adéquat de protection » selon le standard de l'Union européenne. Il en va de même pour le Royaume-Uni suite au Brexit, à défaut d'accord spécifique entre l'Union européenne et le Royaume Uni au plus tard le 29 mars 2019, le Royaume-Uni deviendra un pays tiers à l'Union Européenne dès le 30 mars 2019. Concrètement, si l'Union européenne n'adopte pas une décision spécifique d'adéquation pour le Royaume-Uni avant la date de prise d'effet du Brexit, le Royaume Uni ne pourra plus importer des données depuis l'Union européenne.

108 Des dérogations au principe de protection adéquate. La décision d'adéquation de la Commission n'est pas le seul moyen pour transférer les données hors de l'Union européenne. Il existe des dérogations au principe du niveau de protection « adéquat », l'article 26§2 de la directive 95/46 posait le principe selon lequel un transfert vers un État tiers ne présentant pas un niveau de protection adéquat pouvait néanmoins être autorisé « lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants » ces garanties peuvent « notamment » résulter de « clauses contractuelles appropriées ». L'usage de la formule « notamment » a permis d'élaborer à côté de la solution contractuelle expressément prévue à l'article 26, les « Clauses contractuelles types, des mesures autres permettant de remplir les obligations posées à l'article 26 »[793]. On a assisté alors au développement des règles internes d'entreprise ou *binding corporate rules* (BCR) qui prévoient des engagements et garanties établies dans des codes de conduite et procédures internes à des

---

Voy. S. PEYROU "Protection des données à caractère personnel dans le contexte de l'Accord de partenariat économique UE-Japon : des systèmes en voie de convergence", in *Revue des affaires européennes, Bruylant*, 2018, p. 53

791 Voy. Règlement (UE) no 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

792 Toutefois, le règlement prévoit à l'art. 96 que les accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales qui ont été conclus par les États membres avant le 24 mai 2016 et qui respectent le droit de l'Union tel qu'il est applicable avant cette date restent en vigueur jusqu'à leur modification, leur remplacement ou leur révocation. Le RGPD maintient le principe d'interdiction de transfert des données hors UE. Par exception le Responsable de traitement ou le sous-traitant peuvent transférer des données hors UE seulement s'ils encadrent ces transferts avec des outils assurant un niveau de protection adéquat des personnes. Ainsi aux termes de l'art. 46 ils devront mettre en place : des règles d'entreprises contraignantes (BCR), des clauses contractuelles type approuvées par la Commission européenne, des clauses contractuelles adoptés par une autorité de contrôle nationale et approuvées par la Commission européenne, l'adhésion à des codes de conduites ou mécanismes de certification.

793 J. R. REIDENBERG, « The simplification of international data privacy rules », *Fordham International Law Journal*, 2006, Vol. 29, p. 1133.

groupes de société. Une ultérieure modalité pour le transfert prévu par la directive 95/45 était le transfert des données personnelles bénéficiant d'une autorisation de l'autorité de contrôle. Dans ce dernier cas, l'autorité de contrôle se prononçait favorablement lorsque le traitement garantissait un « niveau de protection suffisant de la vie privée » en tenant compte de clauses contractuelles ou des règles internes appliquées par les parties au transfert. Concrètement, lorsque les parties ont encadré le transfert par un accord intégrant le contenu des « clauses contractuelles types » adoptées par la Commission européenne, par des règles d'entreprise contraignantes (BCR), l'autorité de contrôle autorisait le transfert. Le RGPD simplifie l'ancien régime issu de la directive 95/46, en prévoyant un mécanisme de dispense d'autorisation de l'autorité de contrôle pour les transferts s'appuyant sur des « garanties appropriées ». Il peut s'agir d'un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics; des règles d'entreprise contraignantes[794]; des clauses types de protection des données adoptées par la Commission[795] ; des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission[796]; un code de conduite approuvé[797] , assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées; ou un mécanisme de certification approuvé[798] , assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées. En l'absence de telles garanties, l'autorisation de l'autorité de contrôle reste requise.

109 Les exceptions prévues dans le RGPD. Certaines dérogations au principe d'encadrement général des transferts vers un État non membre de l'Union sont prévues par l'article 49 du RGPD. Ces exceptions ne peuvent être mobilisées que dans des situations particulières. Lorsqu'un État tiers n'est pas reconnu comme offrant un niveau de protection adéquat et en l'absence de garanties appropriées encadrant ce transfert, le transfert peut néanmoins, par exception, être opéré. Ces dérogations ne peuvent être utilisées que dans des situations particulières : les responsables de traitement doivent s'efforcer de mettre en place des garanties appropriées et ne doivent recourir à ces exceptions qu'en l'absence de telles garanties. L'article 49 du RGPD fait l'objet d'une interprétation stricte par les autorités de protection des données, afin que l'exception ne devienne pas la règle. Le RGPD prévoit enfin, lorsqu'aucune de ces dérogations n'est applicable, la possibilité de procéder au transfert suivant des dérogations qui doivent faire l'objet d'une lecture stricte et en présence des conditions cumulatives suivantes : le transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits

794 Conformément à l'article 47 du RGPD.

795 Conformément à la procédure d'examen visée à l'article 93, paragraphe 2 du RGPD.

796 Conformément à la procédure d'examen visée à l'article 93, paragraphe 2 du RGPD.

797 Conformément à l'article 40 du RGPD.

798 Conformément à l'article 42 du RGPD.

et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. L'évaluation faite par l'organisme et les garanties mises en place pour encadrer le transfert, doivent être inscrites dans le registre du responsable de traitement ou du sous-traitant. Dès lors un transfert peut se fonder sur le consentement de la personne[799]; sur la nécessité de sauvegarder les intérêts vitaux de la personne et à ceux d'autres personnes ; sur le nécessité pour des motifs important d'intérêt public[800]; sur la nécessité d'exercer un droit en justice[801]; transfert ayant lieu au départ d'un registre public [802] ; sur la nécessité d'exécuter un contrat entre la personne concernée et le responsable de traitement ou à des mesures précontractuelles prises à la demande de celle-ci[803]; sur la nécessité de conclure un contrat entre le responsable de traitement et un tiers dans l'intérêt de la personne concernée[804]; le transfert est justifié par des intérêts légitimes impérieux du responsable de traitement[805].

B. Du niveau de protection « adéquat » au niveau « substantiellement équivalent »

799 Voy. l'article 49.1 a) du RGPD: La personne dont le consentement est demandé doit avoir été préalablement informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées.

800 Le considérant 112 donne quelques exemple d'intérêt public: par exemple en cas d'échange international de données entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport.

801 Le G29 dans son avis WP 114, p. 17-18 avait exprimé l'idée selon laquelle, appliquée à un contentieux opposant une société mère d'un groupe multinational poursuivie en justice par un salarié en poste dans une filiale européenne, seule certaines données relatives au salariés pourraient être transférées vers le pays tiers et à condition que ces données soient nécessaires à la défense de la maison mère. D'ailleurs cette exception ne pourrait pas être invoquée dans une procédure de Discovery (correspondant à la phase d'investigation et d'instruction préalable au procès civil et commercial devant une juridiction américaine, dans laquelle des milliers de documents peuvent être demandé) lorsque le transfert revêt d'un caractère massif et répété.

802 L'article 49. 1 g) du RGPD précise : le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce. De plus un tel transfert ne doit pas porter sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes justifiant d'un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

803 Selon le G29 dans son avis de 2005 WP 114, p. 115, entrerait dans ce cas l'agence de voyage qui transfère les données personnelles de ses clients à des hôtels situés dans des pays tiers où ces clients sont amenés à séjourner.

804 La CNIL dans son Guide Transfert hors UE, nov. 2012, p. 38 cite comme exemple de cette exception, celui d'un assuré victime d'un accident survenu dans un pays tiers où il séjournait et dont la prise en charge exige que sa compagnie d'assurance (établie dans l'Union européenne) transmet certaines données de l'assuré à la compagnie aérienne du paytiers.

805 Le considérant 113 du RGPD précise que seul les transferts qui peuvent être qualifiés de non répétitifs et qui ne touchent qu'un nombre limité de personnes concernées pourraient également être autorisés aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement, lorsque ces intérêts prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée et lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données.

110 Le *privacy Shield*. L'Union européenne n'a pas reconnu les États-Unis comme un pays disposant d'un niveau de protection adéquat, en raison de sa tradition juridique qui favorise la libre circulation de l'information et octroie d'importants droits à l'État, notamment en ce qui concerne la poursuite des infractions et la lutte contre le terrorisme. Néanmoins, les échanges des données outre-Atlantique occupent une place particulière dans le marché numérique. Afin de faciliter les échanges, un dispositif particulier, le « *Safe Harbor* » ou « sphère de sécurité » a été adopté pour les encadrer. Ce dispositif prévoyait un mécanisme d'autocertification des entreprises américaines qui devait assurer un niveau de protection adéquat. Ce mécanisme se fondait sur la confiance. Toutefois, à cause des révélations dans l'affaire Snowden[806] mettant en lumière les pratiques de surveillance massive des autorités américaines et notamment la *National Security Agency* (« NSA »), cette confiance a été entamée. En effet la Cour de justice a invalidé le « *Safe Harbor* » le 6 octobre 2015 et demandé un niveau de protection substantiellement équivalent à celui de l'Union européenne[807]. Cet accord a été remplacé par un nouveau dispositif, le *Privacy Shield*[808], entré en vigueur le 1er août 2016, suite à une décision d'adéquation de la Commission européenne malgré d'importantes critiques et réserves publiés par le G29 le 13 avril 2016 sur le projet d'accord[809]. Il s'agit d'un mécanisme d'auto-certification pour les entreprises établies aux États-Unis qui a été reconnu par la Commission européenne comme offrant un niveau de protection adéquat aux données à caractère personnel transférées par une entité européenne vers des entreprises établies outre-Atlantique. Il est donc possible de transférer des données personnelles vers les États-Unis, à condition que les entreprises destinataires des données soient référencées dans le registre tenu par l'administration américaine et respectent les obligations et les garanties de fond de cet accord.

806 Voy. l'article : « En trois ans, qu'a-t-on appris des documents Snowden? » Disponible à l'adresse : https://www.lemonde.fr/surveillance-NSA-France/article/2016/12/07/en-trois-ans-qu-a-t-on-appris-des-documents snowden_5044874_4660509.html

807 Voy. le §73 de la décision: Certes, le terme «adéquat» figurant à l'article 25, paragraphe 6, de la directive 95/46 implique qu'il ne saurait être exigé qu'un pays tiers assure un niveau de protection identique à celui garanti dans l'ordre juridique de l'Union. Toutefois, comme l'a relevé M. l'avocat général au point 141 de ses conclusions, l'expression «niveau de protection adéquat» doit être comprise comme exigeant que ce pays tiers assure effectivement, en raison de sa législation interne ou de ses engagements internationaux, un niveau de protection des libertés et droits fondamentaux substantiellement équivalent à celui garanti au sein de l'Union en vertu de la directive 95/46, lue à la lumière de la Charte. En effet, à défaut d'une telle exigence, l'objectif mentionné au point précédent du présent arrêt serait méconnu. En outre, le niveau élevé de protection garanti par la directive 95/46, lue à la lumière de la Charte, pourrait facilement être contourné par des transferts de données à caractère personnel depuis l'Union vers des pays tiers aux fins de leur traitement dans ces pays.

808 La décision sur l'adéquation du Dispositif du Bouclier de Protection des Données UE – États-Unis (« Bouclier de Protection des Données ») ou (« Dispositif), a été adoptée par la Commission européenne le 12 juillet 2016. Ce dispositif a été élaboré par la Commission européenne et le Département du Commerce américain pour remplacer la Décision *Safe Harbor* 2000/520/EC qui a été déclarée invalide par la Cour européenne de Justice le 6 octobre 2015. Voy. la Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 Disponible à l'adresse: https://eur-lex.europa.eu/legal-content/FR/TXT/PDF/?uri=CELEX:32016D1250&from=EN. Pour voy. le rapport annuel sur le *Privacy Shield :* file:///C:/Users/fcaloprisco/Downloads/Reportpdf.pdf

809 En particulier selon l'avis du G29 n° 01/2016 adopté le &3 avril 2016, les modalités d'application du principe de finalité limitée du traitement de données demeurent peu claires. Le principe de durée de conservation limitée des données n'est pas expressément mentionné et ne peut pas se déduire de façon précise en l'état des documents analysés. De plus, il n'existe pas de disposition dédiée à la protection qui devrait être offerte lorsque des décisions individuelles automatisées sont prises sur le seul fondement d'un traitement automatisé de données. Concernant les possibilités nouvelles de recours offertes aux individus pour exercer leurs droits, il remarque que ce mécanisme risque d'être complexe en pratique et difficile à utiliser pour les personnes, notamment du fait qu'il ne s'exercerait qu'en anglais et qu'il pourrait, de ce fait, ne pas offrir une garantie effective. Des précisions doivent donc être apportées sur ces procédures de recours ; en particulier les autorités nationales de protection des données qui le souhaitent devraient pouvoir servir de point de contact pour les citoyens européens et avoir la possibilité d'exercer les recours en leur nom.

Afin de pouvoir s'auto-certifier au « Bouclier de Protection des Données », une entreprise établie aux États-Unis doit être soumise aux pouvoirs de contrôle et d'exécution de la Commission Fédérale du Commerce (« FTC ») ou du Département des Transports américain (« DoT »). D'autres autorités habilitées par la loi pourraient également rejoindre le dispositif à l'avenir. Cela signifie par exemple, que les organismes à but non lucratif, les banques, les sociétés d'assurances et les fournisseurs de services de télécommunication (s'agissant des services fournis au public) ne relèvent pas de la compétence de la FTC ou du DoT et ne peuvent donc pas adhérer au Bouclier de Protection des Données. Dernièrement le Parlement européen a pointé ces défaillances par un projet de résolution. Le texte a été examiné par la Commission des libertés civiles. Suivant l'arrêt de la CJUE, dans le *Privacy Shield*, une clause de revoyure ou de vérification annuelle a été intégrée afin d'apprécier dans le temps la solidité des engagements initiaux. À l'approche de la première vérification programmée en septembre, une délégation de la commission des libertés civiles (LIBE) s'est rendue à Washington. La Commission a constaté des problèmes persistants [810] . Le Parlement a donc adopté une Résolution pour demander à la Commission européenne la suspension de l'accord si les défaillances subsistent au 1er septembre car il « n'assure pas une protection suffisante »[811]. Ces critiques ont été agrémentées du récent Cloud Act [812] qui étend la territorialité des lois américaines au-delà des frontières sans passer par l'entraide judiciaire, et du scandale Facebook-Cambridge Analytica. Deux entreprises pourtant « certifiées » dans le cadre du *Privacy Shield*.

§2. Les instruments de droit privé comme « garanties suffisantes » pour le transfert

111 Des garanties complétant le régime de protection. La décision d'adéquation et le *Privacy Shield* ne sont pas les seuls instruments juridiques pour transférer les données hors UE. En effet échappent à l'interdiction les transferts des données s'appuyant sur un instrument juridique approprié de droit privé. L'objet du transfert des données est économique puisque les données ont progressivement acquis une valeur marchande et constituent une source de revenus pour les entreprises. Ainsi l'exploitation économique des données personnelles par les entreprises peut prendre trois formes : la publicité ciblée, l'amélioration du service rendu, la vente de données personnelles[813]. Cependant, comme affirmé par la Cour de justice dans l'affaire *Osterreicher Rundfunk*, l'objectif de la directive 95/46 n'est pas limité à la libre circulation des donnés pour la réalisation du marché intérieur mais aussi celui d'assurer la protection des droits

810 Voy. le communiqué de presse du parlement européen disponible à l'adresse : http://www.europarl.europa.eu/news/fr/press-room/20170720IPR80211/privacy-shield-deficiencies-still-remain-and-must-be-resolved-says-chair

811 Voy. le texte de la résolution du parlement européen disponible à l'adresse : http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/RE/2018/06-11/1149002EN.pdf

812 Pour comprendre la portée du Cloud Act Voy. l'article disponible à l'adresse : https://www.nextinpact.com/news/106367-cloud-act-lacces-aux-donnees-extraterritoriales-clarifie-auxetats-unis-mais-critique.htm

813 Voy. Conseil D 'État, Etude annuelle 2014. « Le numérique et les droits fondamentaux », p. 6185.

fondamentaux[814]. C'est pour ce motif qu'à côté de la décision d'adéquation de la Commission, d'autres instruments ont été élaborés pour garantir la libre circulation des données tout en garantissant le respect des droits de la personne. L'originalité de ces solutions contractuelles est de permettre à des solutions élaborées par le droit privé d'apprécier la conformité de la législation d'un État tiers au standard européen. Il s'agit de clauses contractuelles (A), clauses contractuelles types et règles internes d'entreprise contraignantes (ci-après BCR) et de l'élaboration de codes de conduites et certifications suivant une logique d'autorégulation (B).

A. Les clauses contractuelles

112 Les clauses contractuelles types. Conformément à l'article 26 §2 de la directive 95/46 et 46 du règlement 679/16, une autorité de contrôle d'un État membre peut autoriser un transfert, ou un ensemble de transferts, vers un pays tiers n'assurant pas un niveau de protection adéquat « lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants ». Cette disposition précise ensuite que « ces garanties peuvent notamment résulter de clauses contractuelles appropriées »[815]. Le règlement 679/16, habilite également la Commission, agissant conformément à la procédure établie à l'article 93 du RGPD, à décider que certaines clauses contractuelles types présentent les « garanties suffisantes ». La notion de « garanties suffisantes », renvoie à celle de « protection adéquate ». Ces garanties sont les suivantes : limitation des transferts à une finalité spécifique ; qualité et proportionnalité des données ; transparence ; sécurité ; droits d'accès, de rectification et d'opposition ; restrictions aux transferts ultérieurs vers des personnes qui ne sont pas parties au contrat ; offre de voies de recours appropriées à la partie lésée en cas d'inobservation des règles. Ces critères doivent servir à apprécier l'efficacité de l'instrument contractuel. Ainsi un contrat joue pleinement son rôle lorsque, en l'absence d'un niveau général de protection adéquat, il renferme dans ses dispositions les éléments essentiels de protection. La Commission européenne, avec l'assistance du Groupe de travail Article 29, a développé des clauses contractuelles types[816] liant les États membres, les autorités nationales en charge de contrôler les flux transfrontaliers de données qui doivent reconnaître ces clauses contractuelles types dans

---

814 CJCE, Österreichischer Rundfunk, affaires jointes C-465/00, C-138/01 et C-139/01, 18 octobre 2007, §39.

815 L'idée d'encadrer les transferts internationaux de données remonte au 1992, lorsque le Conseil de l'Europe, la Chambre de commerce internationale et la Commission européenne ont produit conjointement une étude sur cette question. Voy. "Contrat type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières des données et rapport explicatif", étude entreprise conjointement par le Conseil de l'Europe, la Commission des Communautés européennes et la Chambre de commerce internationale, Strasbourg, 2 novembre 1992.

816 Voy. la Directive 95/46/CE relative à la protection des données, art. 26, para. 4. et la Décision de la Commission, du 27 Décembre 2004 modifiant la Décision 2001/497/CE relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE et la Décision de la Commission du 5 Fevrier 2010,2 010/87relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE du Parlement européen et du Conseil.

leurs procédures[817]. Par conséquent, si le responsable du traitement qui exporte les données et le destinataire du pays tiers concluent et signent ces clauses, celles-ci constituent envers l'autorité de contrôle une preuve suffisante de l'existence de garanties adéquates[818]. Toutefois, l'autorité nationale de contrôle pourra intervenir lorsque les clauses contractuelles types ne sont pas respectées ou que cela est probable et que la poursuite du transfert ferait courir aux personnes concernées un risque imminent de subir des dommages graves[819]. Si on analyse le transfert via les clauses contractuelles types d'un responsable de traitement vers un autre responsable de traitement hors UE, il s'agit d'une opération de cession, permettant l'exploitation des données par l'importateur, pour son propre compte. L'objet principal du contrat est le transfert des données. En revanche, dans le cadre d'un transfert de données opéré vers un sous-traitant, l'objet du contrat consiste à encadrer le transfert nécessaire à l'opération de sous-traitance qui est le contrat principal, le transfert en soi est donc un élément accessoire[820]. L'existence de clauses contractuelles types dans le cadre juridique européen n'interdit pas aux responsables du traitement de formuler d'autres clauses contractuelles *ad hoc*. Celles-ci devraient cependant produire le même niveau de protection que celui apporté par les clauses contractuelles types. Il existe aujourd'hui deux ensembles de clauses types pour les transferts de responsable du traitement à responsable du traitement entre lesquels l'exportateur des données peut choisir [821] . Pour les transferts de responsable du traitement à sous-traitant, il n'existe qu'un ensemble de clauses contractuelles types[822]. Il convient de souligner que l'usage des clauses contractuelles types est facultatif, le responsable de traitement peut choisir de recourir à d'autres mécanismes de droit privé conférant des garanties adéquates comme les

---

817 Voy. art. 288 TFUE.

818 Les autorités nationales et la Commission doivent coopérer et se consulter sur les clauses contractuelles qui leur seront présentées.

819 Voy. Voy. Conclusions de l'avocat général M. Yves Bot présentées le 23 septembre 2015, Affaire C-362/14 Maximillian Schrems contre Data Protection Commissioner. Dans ses conclusions, l'avocat général considère d'une part que la décision d'adéquation de la Commission n'exonère pas les autorités nationales en charge du respect de la vie privée de leurs responsabilités en matière de contrô le et, d'autre part, que cette décision est invalide au vu des informations disponibles sur la protection des données aux États- Unis. La CJ a ainsi invalidé la décision d'adéquation de la Commission 2000/520 assurant un niveau de protection adéquat. L'invalidation d'un acte de l'UE par la CJUE est rarissime mais il existe un précédent récent en matière de données personnelles. Jusqu'avril 2014, la directive « conservation des données » de 2006 permettait la création d'un profil très précis des personnes, les États demeurant libres de définir et d'établir les garanties d'accès aux données collectées. La CJUE, estimant que la vie privée était insuffisamment protégée, l'a invalidée. Un arrê t constatant l'invalidité d'un acte de l'UE le prive de tout effet au niveau européen mais n'invalide pas pour autant les lois nationales qui en découlent. Elle ne fait pas non plus revivre le droit antérieur. Elle s'applique à tous ses États (et non au seul État qui a introduit la question préjudicielle, ici l'Irlande) et a un effet rétroactif.

820 Conseil de l'Europe, Groupe de rédaction du comité consultatif pour la protection des personnes à l'égard du traitement automatisé de données à caractère personnel (STE108), « Étude relative aux contrats encadrant les transferts de données personnelles entre les parties à la Convention 108 et les pays tiers n'offrant pas un niveau de protection adéquat », DG 1, Rapport de Jérôme Huet présenté par la Commission européenne (DG 1), 9 NOVEMBRE 2000, P. 4.

821 L'ensemble I figure à l'annexe de la Commission européenne (2001), décision 2001/497/CE de la Commission du 15 juin 2001 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers en vertu de la directive 95/46/CE, JO 2001 L 181 ; l'ensemble II figure à l'annexe de la Commission européenne (2004), décision 2004/915/CE de la Commission du 27 décembre 2004 modifiant la décision 2001/497/CE en ce qui concerne l'introduction d'un ensemble alternatif de clauses contractuelles types pour le transfert de données à caractère personnel vers des pays tiers, JO 2004 L 385.

822 Commission européenne (2010), décision 2010/87 de la Commission du 5 février 2010 relative aux clauses contractuelles types pour le transfert de données à caractère personnel vers des sous-traitants établis dans des pays tiers en vertu de la directive 95/46/CE, du Parlement européen et du Conseil, JO 2010 L 39.

règles internes d'entreprise (*Binding corporate rules*, BCR) ou se fonder sur les exceptions prévues à l'article 26 §1 de la directive 95/46.

113 Les Règles d'entreprises contraignantes ou BCR. À l'instar des clauses contractuelles types, les règles d'entreprise contraignantes ou *Binding corporate rules* (ci-après « BCR ») à l'intention des responsables du traitement et des sous-traitants contiennent tous les principes en matière de protection des données qu'il convient de respecter lors du traitement des données, même lorsqu'un transfert est effectué vers un autre membre du groupe. Le G29 a insisté sur le fait que l'article 26§2 de la directive 95/46 ne limite pas les garanties d'adéquation aux seules clauses contractuelles, citées uniquement à titre d'exemple[823]. A partir de ce constat, les règles internes d'entreprises se sont développées comme instrument pour encadrer le transfert. Les règles internes d'entreprise (ou *Binding Corporate rules* BCR) constituent un code de conduite définissant la politique globale d'une entreprise en matière de transferts de données personnelles hors de l'Union Européenne[824]. Elles permettent ainsi d'assurer une protection adéquate aux données transférées depuis l'Union européenne vers des pays destinataires n'offrant pas une protection suffisante au sein d'un même groupe de sociétés. Elles constituent une alternative aux clauses contractuelles types ou standards établies par la Commission. Cela correspond au besoin de trouver des mécanismes juridiques alternatifs, puisque les mécanismes existants, fondés sur l'adéquation ou sur les solutions contractuelles sont désormais inadaptés face à la multiplicité des transferts et à la multiplicité des organismes concernés par ces échanges de données. Cependant, le processus de mise en place des BCR s'avère également peu efficace et particulièrement long et inadapté aux besoins des groupes d'entreprises. Une simplification s'imposait. Cette simplification des formalités (déjà initiées dès 2012 par 21 Autorités de l'Union)[825] facilite les démarches de transfert des données personnelles intra-groupes vers des pays destinataires n'offrant pas une protection adéquate, ce qui incitera ainsi plus fortement les groupes multinationaux à adopter les BCR. Le mécanisme de protection

---

823 Voy. avis du G29, WP74, p. 5, « Le groupe de travail souhaite rappeler une fois de plus que l'offre de garanties suffisantes, comme le prévoit l'article 26§2 est une vaste concept qui couvre certes les solutions contractuelles ainsi que les règles d'entreprises contraignantes mais également d'autres situations (…) que les autorités de protection des données peuvent juger pertinentes en vue de l'octroi d'autorisation ».

824 Voy. le document de travail: Transferts de données à caractère personnel vers des pays tiers: application de l'article 26 (2) de la directive de l'UE relative à la protection des données aux règles d'entreprise contraignantes applicables aux transferts internationaux de données (WP74), adopté par le groupe de travail «article 29» le 3 juin 20013, ci-après le «WP74»; le document de travail établissant une liste de contrô le type pour les demandes d'approbation des règles d'entreprise contraignantes (WP108), adopté par le groupe de travail «article 29» le 14 avril 2005, ci-après le «WP108»; la recommandation 1/2007 sur la liste de contrô le type pour les demandes d'approbation des règles d'entreprise contraignantes en vue du transfert de données à caractère personnel (WP133), adoptée par le groupe de travail «article 29» le 10 janvier 2007, ci-après le «WP133»; le document de travail établissant un tableau présentant les éléments et principes des règles d'entreprise contraignantes (WP153), adopté par le groupe de travail «article 29» le 24 juin 2008, ci-après le «WP153»; le document de travail établissant un cadre pour la structure des règles d'entreprise contraignantes (WP154), adopté par le groupe de travail «article 29» le 24 juin 2008, ci-après le «WP154»; le document de travail sur les questions fréquemment posées (FAQ) concernant les règles d'entreprise contraignantes (WP155), adopté par le groupe de travail «article 29» le 24 juin 2008, tel que révisé et adopté le 8 avril 2009, ci-après le «WP155»; la recommandation 1/2012 sur la liste de contrô le type pour les demandes d'approbation des règles d'entreprise contraignantes en vue du transfert de données à caractère personnel à des fins de traitement (WP195) - tous les documents sont disponibles sur le site Internet du groupe de travail.

825 Voy., speech/11/817 Viviane Reding Vice-President of the European Commission, EU Justice Commissioner : « Binding Corporate Rules: unleashing the potential of the digital single market and cloud computing », IAPP Europe Data Protection Congress, Paris, 29 November 2011.

offert par les BCR a été repris dans le nouveau règlement européen, cela est une expression du principe d'*accountability*, d'une démarche de responsabilité qui est le nouveau paradigme établi par le règlement. Elles sont devenues au fil du temps un outil efficace pour encadrer les transferts internationaux de données au sein d'un groupe car à la différence des solutions « classiques » elles sont un instrument souple permettant de tenir compte des spécificités de chaque groupe[826]. Ainsi, les entités d'un groupe ayant adopté la procédure des BCR n'auront plus à solliciter, pour chaque type de transfert vers les pays destinataires n'assurant pas un niveau de protection équivalent à celui de l'Union européenne, une autorisation à l'autorité de contrôle nationale. Désormais, les BCR sont approuvé par les autorités de contrôle compétente pour s'assurer qu'ils offrent un niveau de protection adéquat aux données transférées en dehors de l'Union européenne. Cette évaluation est coordonnée par une autorité désignée « chef de file », unique point de contact de l'entreprise, et est facilitée par une procédure dite de « reconnaissance mutuelle », acceptée par 21 autorités européennes. Ces instruments alternatifs ont été exploités surtout depuis l'affaire *Schrems*[827] lorsque la Cour de justice a annulé la décision d'adéquation vis-à-vis des États-Unis et a jugé qu'il était contraire au droit de l'Union de transférer des données sur la base de l'accord « *Safe Harbor* » adopté sur la base de la décision d'adéquation de la Commission[828]. Cela faisait suite au fait qu'un grand nombre de programmes de surveillance auparavant secrets avaient été dévoilés par les médias[829], sur la base de documents transmis pour l'essentiel par Edward Snowden. Ces programmes portaient sur la collecte massive de données à caractère personnel provenant de diverses sources en ligne et concernant des données relatives aussi bien au contenu qu'au trafic. Selon les rapports, la plupart des programmes ne font pas de distinction entre les personnes, que celles-ci soient suspectées ou non. Une fois invalidée la décision d'adéquation de la Commission, permettant le transfert des données vers les États-Unis, plusieurs entreprises, en attendant un nouvel accord, ont dû recourir aux *Binding corporate rule*s (BCR) et aux clauses contractuelles types adoptées par la Commission européenne afin de donner une base légale aux transferts internationaux de données[830]. L'originalité de ces solutions contractuelles est de permettre à

---

826 Au 1er septembre 2015 Cinquante-sept entreprises multinationales ont adopté des règles internes d'entreprises ayant fait l'objet d'une décision d'autorisation. La liste est consultable sur le site de la Commission.

827 CJUE, Gr.Ch, Maximilian Schrems c. Data Protection Commissioner [Ireland] aff. C-362/14, 6 octobre 2015. La Cour a jugé que l'accès massif, non ciblé et secret à des données à caractère personnel dont le traitement initial relève de la juridiction de l'UE et transférées de l'UE vers un pays tiers dans lequel elles sont ensuite accessibles aux programmes de surveillance dudit pays tiers n'est pas conforme aux exigences imposées par les dispositions de la directive 95/46/CE relatives au transfert des données. Les transferts structurels (en masse) effectués par des responsables du traitement relevant de la juridiction de l'UE sont soumis à la législation européenne – une obligation concernant également les transferts ultérieurs vers d'autres parties dans le pays destinataire, lesquels ne peuvent être effectués que si les dispositions de la directive et des divers instruments de transfert disponibles sont respectées. Cependant, aucune de ces conditions ne prévoit le transfert, à des fins de surveillance, de données à caractère personnel détenues par des responsables du traitement du secteur privé vers des autorités du secteur public de pays tiers.

828 Voy. Décision 2000/520/CE de la Commission du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la «sphère de sécurité» et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique.

829 Essentiellement The Guardian et The Washington Post. http://www.theguardian.com/world/the-nsa-files. http://www.washingtonpost.com/nsa-secrets/.

830 Le règlement 679/16 prévoit d'autres mécanismes pour le transfert, l'article 49 il dispose : En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à

des solutions élaborées par le droit privé d'apprécier la conformité de la législation d'un État tiers au standard européen.

B. Les codes de conduites et certifications

114 Des mesures d'*accountability*. Au titre de l'article 40 du RGPD, les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises. Afin d'encadrer le transfert, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous•traitants peuvent élaborer des codes de conduite, les modifier ou les proroger. Lorsque le code de conduite est approuvé par l'autorité de contrôle il devient contraignant. De plus, si le code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle doit soumettre le projet de code, la modification ou la prorogation, avant approbation, seau du comité, qui rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le RGPD. Lorsque l'avis du comité est positif, le comité soumet son avis à la Commission laquelle peut décider, par voie d'actes d'exécution, que le code de conduite, la modification ou la prorogation approuvés qui lui ont été soumis sont d'application générale au sein de l'Union. En tout état de cause, selon un processus transparent et volontaire, le responsable de traitement peut adhérer à un mécanisme de certification délivré par l'autorité de contrôle ou par un organisme de certification agréé. Ces différents instruments disponibles montrent une faiblesse, due à la carence d'une effective activité de contrôle sur le niveau de protection assuré par ces types d'instruments. Le risque est toujours une nette séparation entre le modèle défini par la législation et la pratique, ainsi la protection des données au-delà des frontières de l'UE peut se traduire dans une formule purement « déclaratoire ».

---

une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes: a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées; b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée; c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale; d) e transfert est nécessaire pour des motifs importants d'intérêt public; e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice; f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement; g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des 'informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.

Section II. Les données personnelles, objet d'une politique économique étrangère de l'Union européenne

115 Des accords spécifiques permettant le transfert des données. À la valeur commerciale de la donnée correspond un flux de transfert des données de plus en plus important. Ainsi des accords internationaux permettant ce transfert ont vu le jour. Grâce au cadre juridique instauré par la Directive 95/46/CE, l'Union européenne a su affirmer au niveau international son modèle de protection[831]. Ainsi certains États tiers ont estimé avantageux d'adopter des règles en matière de protection de données, conformes au modèle communautaire, afin de réduire les charges des entreprises pour s'aligner à la discipline de l'Union européenne[832]. C'est le cas pour le Canada, Israël, Suisse, l'Uruguay et l'Argentine. Cependant, les États-Unis, n'ont jamais modifié leur législation pour aller à l'encontre du standard européen, tout d'abord en raison du pouvoir des sociétés américaines sur le plan international mais surtout de la force politique du gouvernement et des institutions américaines. Ainsi l'accord Union européenne-États-Unis dit « *Safe Harbor* » sur l'échange des données a vu le jour comme un compromis entre deux approches différentes[833]. Cet accord vise à simplifier les transferts des données entre l'Union européenne et les entreprises américaines adhérentes au programme dit de la « Sphère de sécurité » à travers un mécanisme d'auto certification d'adéquation au standard instauré par la directive 95/46[834]. Il convient d'étudier la mise en œuvre de la politique externe de l'Union européenne à travers ces négociations avec les États-Unis §1) afin de vérifier la cohérence entre la protection offerte au niveau interne, et celle offerte au niveau externe §2).

§1 Le bras de fer entre les États-Unis et l'Union européenne

Les États-Unis ont une tradition juridique qui diffère de celle de l'Union européenne. Néanmoins, en raison de l'importance des opérateurs économiques qui y sont établis, un mécanisme particulier alternatif à ceux déjà existantes a été adopté pour encadrer le transfert des données. En 1998, le US *Department of Commerce* et la Commission européenne commencèrent à engager négociations de la durée de deux ans afin d'atteindre une solution de compromis [835]. Ces négociations se sont terminées par la finalisation de l'accord « *Safe*

831 B. HAVELAGE, et A. Ch. LACOSTE, *Les flux transfrontaliers de données à caractère personnel en droit européen*, *JTDE*, Bruxelles, 2001, n°84, p. 14.

832 A. MANTELERO, « La nuova normativa indiana in materia di data protection: la protezione dei dati declinata in maniera funzionale all'outsourcing », *in Contratto e impr. Europa*, 2011, 728 ss. Voy. aussi : G. GREENLEA, « Promises and illusions of data protection in Indian law », in *International Data Privacy Law*, 2011, 1 (1), 47 ss.

833 Sur l'approche différente en matière de protection de données Voy. C.J. BENNET, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca, Cornell University Press, 1992. Voy. également Patrick E. COLE, *New challenges to the US Multinational Corporation in the European Economic Community: Data Protection Laws* ; in *17 N.Y.U J. INTL L. & POL.*, 1995, 893, 897-98.

834 M. FRANCE, « Once again, technology is outrunning privacy law », in *Business Week Online*, Mar. 13 2000 at http://www.businessweek.com/technology/content/003/ep0313.htm, mis à jour le 14.02.2013.

835 W. J LONG, M. P. QUEK, « Personal data privacy protection in an age of globalization: the UE-EU safe harbor compromise », *in Journal of European Public Policy*, 3 June 2002, p. 325-344.

Harbor » en 2000, avec l'adoption par la Commission européenne de la décision d'adéquation 520/2000/CE[836]. Il est important de souligner qu'à l'époque de la conclusion de l'accord *Safe Harbor*, le Parlement européen pouvait seulement être consulté sans aucun pouvoir contraignant d'empêcher la conclusion de l'accord ou influencer son contenu. D'ailleurs il avait exprimé son avis contraire à la Décision 520/2000 de la Commission, tant sous un angle substantiel que procédural et demandait une révision du texte[837] sans que cela ait la moindre résultat sur la conclusion de l'accord. Les principales critiques concernaient le caractère trop restreint de l'accord (il était limité aux secteurs relevant de la juridiction de la *Federal Trade Commission*, il excluait certains secteurs comme les télécommunications et les services financiers, les registres publics) ; l'absence de recours devant une autorité publique et l'absence de garanties concernant la réparation des dommages subis par les particuliers[838]. Ces critiques étaient reprises par le G29 qui, dès le début des négociations, avait montré son hostilité au projet [839] . De plus l'adhésion au *Safe Harbor* de la part des entreprises américaines était facultative, en se basant sur un système d'auto-certification d'adéquation aux règles de l'Union européenne lors du traitement des données provenant de l'UE[840] sans qu'aucun contrôle effectif puisse le vérifier. Au contraire une entreprise de l'UE qui voulait procéder au transfert des données vers les États-Unis avait une obligation de notification à l'Autorité de contrôle nationale. Il s'agissait d'un accord hybride, constitué par la *self regulation*, c'est-à-dire l'auto-certification de l'entreprise américaine (dans le respect de la tradition américaine) et par le contrôle administratif de la part de l'autorité nationale compétente (dans le respect de la tradition européenne). De plus, suite aux révélations du scandale Prism sur le programme d'écoutes développé entre l'Agence américaine de sécurité nationale (NSA) et les GAFA, la pertinence de la décision d'adéquation relative au *Safe Harbor* a été fortement remise en cause et a fait l'objet d'une question préjudicielle devant la Cour de justice[841]. Dans cette optique la décision *Schrems*, a marqué la prise en compte des révélations de Snowden par l'Union

---

836 Commission européenne, décision 520/2000/CE du 26 juillet 2000 conformément à la directive 95/46/CE du Parlement et du Conseil relative à la pertinence de la protection assuré par les principes de la « sphère de sécurité » et par les questions souvent posée y afférentes, publiées par le ministère du commerce des États-Unis d'Amérique, JO 215 du 28 aout 2000, p. 7.

837 European Parliament resolution on the Draft Commission Decision on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (C5-0280/2000 - 2000/2144(COS)), consultabile su http://epic.org/privacy/intl/EP_SH_resolution_0700.html.

838 Voy. P.M. SCHWARTZ, « The EU-U.S. Privacy Collision: a Turn to Institutions and Procedures », in *126 Harv. L. Rev. 1966*, 2012-2013, lequel souligne que «at the start of July 2000, the Commission released the final text of the «*Safe Harbor* Arrangement» and a series of supporting documents. That same month, the EU Parliament rejected the agreement in a nonbinding resolution before the Commission approved it on July 25, 2000».

839 Voy. Avis du G29, WP 15, Avis 1/99, 26 janvier 1999 ; WP 19, Avis 2/99, 19 avril 1999 ; WP 21, Avis 4/99, 7 juin 1999 ; WP 23, 7 juillet 1999 ; WP 27, Avis 7/99 15 et 16 novembre 1999 : WP 31, aVIS 3/2000, 16 MARS 2000 ; WP 32, Avis 4/2000, 16 mai 2000.

840 L'auto certification se fait à travers l'enregistrement en ligne de la part de la société ou de l'entreprise près du *Department of Commerc*e. L'autocertificazione doit inclure une description de la privacy policy de l'entreprise. Le *Federal Trade Commission* maintient une liste d'organismes adhérant au *Safe Harbor* sur le propre site web. L'adhésion au *Safe Harbor* permet à une entreprise américaine d'éviter des négociations avec les autorités de protection des données de chaque État membre ou il exploite sa propre activité.

841 CJUE, question préjudicielle, 25 juillet 2014. Aff. C-362/14, par la Cour suprême irlandaise dans le cadre d'un litige opposant un citoyen autrichien, étudiant en droit à la société Facebook. Voy. sur ce point : Y. PADOVA, « La Cour de justice va-t-elle invalider les accords *Safe Harbor* ? », *RLDI*, 2014, n° 110, p. 14, n° 3624.

européenne et le Conseil de l'Europe[842]. La question préjudicielle avait été soulevée par une juridiction irlandaise qui demandait à la Cour de justice si au regard des articles 7, 8 et 47[843] de la Charte des droits fondamentaux, l'autorité de protection des données nationales, saisie d'une plainte relative au transfert de données vers les États-Unis, était absolument liée par la décision d'adéquation de la Commission du 26 juillet 2000 (2000/540/CE). Déjà avant le renvoi préjudiciel, le G29, avait remis en question l'appréciation du niveau de protection adéquat prévu par le *Safe Harbor* dans une lettre adressée à Mme Viviane Reding, vice-présidente de la Commission européenne [844] . Ces critiques ont constitué le terrain pour l'invalidation de la décision d'adéquation 2000/520/CE de la Commission dans l'affaire *Schrems*[845] (A). Suite à l'invalidation de l'accord *Safe Harbor*, Union européenne et États-Unis ont rapidement conclu un nouvel accord le *Privacy Shield* (B).

A. L'exportation du modèle européen de protection.

116 L'affaire *Schrems*. Dès sa conclusion, l'accord *Safe Harbor* a été fortement critiqué du fait qu'il n'y avait aucune obligation d'adhésion de la part des entreprises américaines. En effet, il s'agissait d'un texte de compromis basé sur l'autocertification facultative des compagnies et avec la totale absence d'un contrôle effectif de la part du *Department of Commerce* américain sur le niveau de protection adéquat des engagements des entreprises américaines[846]. À cet égard, une des critiques majeures de la Cour de justice dans l'affaire *Schrems*[847] porte sur le fait que l'accord *Safe Harbor*, «concerne uniquement le caractère adéquat de la protection fournie aux États Unis par les principes de la sphère de sécurité en vue de répondre aux exigences de l'article 25, paragraphe 1, de la directive 95/46, sans pour autant contenir des constatations suffisantes quant aux mesures législatives interne par lesquelles les États Unis d'Amérique

---

842 Voy. la Résolution du Parlement P7_TA-PROV(2014)0230 du 12 mars 2014 sur le programme de surveillance de la NSA, les organismes de surveillance dans divers États membres et les incidences sur les droits fondamentaux des citoyens européens et sur la coopération transatlantique en matière de justice et d'affaires intérieures du 2 mars 2014; et plus récemment, les études du Parlement européen sur les risques et opportunités suscités par les mutations numériques et l'émergence de la surveillance de masse : « Mass surveillance, part II – Technology foresight, options for longer term security and privacy improvements » ; « Mass surveillance, part I – Risks and opportunities raised by the current generation of network and applications », décembre 2014. Voy. également sur ce point Arcadio Diaz Terera, « La sécurité nationale et l'accès à l'information », Conseil de l'Europe, CDCJ(2013)13293, Strasbourg, Septembre 2013 ; et, plus récemment, Peter Omtizgt, « Les opérations massives de surveillance en Europe », Conseil de l'Europe, CDCJ(2014), AS/Jur(2015)01, Strasboug, janvier 2015.

843 Art. 7 respect de la vie privée, art. 8 droit à la protection des données personnelles, art 47: droit à un recours effectif

844 G29, Letter from the Article 29 Working Party to Vice-President Viviane Reding on the actions set out by the European Commission in order to restore trust in data flows between the EU and the US, 1à avril 2014.

845 CJUE, *Schrems*, aff. C-362/14, 6 octobre 2015.

846 B. EDE, D. BRITNEY, D. STEPHEN, T. SOMA, « An analysis of the bilateral agreements between transnational trading groups: the US/EU E-commerce privacy Safe Harbor », in *Texas International Law Journal*, 2004, 39 no 2 171-214.

847 Il est important de souligner que, dans l'arrêt Schrems, la Cour de justice déclare la nullité de l'acte en cause à titre préjudiciel sans être explicitement requise par la requérante au principal ou par la juridiction de renvoi. La Cour justifie cette intervention sous l'angle du principe d'un recours effectif dans un État de droit et cite sa jurisprudence, voy. *Schrems* §96: affaire *Les Verts/Parlament*, 294/83,§ 23; *Johnston*, 222/84, §18 et 19; *Heylens e a.*, 222/86, §14, et *UGTRioja e a.*, da C428/06 a C434/06, §80.

assurent un niveau de protection adéquat, au sens de l'article 25, paragraphe 6, de cette directive » [848] . De plus, il existait des dérogations générales à l'accord. Ainsi, la décision 2000/520 consacre la primauté des « exigences relatives à la sécurité nationale, à l'intérêt public et au respect des lois des États Unis » sur les principes de la sphère de sécurité des données personnelles. En vertu de ladite primauté, les organisations américaines auto-certifiées recevant des données à caractère personnel depuis l'Union européennes étaient tenues d'écarter, sans limitation, ces principes lorsque ces derniers entraient en conflit avec ces exigences et s'avéraient donc incompatibles avec celles-ci[849] . Selon la Cour de justice, la décision de la Commission, lue à la lumière de l'art. 25 §6 de la directive 95/46/CE[850], ne satisfait pas aux exigences découlant des articles 7, 8 et 47 de la Charte des droits fondamentaux[851]. En effet, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par les articles 7 et 8 de la Charte [852] . De plus, selon la Cour de justice, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de recours afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte[853]. Le motif d'invalidité de la décision de la Commission concerne la façon dont les données sont traitées aux États-Unis une fois transférées. En effet, dans l'ordre juridique des États-Unis, aucune règle n'a été envisagée pour limiter l'ingérence à ce qui est « strictement

---

848 CJUE C-362/14, précité, § 83.

849 CJUE C-362/14, précité, §86.

850 Selon les règles posées par la directive 95/46 (confirmées par le Règlement général de 2016), le transfert de données personnelles des États membres de l'Union vers des pays tiers est interdit, sauf si un niveau de protection «adéquat» est assuré et validé par la Commission par une décision spécifique. Par dérogation à cette interdiction, le transfert vers des pays tiers est également autorisé en cas de consentement de l'intéressé, d'intérêt public prépondérant et sur la base d'instruments contractuels appropriés. Voy. art. 25 §6 de la Directive 95/46: La Commission peut constater, conformément à la procédure prévue à l'article 31 paragraphe 2, qu'un pays tiers assure un niveau de protection adéquat au sens du paragraphe 2 du présent article, en raison de sa législation interne ou de ses engagements internationaux, souscrits notamment à l'issue des négociations visées au paragraphe 5, en vue de la protection de la vie privée et des libertés et droits fondamentaux des personnes. Les États membres prennent les mesures nécessaires pour se conformer à la décision de la Commission.

851 Voy. point 37 de l'arrêt: Par ses questions préjudicielles, qu'il convient d'examiner conjointement, la juridiction de renvoi demande, en substance, si et dans quelle mesure l'article 25, paragraphe 6, de la directive 95/46, lu à la lumière des articles 7, 8 et 47 de la Charte, doit être interprété en ce sens qu'une décision adoptée au titre de cette disposition, telle que la décision 2000/520, par laquelle la Commission constate qu'un pays tiers assure un niveau de protection adéquat, fait obstacle à ce qu'une autorité de contrôle d'un État membre, au sens de l'article 28 de cette directive, puisse examiner la demande d'une personne relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel la concernant qui ont été transférées depuis un État membre vers ce pays tiers, lorsque cette personne fait valoir que le droit et les pratiques en vigueur dans celui-ci n'assurent pas un niveau de protection adéquat.

852 La Cour de justice rappelle ici sa jurisprudence dans l'affaire Digital Rights (voy., en ce sens, arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, point 39).

853 Voy. §89 de la décision : Ainsi que l'a relevé l'Avocat général aux points 204 à 206 de ses conclusions, les mécanismes d'arbitrage privé et les procédures devant la Commission fédérale du commerce, dont les pouvoirs, décrits notamment dans les FAQ 11 figurant à l'annexe II de cette décision, sont limités aux litiges commerciaux, portent sur le respect, par les entreprises américaines, des principes de la sphère de sécurité et ne peuvent être mis en œuvre dans le cadre des litiges portant sur la légalité d'ingérences dans les droits fondamentaux résultant de mesures d'origine étatique.

nécessaire » pour atteindre l'objectif de la protection de la sécurité nationale, ni des recours spécifiques de nature judiciaire ou administrative pour protéger les personnes concernées. De plus, l'absence d'un mécanisme de contrôle indépendant dans la législation n'est pas conforme au niveau de protection « adéquat »[854]. Ici, la Cour de justice, suivant le chemin tracé par l'Avocat général[855], examine la question relative à la conformité de la décision d'adéquation de la Commission 2000/520 aux exigences découlant de la directive 95/46, lue à la lumière de la Charte[856]. Ainsi la décision 2000/520 ne passe pas le test de nécessité et proportionnalité, puisqu'elle ne prévoit pas un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure[857]. Une telle ingérence va bien au-delà de ce qui est strictement nécessaire aux buts d'intérêt général et n'est pas proportionnée à la finalité à atteindre. Or, la Cour de justice se livre à un constat sévère sur l'inertie de la Commission, n'ayant pas réexaminé les circonstances justifiant l'adoption de sa décision 2000/520, alors qu'elle avait elle-même constaté un certain nombre de dysfonctionnements (accès des autorités américaines aux données transférées, traitées en outre d'une manière incompatible avec les finalités de leur transfert, absence de voies de droit administratives ou judiciaires pour les citoyens européens) dans ses communications, intitulées respectivement « Rétablir la confiance dans les flux de données entre l'Union européenne et les États-Unis d'Amérique » et « Communication relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire »[858]. Cette décision semble être la réaction politique de l'Union européenne au scandale « Prism » et marque le changement d'approche, non plus basée sur le critère « d'adéquation » contenu à l'art. 25 de la directive 95/46/CE, mais sur le principe « d'équivalence » au cadre juridique de l'Union européenne[859]. Ce faisant, la Cour de justice a donné un effet extraterritorial au droit à la protection des données personnelles de l'Union obligeant les États-Unis à conclure un nouvel accord, le *Privacy Shield*. Cette « exportation » des normes de l'Union s'est faite grâce au contrôle juridictionnel de la Cour de justice. Cela signifie très nettement que le droit à la protection des données personnelles a plus que jamais une portée mondiale, ce que visait à éviter l'arrêt *Lindqvist* mais qu'avait déjà préfiguré la décision *Google Spain* sur le « droit à l'oubli »[860].

---

854 Voy. § par. 93, 94 e 95 de la décision.

855 L'Avocat général relève que le droit et les pratiques des États-Unis n'assurent pas un niveau de protection adéquat au sens de l'article 25 de la directive 95/46, points 123 et 124 de ses conclusions.

856 Voy. §87 de la décision.

857 Voy. § 93 de la décision.

858 Voy. COM (2013)846 final et COM (2013)847 final.

859 Voit point 72 de la décision : Ainsi, l'article 25, paragraph 6, de la directive 95/46 met en œuvre l'obligation explicite de protection des données à caractère personnel, prévue à l'article 8, paragraphe 1, de la Charte, et vise à assurer, comme l'a relevé M. l'avocat général au point 139 de ses conclusions, la continuité du niveau élevé de cette protection en cas de transfert de données à caractère personnel vers un pays tiers.

860 V. SPIROS TASSIS et M. PERISERAKI, « The Extraterritorial Scope of the Right to Be Forgotten and How This Affects Obligations of Search Engine Operators Located outside the EU », *Eur. Networks L. & Reg*. Q., 2014, p. 244. Disponible à l'adresse: https://heinonline.org/HOL/LandingPage?handle=hein.journals/enlr2&div=31&id=&page=.

B. Le « *Privacy Shield* ». Un accord de compromis

117 Un accord insatisfaisant. Suite à l'affaire *Schrems*, la Commission a dû adopter rapidement une nouvelle décision d'adéquation qui a été suivi par un nouvel accord, le «EU-US *Privacy Shield*» en 2016. Toutefois, la conclusion de ce nouvel accord reste insatisfaisante car il s'est réalisé sans la participation directe des autorités de contrôle des États membres. Or, il s'agit toujours d'un texte de compromis, dû aux différentes approches de la matière. En fait, la protection des données aux États-Unis n'est pas inspirée d'une conception générale et chaque secteur est réglementé par des règles qui lui sont propres. Aux États-Unis, le texte deréférence pour la protection des données personnelles est le *Privacy Act* de 1974 qui régit la protection des données en général. Ce dernier pose trois problèmes au regard de la coopération transatlantique, tout d'abord, il ne protège que les citoyens américains, car il s'applique aux « individus », qui sont définis comme tout « citoyen des États-Unis ou un étranger légalement admis pour une résidence permanente ». Par ailleurs, aucune base juridique n'a été établie pour le principe de finalité reconnu par le *Privacy Act* et de nombreuses dérogations à ce principe sont possibles. Ainsi, même si le consentement de la personne concernée n'est pas obtenu, les données peuvent être utilisées à des fins différentes de celles pour lesquelles elles avaient été collectées. Alors que ce principe est considéré comme fondamental dans la conception européenne, il ne fait pas l'objet d'une affirmation suffisamment claire dans la loi américaine. Enfin, aucun principe général n'existe aux États-Unis pour la durée de conservation des données. Il en résulte un cadre juridique sectoriel, basé sur l'autoréglementation, une approche très différente de celle de l'Union européenne[861]. Ainsi le nouvel accord *Privacy Shield* ne semble pas résoudre les difficultés du *Safe Harbor* et s'aligner à la décision de la Cour de justice dans l'affaire *Schrems*. Si l'on regarde de près, ce nouvel accord peut être analysé en deux parties : d'une part, l'élaboration des *Privacy Principles* (annexé II), d'autre part, les déclarations et engagements du gouvernement et du *Department of Commerce* des États-Unis (annexé I et III au VII). Dans la section dédiée aux *Privacy Principles*, l'accord offre une protection plus élevée par rapport à l'accord *Safe Harbor*, notamment concernant l'adoption de l'approche sur les risques, un renforcement du principe de responsabilité, dans la définition de procédures spécifiques contre des traitements illégaux sur saisine tant de citoyens européens que de la part des autorités de contrôle nationales et surtout un système de contrôle de la part des autorités américaines afin de veiller à la bonne application de l'accord par les entreprises adhérents. Ces avancements s'expliquent par le fait que le nouvel accord *Privacy Shield* a dû tenir compte des nouveaux principes contenus dans le règlement général sur la protection des données pour éviter un clivage substantiel dans la discipline[862]. Cependant, concernant la

861 V. D'ANTONIO, « Il trasferimento dei dati all'estero », in P. STANZIONE, S. SICA (a cura di), *La nuova disciplina della privacy*, Milano, 2004, p. 155 et s.

862 Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. «*Privacy Shield*» draft adequacy decision, «The WP29 considers a review [of the «*Privacy Shield*» adequacy decision] must be undertaken shortly after the entry into application of the General Data Protection Regulation, in order to ensure the higher level of data protection offered by the Regulation is followed in the adequacy decision and its annexes».

deuxième partie de l'accord[863] , en particulier concernant l'accès aux informations et leur utilisation de la part des autorités américaines, les autorités de contrôles européennes ont avancé des critiques concernant le flou dans le texte, et le manque de principes certains, comme la durée de la conservation (*data rétention principle*) et la finalité des traitements et leur limitation (*purpose limitation principle*). Ainsi il manque une discipline détaillée et entourée de garanties concernant le transfert des données qui se trouvent aux États-Unis vers des pays tiers. Des questions liées à l'effectivité du nouvel accord laissent la place à des doutes quant à sa durée dans le temps avant que la Cour de justice n'intervienne à nouveau[864]. Toutefois il est prévu chaque année une révision de l'accord entre la Commission et le *Federal Trade Commission* afin de vérifier que les engagements soient respectés [865] . L'arrêt *Schrems* rappelle le rang constitutionnel du droit à la protection des données personnelles. Toutefois la mise en œuvre par l'Union européenne de sa conception constitutionnelle de la protection des données personnelles lors de ces négociations avec les États-Unis apparaît partielle[866]. Seule une réforme du système de surveillance américain conduisant à instaurer une surveillance ciblée et à mettre en place un contrôle indépendant devrait permettre des échanges de données transatlantiques. Dans cette perspective, le nouvel accord *Privacy Shield* ne semble pas satisfaisant. C'est alors au juge et aux autorités indépendantes de jouer leur rôle dans la société civile afin de garantir une protection effective aux citoyens européens[867]. En conclusion, à travers l'annulation de l'accord *Safe Harbor* et à travers l'analyse du nouvel accord *Privacy Shield*[868] on constate que l'Union européenne n'est pas totalement parvenue à « exporter » son standard de protection des données personnelles sûrement pour ne pas endommager les relations diplomatiques entre les

---

863 Annexé I et de III à VII.

864 S. CARRERA, E. GUILD, « Safe Harbour or into the Storm? EU-US Data Transfers after the Schrems Judgment », in *CEPS Liberty and Security in Europe Papers*, November 2015. Sur l'arrêt et ses effets: V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali Dai "safe harbour principles" al "privacy shield"*, Roma, 2016, Pour un cadre généralsur la protection des données personnelles dans l'Union européenne: C. FOCARELLI, *La privacy, Proteggere i dati personali oggi*, Bologna, 2015, p.16.

865 Voy.: First review on EU-US privacy Shield 18 october 2017. Dispobile sur le site de la Commission: http://europa.eu/rapid/press-release_IP-17-3966_en.htm Le rapport suggère un certain nombre de recommandations pour assurer le bon fonctionnement du *Privacy Shield*: Un suivi plus proactif et régulier de la conformité des entreprises à leurs obligations par le Département du Commerce des États-Unis. Le Département du Commerce des États-Unis devrait également effectuer des recherches régulières pour les entreprises faisant de fausses déclarations au sujet de leur participation au *Privacy Shield*. Plus de sensibilisation pour les individus de l'UE sur la façon d'exercer leurs droits dans le cadre du *Privacy Shield*, notamment sur la manière de porter plainte. Une coopération plus étroite entre les responsables de la protection de la vie privée, à savoir le Département du Commerce des États-Unis, la Federal Trade Commission et les autorités de protection des données de l'UE (DPA), notamment pour élaborer des directives pour les entreprises et les autorités. Enchâssant la protection des non-Américains offerte par la Directive Politique Présidentielle 28 (PPD-28), dans le cadre du débat en cours aux États-Unis sur la réautorisation et la réforme de l'article 702 de la loi FISA. Désigner dans les plus brefs délais un ombudsman permanent du bouclier de protection des renseignements personnels, et veiller à ce que les postes vacants soient pourvus par le Conseil de surveillance de la protection de la vie privée et des libertés civiles.

866 M.VALERIE, « La dimension externe de la protection des données à caractère personnel: acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, 2006, p. 549-559.

867 Voy. CJUE, Schrems, §54 et 58 et dans le même sens : CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., aff. j. C-293/12 & C-594/12, §68.

868 Voy. la décision d'adéquation de la Commission C(2016) 4176 final du 12 juillet 2016 concernant le transfert des données UE-États-Unis dans l'accord *Privacy Shield*. Le nouvel accord fait suite à l'arrêt du 6 octobre 2016 (affaire *Schrems*) qui ainvalidé la décision d'adéquation de la Commission sur le transfert des données de l'accord *Safe Harbor*.

deux entités. Ce qui nous mène à analyser une ultérieure tentative d'imposer le standard de protection de l'Union européenne, grâce à l'effet extraterritorial du droit à la protection des données personnelles dans l'affaire *Google Spain*.

§2. L'extraterritorialité à l'ère du numérique

118 La souveraineté digitale comme moyen pour affirmer l'identité de l'Union. À l'ère de la globalisation et de l'internationalisation des échanges, le traitement des données ne connaît plus de frontières et la technologie rend de plus en plus facile la dissémination ou la délocalisation des traitements[869]. Dans l'environnement particulier que représente Internet, la question de *l'applicabilité* du droit de l'Union européenne, demeure cruciale[870]. Or, une fois les données transférées hors des frontières, le régime de protection ne s'applique pas et d'importantes disparités existent entre d'une part, ceux pour lesquels la protection des données repose pour l'essentiel sur l'autorégulation comme les États-Unis et d'autre part les pays dotés de législations spécifiques comme l'Union [871] . Dans un cyberespace qui s'affranchit des frontières géographiques, les notions traditionnelles de territoire et de souveraineté nationale sont peu opérantes. En conséquence, le pouvoir de contrainte de l'État est considérablement plus compliqué. Si l'idée que l'Internet est une zone de « non droit » doit être écartée (le droit national s'applique aux individus notamment là où ils résident) il n'en reste pas moins que sa régulation demeure un défi de taille pour l'Union européenne. La protection des données personnelles sur l'Internet est donc un enjeu primordial, indissociable de la préservation des libertés fondamentales et notamment du droit à la vie privée qui repose sur la reconnaissance du droit pour tout individu de disposer d'un espace privé protégé de la vie en société. Ainsi il n'est pas possible de parler de « dimension externe » de la protection des données personnelles sans évoquer le débat sur la gouvernance de l'Internet, sur le rôle de l'Union européenne dans la défense de ses valeurs. Il faut donc questionner sur la notion de souveraineté numérique et repenser notre conception classique de souveraineté puisque les enjeux pour l'Union européenne sont multiples, tout d'abord sociétaux avec une interrogation sur l'application effective de ses valeurs et les droits fondamentaux. Ainsi l'analyse de l'affaire *Google Spain* nous permet d'analyser le raisonnement de la Cour de justice permettant un effet extraterritorial du droit de l'Union européenne (A) ce qui a conduit le législateur à le codifier dans le RGPD (B).

869 Voy. Conseil de l'Europe, rapport de J. Ph. WALTER, *Défis posés par les flux transfrontières de données à caractère personnel*, 30 mai 2006.

870 B. HAVALANGE et A. Ch. LACOSTE, « Le flux transfrontaliers des données à caractère personnel en droit euroopéen », *JTDE*, Bruxelles, 2001, n°48, p. 240.

871 L. CADOUX, « La protection des données personnelles en dehors de l'Europe communautaire », *RFAP*, 1999, n° 89, p. 83.

A. « L'affaire *Google Spain* ». L'extension du champ de protection

119 Le raisonnement de la Cour de justice. Lorsque la Cour de justice affirme dans l'affaire *Google Spain* que la société américaine Google Inc. est établie dans l'Union européenne au titre de la directive 95/46, et qu'elle est soumise au respect de sa législation, elle affirme sa souveraineté sur une entité économique qui opère dans l'espace européen à travers Internet bien qu'établie aux États-Unis. Il s'agit d'une vision confirmée un an plus tard dans l'affaire *Schrems* lorsque la Cour de justice affirme que le transfert des données des citoyens européens vers les États-Unis est interdit si le transfert ne respecte pas la législation de l'Union européenne. Cela correspond à la tentative d'affirmer une souveraineté digitale de l'Union européenne au-delà de ses frontières. Ainsi l'idée selon laquelle Internet constituerait un espace a-territorial et donc non soumis à la souveraineté de l'État a été dépassée et les activités liées à Internet ont été réglementées[872]. Dans la société de l'information, les fournisseurs de moteurs de recherche sur Internet jouent un rôle essentiel d'intermédiaires. D'une part, en tant que prestataires de services[873] aux utilisateurs, les moteurs de recherche collectent et traitent de grandes quantités de données d'utilisateurs, d'autre part, en tant que fournisseurs de contenus, les moteurs de recherche contribuent à rendre les publications sur Internet facilement accessibles et gratuites. L'affaire concernant le moteur de recherche *Google Spain* s'inscrit dans une démarche de revendication de la souveraineté de l'Union à l'ère du numérique. Certains auteurs ont également parlé de l'applicabilité de la théorie des effets[874]. Ainsi statuer en sens inverse serait revenu à désavantager grandement les responsables de traitement européens qui, eux, sont déjà soumis à la directive[875].Dans cette affaire, la Cour de justice a été saisie de plusieurs questions préjudicielles concernant l'interprétation de plusieurs dispositions de la directive 95/46 sur la protection des données personnelles[876]. La première question se référait au champ d'application

---

872 Le concept de Souveraineté dans son sens traditionnel : le pouvoir de contrôler de iure et de facto, un espace déterminé, les activités, ceux qui rentrent dans cet espace, son organisation, l'administration des pouvoirs de police, judiciaires et la sécurité dans cet espace. Voy. T.S. WU, *Cyberspace Sovereignty? The Internet and the International System*, 10 *Harv. J. L.&Tech*., 1997, p. *647*. Voy. également V. Z. ZENCOVICH, *Around the CJEU Schrems Decision: Digital Sovereignty and International Governance of Telecommunication Networks*, 2 june 2016, available at https://ssrn.com/abstract=2788789 or http://dx.doi.org/10.2139/ssrn.2788789.

873 Dans le contexte de la directive sur le commerce électronique (2000/31/CE), les moteurs de recherche sont considérés comme une catégorie de service de la société de l'information, en l'occurrence, des outils de localisation d'informations. Voy. l'article 2 de la directive 2000/31/CE. Cet article fait référence à la directive 98/34/CE, qui définit la notion de service de la société de l'information et l'article 21.2, en relation avec le considérant 18, de la directive sur le commerce électronique (2000/31/CE).

874 M. KOEKKOEK et B. VAN ALSENOY, « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted », *International Data privacy law*, 2014, p. 109. Bien que cette théorie soit généralement pratiquée en matière de droit de la concurrence, elle permet à un État d'intervenir à l'égard d'actes perpétrés à l'étranger dès lors que ceux-ci produisent des effets substantiels sur son territoire

875 M. KOEKKOEK et B. VAN ALSENOY, « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted », *op. cit.*, p. 113.

876 Il était demandé l'interprétation des articles de la directive 95/46 Articles 2, 4, 12 et 14 concernant le champ d'application matériel et territorial, le rôle des Moteurs de recherche sur Internet, la responsabilité de l'exploitant du moteur de recherche et

territorial de la directive, la seconde à la position juridique du moteur de recherche Google en tant que fournisseur de services et en particulier si celui-ci pouvait être considéré comme un responsable de traitement *ratione materiae*. La troisième question concernait le droit à l'oubli, c'est-à-dire la possibilité pour la personne de demander au moteur de recherche en tant que responsable du traitement, l'effacement des liens hypertextes afin que les résultats la concernant ne soient plus accessibles. Nous nous pencherons ici sur la première et deuxième question, la troisième question relative au droit à l'oubli ayant été analysée dans le premier chapitre.

120 L'application de la directive 95/45 lorsque le responsable de traitement dispose d'un établissement secondaire sur le territoire d'un État membre. Concernant la première question préjudicielle, la Cour de justice établit que les activités du moteur de recherche Google sont déroulées, par la société mère établie dans un pays tiers (Californie/Usa) laquelle indexe et archive les recherches effectuées sur le web des filiales qui se trouvent dans différents États membres de l'Union européenne qui offrent l'interface du service du moteur de recherche aux utilisateurs d'un État membre déterminé. L'article 4, § 1er, a), de la directive 95/46 dispose que lorsque « le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire [d'un] État membre », les règles nationales de cet État, transposant le droit européen, doivent s'appliquer.
L'article 4 de la directive concernant le droit applicable a deux raisons d'être. La première est d'éviter qu'il y ait des lacunes dans le système communautaire de protection des données en place et que celui-ci ne soit contourné[877]. La seconde est d'empêcher que la même opération de traitement puisse être régie par le droit de plusieurs États membres de l'UE[878]. Sur base de cette disposition, la Cour de justice de l'Union européenne a estimé que « lorsque l'exploitant d'un moteur de recherche crée dans un État membre une succursale ou une filiale destinée à assurer la promotion et la vente des espaces publicitaires proposés par ce moteur et dont l'activité vise les habitants [d'un] État membre », il faut alors considérer que l'établissement ainsi créé effectue un traitement de données à caractère personnel « dans le cadre des activités d'un

la portée des obligations de cet exploitant et les droits de la personne concernée à la lumière de la Charte des droits fondamentaux de l'Union européenne (Articles 7 et 8).

877 La directive 95/46 dispose dans son article 4 §1a) qu'elle s'applique lorsque: « le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement sur le territoire de l'État membre; si un même responsable du traitement est établi sur le territoire de plusieurs États membres, il doit prendre les mesures nécessaires pour assurer le respect, par chacun de ses établissements, des obligations prévues par le droit national applicable » et §1 c) lorsque le responsable du traitement n'est pas établi sur le territoire de la Communauté et recourt, à des fins de traitement de données à caractère personnel, à des moyens, automatisés ou non, situés sur le territoire dudit État membre, sauf si ces moyens ne sont utilisés qu'à des fins de transit sur le territoire de la Communauté.

878 Avec l'entrée en vigueur du règlement 679/2016 le problème relatif à la législation nationale applicable n'a plus raison d'exister car il y aura une règlementation uniforme pour tous les États membres. Le règlement reprend dans son art. 3 le concept de cadre d'activité présent dans la directive 95/46 et précise : 1) « Le présent règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union ». 2) « Le présent règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union.

établissement du responsable de ce traitement sur le territoire de [cet] État membre »[879]. Pour autant, l'établissement dont il est question ne doit pas nécessairement avoir été préalablement qualifié de « responsable de traitement » et le traitement ne doit pas nécessairement avoir lieu sur le territoire de l'un des États membres de l'Union[880].

Le Groupe de travail art. 29 avait déjà rendu un avis concernant l'interprétation de la directive 95/46 aux traitements des données personnelles par les moteurs de recherche. Selon l'avis 1/2008[881], le fournisseur de moteur de recherche en qualité de responsable du traitement est tenu au respect de la directive 95/46 laquelle s'applique généralement au traitement des données à caractère personnel par les moteurs de recherche, même lorsque le siège de ces derniers se trouve en dehors de l'EEE si se réalise l'exercice effectif et réel de l'activité à travers une organisation stable. L'existence d'un « établissement » au sens de la directive 95/46 implique « l'exercice effectif et réel d'une activité stable ». La forme juridique de l'établissement, un bureau, une filiale possédant la personnalité juridique ou une agence n'est pas déterminante. Cependant, l'opération de traitement doit être effectuée « dans le cadre des activités » de l'établissement. Cela signifie que la législation applicable n'est pas celle de l'État membre où le responsable est établi mais celle de l'État où le responsable mène ses activités de traitement des données[882]. Le critère de « cadre d'activités » a été choisi par le législateur pour éviter que les entreprises contournent le droit européen et bénéficient d'un régime juridique moins contraignant[883]. Ainsi la Cour de justice considère que le lieu où les données sont physiquement traitées n'est pas déterminant pour l'application de la législation de l'Union européenne[884]. Ce qui relève est le lieu où le moteur de recherche exerce son activité, il peut s'agir d'une succursale ou une filiale dans un État membre finalisé à la promotion et la vente de l'espace publicitaire proposé par ce moteur de recherche et dont l'activité est destinée aux habitants de cet État membre. L'interprétation de la Cour de justice anticipe les règles contenues dans le règlement 679/16 sur le champ d'application territorial. Or, selon l'interprétation de la directive 95/46 par la Cour de justice, le droit de l'Union européenne s'applique premièrement, lorsque le fournisseur de moteur de recherche possède un établissement dans un État membre, tel que prévu à l'article 4, paragraphe 1, point a). Deuxièmement, lorsque le moteur de recherche

---

879 En l'espèce, il s'agissait de la société *Google Spain*, filiale de Google Inc. Les activités du moteur de recherche de Google ont été considérées comme étant effectuées *dans le cadre des activités* de *Google Spain*, établissement secondaire situé en Espagne.

880 En l'espèce, il s'agissait de la société *Google Spain*, filiale de Google Inc. Les activités du moteur de recherche de Google ont été considérées comme étant effectuées *dans le cadre des activités* de *Google Spain*, établissement secondaire situé en Espagne. Sur ce point Vo. L. MOEREL, « The long arm of EU data protection law : Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide ? », *International Data Privacy Law*, 2011, p. 29.

881 Voy. l'Avis du G29, 1/2008 du 4 avril 2008 sur les moteur de recherche.

882 G. CAGGIANO, « L'interpretazione del criterio di collegamento del contesto delle attività di stabilimento », del responsabile del trattamento dei dati personali, In *Il diritto all'oblio dopo la sentenza Google Spain*, G. RESTA e V. Z. ZENCOVICH (a cura di), Roma Tre Press sp. p.43 et ss.

883 Voy. considérant 18 de la directive 95/46. En pratique, le critère du cadre des activités a été préféré à des critères territoriaux rigides, tels que la localisation du fichier contenant les données à caractère personnel (critère du pays d'origine).

884 Dans son arrêt *Weltimmo*, postérieur à *Google Spain*, la Cour considère qu'un responsable de traitement dispose d'un établissement établi dans un État membre si ce dernier peut être qualifié « d'installation stable » et qu'il exerce une « activité effective et réelle, même minime » dans le cadre du traitement des données personnelles dont il est question. *Voy*. C.J.U.E., 1er octobre 2015 (Weltimmo s.r.o. c. Nemzeti Adatvédelmi és Információszabadság Hatóság), C-230/14, § 41.

recourt à des moyens situés sur le territoire d'un État membre, tel que prévu à l'article 4, paragraphe 1, point c) de la directive. Dans ce second cas, le moteur de recherche, en vertu de l'article 4, paragraphe 2 de la directive, doit désigner un représentant sur le territoire dudit État membre. En vrai il n'était pas contesté que *Google Spain* était bien un établissement au sens de la directive 95/46 mais plutôt que les activités « d'exploration » et « d'indexation » pour les besoins du moteur de recherche devaient être considérées comme « effectuées dans le cadre des activités » de Google. La Cour de justice estime que l'activité de *Google Spain* rentre dans le cadre d'activité de Google Inc. puisque l'établissement *Google Spain* « est destiné à assurer la promotion et la vente des espaces publicitaires proposés par le moteur de recherche, qui servent à rentabiliser le service offert par ce moteur qui servent à rentabiliser le service offert par ce moteur »[885] . La Cour de justice reprend la position du G29[886] et affirme que l'application territoriale de la directive 95/46 dépend du lieu d'établissement du responsable du traitement. Pour qu'il soit possible de parler d'établissement il faut se référer au « cadre d'activités » et aux « moyens ». Le concept « cadre d'activité stable » avait déjà été précisé par la jurisprudence de la Cour de justice, ce qui implique « la réunion permanente de moyens humains et techniques nécessaires à la détermination des prestations des services » [887] . La notion de « cadre d'activités » comporte que la législation applicable sera celle de l'État où le responsable de traitement mène les activités liées au traitement des données[888]. Le législateur européen a choisi comme critère d'application territoriale de la directive 95/46 le responsable du traitement (qu'il soit établi ou non sur le territoire de l'Union européenne) et non un critère excentré sur la personne dont les informations sont traitées (la personne concernée). Cela s'explique par le fait que la directive a été adoptée premièrement pour promouvoir le marché intérieur et non sur la base d'un droit fondamental à la vie privée[889].

B. La codification de l'extraterritorialité dans le RGPD

121 Un champ d'application territorial plus élargi. Le droit à l'oubli est une réalité devenue nécessaire, spécialement au regard de notre conception européenne du droit à la vie privée. Les

---

885 Voy. point 56.

886 Dans l'Avis n. 8/2010 sur le droit applicable (WP 179), p. 8 et ss,le Groupe de travail «Article 29» a souligné que les principaux critères à prendre en considération pour déterminer le droit applicable sont le lieu d'établissement du responsable du traitement et, si celui-ci se trouve en dehors de l'EEE, la localisation des moyens utilisés.

887 CJCE, 4 juillet 1985, Bergholz, C-168/84, point 19 « l'installation destinée à une activité commerciale (…) ne saurait être qualifiée comme établissement stable au sens de la disposition citée que si cet établissement comporte une réunion permanente de moyens humains et techniques nécessaires aux prestations de services en cause et si ces prestations ne peuvent pas être utilement rattachées au siège de l'activité économique du prestataire ».

888 Voy. point 57 de l'arrêt *Google Spain* : « À cet égard, il convient de rappeler que, ainsi qu'il a été précisé aux points 26 à 28 du présent arrêt, l'affichage même de données à caractère personnel sur une page de résultats d'une recherche constitue un traitement de telles données. Or, ledit affichage de résultats étant accompagné, sur la même page, de celui de publicités lié es aux termes de recherche, force est de constater que le traitement de données à caractère personnel en question est effectué dans le cadre de l'activité publicitaire et commerciale de l'établissement du responsable du traitement sur le territoire d'un État membre, en l'occurrence le territoire espagnol ».

889 Voy. Considérant 3 Dir.95/46/CE.

difficultés liées à l'ubiquité de l'Internet ont obligé le législateur européen à adopter des mesures qui, par la force des choses, s'appliquent à des entités établies à l'étranger. En effet, la problématique est susceptible de toucher n'importe quel citoyen du monde ayant accès à une connexion Internet, c'est en effet une solution globale, et non pas exclusivement européenne, qu'il faudra trouver dans le futur. Certains auteurs plaident pour des négociations internationales[890].

Le droit à l'oubli, bien que présenté comme un « droit à l'effacement » à l'article 17 du nouveau règlement, est expressément mentionné dans ses considérants 65 et 66. Ce dernier serait particulièrement pertinent « lorsque la personne concernée a donné son consentement à l'époque où elle était enfant et n'était pas pleinement consciente des risques inhérents au traitement, et qu'elle souhaite par la suite supprimer ces données à caractère personnel, en particulier sur Internet »[891].

Ce droit à l'oubli devrait également permettre de demander la suppression de données automatiquement collectées, tels que les adresses IP ou les cookies[892], grâce à la définition large de la nouvelle notion de « données à caractère personnel ».[893]

Le premier paragraphe de l'article 17 établit une liste de six situations dans lesquelles « la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant » : a) les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ; b) la personne concernée retire son consentement sur lequel est fondé le traitement ; c) la personne concernée s'oppose au traitement ; d) les données ont fait l'objet d'un traitement illicite; e) les données à caractère personnel doivent être effacées pour respecter une obligation légale; f) les données ont été collectées dans le cadre d'une offre de services d'une société de l'information durant l'adolescence.

Parmi les obligations les plus contraignantes du nouveau règlement, l'obligation de notifier aux tiers les corrections apportées aux données est sans nul doute l'une des plus remarquables[894]. L'article 17, §2, dispose en effet que « lorsqu'il a rendu publiques les données à caractère personnel et qu'il est tenu de les effacer […], le responsable de traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, y compris d'ordre technique, pour informer les responsables de traitement qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement par ces responsables du traitement de tout lien vers ces données à caractère personnel, ou de toute copie ou

---

890 S. CORBETT, « The retention of personal information online ; A call for international regulation of privacy law », *Computer Law & Security Review*, 2013, pp. 246-254.

891 Voy. Considérant 65 du règlement 2016/679.

892 C. TANKARD, « What the GDPR means for business », *Network Security*, 2016, n° 6, p. 5.

893 *Voy*. art. 4, 1) du règlement 2016/679. L'identification pourra s'opérer directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

894 M. BURRI, R. SCHÄR, T*he Reform of the EU Data Protection Framework : Outlining Key Changes and Assessing Their Fitness for a Data-driven Economy*, Journal of Information Policy, 2016, Vol. 6, p. 14 ; P. DE HERT et V. PAPAKONSTANTINOU, *The new General Data Protection Regulation : Still a sound system for the protectionof individuals*, In Computer Law & Security Review, 2016, p. 188.

reproduction de celles-ci. ». Toutefois, il s'agit d'une *obligation de moyen* et non pas *de résultat*. Le responsable de traitement ne sera pas nécessairement sanctionné s'il ne parvient pas à informer l'ensemble des responsables de traitement qui traitent les données de la personne concernée. Il pourra notamment invoquer l'impossibilité de satisfaire à ses obligations dû à des raisons techniques (il ne dispose pas des technologies nécessaires) ou à des coûts de mise en œuvre trop élevés.

L'article 17, §3, établit une liste de cinq exceptions limitant le droit à l'effacement[895]. Concernant l'exception de la liberté d'expression, une analyse au cas par cas devrait permettre de mettre en balance les différents droits fondamentaux en présence[896].

La question de l'équilibre à entretenir entre les droits fondamentaux reste, malgré l'entrée en vigueur du règlement 679/16, l'un des enjeux les plus cruciaux. L'introduction de la liberté d'expression comme exception à l'exercice du droit à l'oubli souligne la volonté politique de l'Union de maintenir sur un même pied d'égalité les droits reconnus par la Charte européenne. A nouveau, seule une analyse au cas par cas, avec l'aide de la jurisprudence permettra de partager les intérêts opposés des personnes concernées et des responsables de traitement.

Dans l'affaire *Google Spain*, la Cour de justice reprend les conclusions de l'Avocat général et estime que Google « développe ses activités essentiellement à destination des entreprises établies en Espagne, agissant en tant qu'agent commercial (du groupe Google Inc.) dans cet État membre. Son objet social est de promouvoir, de faciliter et d'effectuer la vente de produits et de services de publicités en ligne à des tiers ainsi que le marketing de cette publicité »[897]. Les deux finalités, de recherche et de publicité du moteur de recherche doivent être considérées comme inséparables et le traitement des données doit être considéré comme effectué dans « le cadre d'activités » de la filiale[898]. Une telle interprétation de l'art. 4 de la directive 95/46, a justifié la refonte de la législation en matière de protection des données personnelles[899]. Ainsi

---

895 Les autres exceptions sont relatives au respect d'une obligation légale, à des motifs d'intérêt public dans le domaine de la santé publique, à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, ou à la contestation, l'exercice ou la défense de droits en justice.

896 C'est d'ailleurs ce que suggère le considérant 4 du règlement 2016/679.

897 Voy. Point §58 de la décision.

898 Voy. la différence entre l'affirmation de la Cour de justice dans l'arrêt du 20 mai 2003, Österreichischer Rundfunk, aff. Jointes C-465/00, C-138/01 et C-139/01, §37 : Après avoir constaté que la directive, adoptée sur le fondement de l'article 100 A du traité, a pour objectif la réalisation du marché intérieur, dans le cadre duquel s'inscrirait la protection du droit à la vie privée (…) et l'affirmation dans l'arrêt du 7 mai 2009, Rijkeboer, aff. C-553/07, § 38 : Il convient de rappeler, à titre liminaire, que les dispositions de la directive 95/46, en ce qu'elles régissent le traitement de données à caractère personnel susceptible de porter atteinte aux libertés fondamentales et, en particulier, au droit au respect de la vie privée doivent nécessairement êt re interprétées à la lumière des droits fondamentaux garantis par la Charte (voy. arrêts *Google Spain* et Google, C 131/12, EU:C:2014:317, point 68, ainsi que Ryneš, C 212/13, EU:C:2014:2428, point 29). Une vision équilibrée de la CJ on la retrouve dans l'affaire 7 novembre 2013, IPI, aff. C-473/12, § 28: Il ressort des considérants 3, 8 et 10 de la directive 95/46 que le législateur de l'Union a entendu faciliter la libre circulation des données à caractère personnel en rapprochant les législat ions des États membres tout en sauvegardant les droits fondamentaux des personnes, notamment le droit à la protection de la vie privée, et en garantissant un niveau élevé de protection dans l'Union. L'article 1er de cette directive prévoit ainsi que les États membres doivent assurer la protection des libertés et des droits fondamentaux des personnes physiques, notamment de leur vie privée, à l'égard du traitement des données à caractère personnel (arrêts Huber, précité, point 47, ainsi que du 24 novembre 2011, ASNEF et FECEMD, C 468/10 et C 469/10, Rec. p. I 12181, point 25). Voy. G. Caggiano, précité, *L'interpretazione del 'contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personal*i, in Dir. Inf. 2014, 616-618; e in G. Resta – V. Zeno-Zencovich (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, p.55 ss.

899 Voy. Commissione, doc. COM(2012)11 def. - 2012/0011(COD) cit., p. 2, par. 1, COM(2010) 245 def. du19 mai 2010; COM(2010)2020 def. du 3 mars 2010.

selon le nouveau règlement 679/2016, le responsable du traitement établi dans un pays tiers sera tenu à l'application du règlement lorsqu'il offre des biens ou des services aux personnes résidant dans l'Union européenne. Une telle approche, qui lie l'applicabilité territoriale du droit de l'Union au public ciblé, garantit une protection effective du droit à la protection des données personnelles. Le RGPD prévoit un champ d'application territoriale du droit de l'Union européenne beaucoup plus large, au point de faire parler d'extraterritorialité. Ainsi le RGPD s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. Ce critère d'établissement du traitement était déjà consacré par la directive 96/46 mais dans le RGPD il est pris en compte aussi le lieu d'établissement du sous-traitant puisque sa responsabilité peut désormais être engagée. Le RGPD prévoit également un deuxième critère de rattachement en considération de la situation géographique des personnes concernées par le traitement de données. En effet, lorsque ces dernières se situent sur le territoire de l'Union le RGDP s'appliquera alors même que le responsable et le sous-traitant ne l'est pas et cela dans deux hypothèses : lorsque les activités de traitement sont liées à l'offre de bien ou de services à des personnes concernées dans l'UE, qu'un paiement soit exigé ou non desdites personnes, et lorsque de telles activités sont liées au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union européenne.

CONCLUSION DU CHAPITRE I

Dans l'environnement particulier que représente Internet, la question de l'applicabilité du droit de l'Union européenne en matière de protection des données personnelles est stratégique. Lorsque le responsable de traitement est situé au sein de l'Union européenne, le droit européen s'applique naturellement au travers des lois nationales le transposant. Mais force est de constater qu'un grand nombre de services numériques, tels que les moteurs de recherche et les réseaux sociaux, bsont issus d'États tiers, tels que les États-Unis par exemple.
Le different approche fait débat : l'Union européenne articule des principes de protection de la personne et de libre circulation, les Etats-Unis favorisent les libertés du commerce et d'expression[900] . Il a été analysé ici que les solutions apportées par la Cour de Justice et l'efficacité des mécanismes à travers lesquels le droit de l'Union européenne garantit un haut degré de protection aux données personnelles dans leur dimension externe, lorsqu'elles font l'objet d'un transfert. A cet égard, aucun des instruments permettant le transfert des données ne comporte de dispositions autorisant des transferts de données massifs, structurels ou illimités. De plus de tels transferts ont fait l'objet d'une analyse sévère de la part de la Cour de justice à plusieurs reprises. Face aux enjeux économiques et sécuritaires dont les données font l'objet,

900 N. MARTIAL-BRAZ, J. ROCHEFELD, E. GATTONE, *Quel avenir pour la protection des données à caractère personnel en Europe* ? Dalloz. 2018, p. 2788.

l'Union européenne a su progressivement affirmer, sur la scène internationale, son standard de protection. Ce standard a influencé d'autres systèmes juridiques de pays tiers qui ont remodelé leurs législations internes relatives à la protection des données personnelles en calquant le modèle européen. Même les États-Unis, avec une tradition en matière de protection des données personnelles opposée à l'Union européenne, ont conclu des accords de compromis avec l'Union européenne. La Directive n° 95/46 a d'une part permis une harmonisation des législations afin de permettre la circulation des données personnelles entre les États membres de l'Union européenne et d'autre part, posé les exigences relatives aux transferts de données personnelles vers des États tiers qui doivent assurer un niveau de protection « adéquat »[901] afin d'éviter que les données ne deviennent une marchandise qui s'échange, se vend ou s'appropri au détriment et sans respect de la personne et des droits qui l'accompagnent. Les transferts des données hors Union européenne sont par principe interdits sauf en présence d'une décision « d'adéquation » de la Commission européenne garantissant un niveau élevé de protection des données à caractère personnel. En l'absence de décision d'adéquation de la Commission, des instruments de droit privé peuvent être adoptés pour encadrer le transfert. Ainsi le responsable du traitement ou le sous-traitant peuvent prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Il est possible de souligner que jusqu'à la décision *Schrems*, les clauses « contractuelles type » et les « *binding corporate rules »* ont eu un rôle marginal dans le transfert des données vers des pays tiers. En effet le *Safe Harbor* était perçu comme un instrument sûr[902], cependant le manque d'effectivité dans les contrôles de la part de la *Federal Trade Commission* avait déjà fait l'objet de critiques par la Commission bien avant la décision de la Cour de justice[903]. Les limites des clauses contractuelles type sont dues à la rigidité de sa structure, ne pouvant pas être modifiées par les parties du contrat, de même, les « *binding corporate rules »* ont pour limite d'être applicables seulement entre sociétés du même groupe ne pouvant pas trouver application pour une entreprise tierce. La formalité de notification préalable à l'autorité de contrôle rendait l'instrument peu efficace en termes de rapidité de transfert des données. Toutefois, suite à la décision *Schrems,* ces instruments ont été redécouverts par les entreprises même si leurs limites restent indiscutables et que le flux massif de données transatlantiques a rendu nécessaire la conclusion d'un nouvel accord « *Privacy Shield »* qui, nonobstant les avancées, présente

---

901 Voy. art. 25 et 26 et cons. 56 à 58 de la directive n° 95/46. Ce niveau de protection adéquat peut prendre la forme d'une législation nationale ou de codes de conduite comme l'illustre l'accord conclu entre les États-Unis et l'Europe autour des Principes du « safe harbour ». Voy. en ce sens L. COUDRAY, *La protection des données personnelles dans l'Union* européenne, Thèse Paris II, 2005, sp. pp.732 et s.; J. FRAYSSINET, « Le transfert et la protection des données personnelles en provenance de l'Union européenne vers les États-Unis : l'accord dit "sphère de sécurité" ou "safe harbor" », *CCE*, 2001, n° 3, pp. 10 et s.

902 La FTC est intervenue 20 fois pour sanctionner la violation des accords *Safe Harbor* , et, en douze cas, il y eu une médiation sur le payement de sanctions avec les parties impliqués. De plus ces interventions de l'autorité américaine sont arrivées au cours du 2014 après les interventions de la Commission européenne, Voy. K. Bloom – K. Royal, Transferring Personal Data Out of the European Union. Consultable au https://www.acc.com/vl/public/ACCDocketArticle/upload/Transferring-Personal-Data-Out-of-the-European-Union-Which-Export-Solution-Fits-your-Needs.pdf.

903 Communication from the Commission to the European Parliament and the Council on the Functioning of the Safe Harbour from the Perspective of EU Citizens and Companies Established in the EU, COM(2013) 847 final, 27.11.2013; Communication from the Commission to the European Parliament and the Council, Restoring Trust in EU-US data flows, COM(2013) 846 final, 27.11.2013, et le Memorandum Restoring Trust in EU-US data flows – Frequently Asked Questions, MEMO/13/1059, 27.11.2013.

toujours des criticités[904]. Ainsi depuis le 1er août 2016, les entreprises américaines peuvent adhérer au bouclier de protection des données auprès du ministère américain du commerce, qui vérifie que leurs politiques sur la protection des données répondent aux conditions rigoureuses en la matière contenues dans le bouclier. Des raisons économiques et politiques ont induit la Commission Européenne et les États-Unis à une renégociation rapide de l'accord. Cependant, ce dernier a été finalisé sans l'implication directe des autorités de contrôle, la Commission n'ayant pas tenu compte de l'avis du G29 sur le niveau de protection offert par le pays tiers[905]. Le Symbole de la politique étrangère de l'Union européenne en matière de protection des données personnelles sont les affaires *Google Spain* et *Schrems*[906]. Dans l'affaire *Google Spain*, afin d'affirmer la souveraineté digitale de l'Union européenne, la Cour de justice interprète de manière très étendue l'art. 4 de la Directive 95/46 concernant le champ d'application territorial du droit de l'union européenne. Dans l'affaire *Schrems*, la Cour de justice confirme son rôle de gardienne constitutionnelle illustrant le débat qui a divisé l'Union Européenne et les États-Unis[907] depuis l'entrée en vigueur de la directive 95/46/CE et qui a déflagré dans la période 2013-2015 avec le scandale « Prism » à la suite des révélations d'Edward Snowden à propos des programmes de surveillance de masse de la part de l'Agence nationale de Sécurité américaine[908]. Ainsi à travers son raisonnement, la Cour de justice a appliqué la législation de

---

904 S.J. SHACKELFOR, « Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations », in Eton Hall J. of Diplomacy & Int'l Rel, 2016.

905 Article 29 Data Protection Working Party, Opinion 01/2016 on the EU – U.S. «*Privacy Shield*» draft adequacy decision, Brussels, 13 aprile 2016, disponible à l'adresse : http://ec.europa.eu/justice/data-protection/article-29/ documentation/opinion-recommendation/files/2016/wp238_en.pdf

906 S. CRESPI, « La tutela dei dati personali UE a seguito della sentenza Schrems », in *www.eurojus.it,* 2 novembre 2015, disponible à l'adresse :

907 Sur le different approche entre UE et États-Unis Voy. : F. BOHEM, *A Comparison between US and EU Data Protection Legislation for Law Enforcement Purposes*, Study for the LIBE Committee, PE 2015; M. SHWARTZ, J. SOLOVES, « Reconciling Personal Information in the United States and European Union », in California L. Rev., 2014, 877; F. BIGNAMI, G. RESTA, « Transatlantic Privacy Regulation: Conflict and Cooperation », in *LCP*, 2015, p.101 ss. Voy. Également F. BIGNAMI, *The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens*, Study for the LIBE Committee, PE 519.215, May 2015.

908 C. BOWDEN, *The U.S. Surveillance Programmes And Their Impact On EU Citizens' Fundamental Right*s, disponible à l'adresse : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf ; Voy. également, D. BIGO, *National Programs for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law.* (2013), disponible à l'adresse : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf. Le 27 novembre 2013, la Commission a adopté la communication au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire COM(2013) 847 final. Au point 7 de cette communication, la Commission a fait état de ce que «toutes les entreprises participant au programme PRISM (programme de collecte de renseignements à grande échelle, qui permettent aux autorités américaines d'avoir accès à des données stockées et traitées aux États Unis semblent être certifiées dans le cadre de la sphère de sécurité» et que celle ci «est donc devenue l'une des voies par lesquelles les autorités américaines du renseignement ont accès à la collecte des données à caractère personnel initialement traitées dans l'[Union]». À cet égard, la Commission a constaté, au point 7.1 de ladite communication, «qu'un certain nombre de bases juridiques prévues par la législation américaine permettent la collecte et le traitement à grande échelle des données à caractère personnel stockées ou traitées par des sociétés établies aux États Unis» et que «[c]es programmes étant à grande échelle, il est possible que les données transférées dans le cadre de la sphère de sécurité soient accessibles aux autorités américaines et traitées par celles ci au-delà de ce qui est strictement nécessaire et proportionné à la protection de la sécurité nationale, comme le prévoit l'exception énoncée dans la décision [2000/520]». a Commission a souligné que «ce sont principalement les ressortissants des États Unis et les personnes qui y résident légalement qui bénéficient des garanties prévues en droit américain» et qu'«il n'existe, en outre, aucune possibilité, que ce soit pour les personnes concernées de l'Union ou des États Unis, d'obtenir l'accès, la rectification ou la suppression de données ou d'exercer des voies de droit administratives ou judiciaires si, dans le cadre des programmes de surveillance des États Unis, des données à caractère

l'Union européenne à des situations de transfert des données qui autrement lui échapperaient[909]. Il est important de souligner que les révélations d'E. Snowden sur la collecte massive des données ont inversé la tendance de hiérarchisation entre sécurité et liberté dans un monde post 11 septembre[910]. Les États-Unis ont dû accepter cette politique étrangère de l'Union européenne en négociant immédiatement un nouvel accord de compromis, le « *Privacy Shield* »[911]. Or, le texte élaboré entre Union européenne et les États-Unis (*Privacy Shield*) n'est pas l'épilogue du « conflit transatlantique » car des observations et critiques ont déjà été exprimées par les autorités de contrôle[912] et l'entrée en vigueur du RGPD implique que « le niveau de protection adéquat » doit être réévalué à la lumière de l'élévation des standards de protection offerts par le nouveau texte normatif. Le Parlement a présenté une résolution, demandant à la Commission de revoir le *Privacy Shield* et le cas échéant le suspendre[913]. Au travers de son jugement *Google Spain*, la Cour a ouvert l'application du droit européen en matière de protection des données à des entités établies dans des États tiers, tels que les États-Unis en l'espèce, et disposant d'un établissement secondaire sur le sol européen, afin de rendre effectifs les droits consentis par la directive. Dans la mise-à-jour de son opinion 8/2010 relative au droit applicable[914], le G29 a interprété l'arrêt de la Cour comme permettant d'appliquer la directive à des sociétés établies en dehors de l'Union européenne, dont le modèle économique serait fondé sur l'offre de « services gratuits » sur le territoire de l'Union, et financées par le traitement de données à caractère personnel, à des fins de prospection par exemple.

---

personnel les concernant sont collectées et traitées ultérieurement». La Commission a conclu, à ce même point 8, que «l'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la sphère de sécurité transfèrent aux États Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États Unis».

909 M. NINO, *Terrorismo internazionale, privacy e protezione dei dati personali*, Napoli, 2012, p. 147-350 ; D. BIGO et al., *Open Season for Data Fishing in the Web: The Challenges of the US PRISM Programme for the EU, Policy Brief*, CEPS, Brussels, June 2013; Voy. également D. BIGO, *Mass Surveillance of Personal Data by EU Member States and its Compatibility with EU Law Pape*r, in Liberty and Security in Europe, CEPS, Brussels, November 2013.

910 S. PEERS, *Europe v Facebook: the beginning of the end for NSA spying on EU citizens* ?, EU Law analysis, 18 juin 2014. Disponible à l'adresse: http://eulawanalysis.blogspot.gr/2014/06/europe-v-facebook-beginning-of-end-for.html

911 Voy. Décision d'exécution (UE) 2016/1250 de la Commission du 12 juillet 2016 conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à l'adéquation de la protection assurée par le bouclier de protection des données UE-États-Unis [notifiée sous le numéro C(2016) 4176] (Texte présentant de l'intérêt pour l'EEE).

912 Voy. la lettre envoyé aux présidents du G29,Working Party et du Comité LIBE du Parlement européen, signé de la part de 27 associacions de défense des données personnelles plus rapresentatives en Europe: https://edri.org/transatlantic-coalition-of-civil- society-groups-privacy-shield-is-not-enough-renogitation-is-needed. Voy. également A. MANTELERO, *From Safe Harbour to Privacy Shield. The 'medieval' sovereignty on personal data*, in Contratto e Impr./Europa, 2016, disponible à l'adresse :https://www.researchgate.net/publication/303522873_From_Safe_Harbour_to_Privacy_Shield_The_Medieval_sovereignty_on_personal_data.

913 Voir le communiqué de presse du parlement européen du 21-07-2017, disponible à l'adresse : http://www.europarl.europa.eu/news/fr/press-room/20170720IPR80211/privacy-shield-deficiencies-still-remain-and-must-be-resolved-says-chair.

914 Groupe de travail « Article 29 » sur la protection des données, « Update of Opinion 8/2010 on applicable law in light of the CJEU judgement in *Google Spain* », 16 décembre 2015, 176/16/EN WP 179 update, p. 7. Voy. également F.H. CATE, C. KUNER, O. LYNSKEY, C. MILLARD et D.J.B. SVANTESSON, « When two worlds collide: the interface between competition law and data protection », *International Data Privacy Law*, 2014, p. 248.

CHAPITRE II. L'EXTRATERRITORIALITÉ DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CONTEXTE DE CRISE SÉCURITAIRE

122 La coopération en matière pénale. La collecte des données personnelles est essentielle au travail des autorités répressives et fait l'objet d'échanges entre l'Union européenne et les autorités des pays tiers. Les nouvelles technologies décuplent les capacités de surveillance et d'intrusion dans la vie privée des citoyens. Le risque est de vivre dans une société surveillée. Le cyber-espionnage remet en question la confiance des citoyens envers les gouvernements et constitue une grave atteinte aux droits fondamentaux, à la vie privée et aux libertés individuelles ou publiques. Toutefois, l'espionnage massif des données personnelles des citoyens dénoncé par l'ancien employé de la CIA Edward Snowden, aurait été justifié selon les autorités américaines par la lutte contre le terrorisme, notamment par le *Patriot Act* aux États-Unis. Toutefois, l'Union européenne condamne la surveillance massive. Les révélations d'E. Snowden sur le programme secret de surveillance des communications par l'Agence nationale de sécurité américaine («NSA») ont suscité un débat mondial sur la protection des données et le droit à la vie privée dans le lutte contre le terrorisme. Dans un rapport sévère publié en janvier 2014, la commission des libertés civiles du Parlement européen a accusé la NSA de violation systématique du droit à la vie privée des citoyens de l'UE et a appelé à une refonte profonde du cadre juridique transatlantique de la coopération dans le domaine de la lutte contre le terrorisme[915]. Ensuite, sous la pression des deux chambres du Congrès[916], le président Obama a présenté publiquement un nouveau plan pour la surveillance électronique du gouvernement américain, qui, tout en confirmant l'autorité accordée à la NSA[917], visait à apaiser les craintes de défenseurs des droits civiques et empêcher la consolidation d'un état de surveillance[918]. Un élément clé de la réforme proposée par le président Obama est la décision de supprimer du contrôle gouvernemental la rétention des métadonnées des communications électroniques en les transférant aux entreprises privées. Selon la proposition, le gouvernement américain ne conserverait plus d'informations sur la date, l'heure, la longueur et l'emplacement des appels téléphoniques ou des e-mails pour l'avenir des fins d'enquêtes antiterroristes. Ces données seraient plutôt traitées par les fournisseurs de télécommunications et mis à leur disposition par

[915] Voy. Comm. on Civil Liberties, Justice and Home Affairs, Draft Report on the US NSA Surveillance Programme, Surveillance Bodies in Various Member States and Their Impact on EU Citizens' Fundamental Rights and on Transatlantic Cooperation in Justice and Home Affairs, EUR. PARL. DOC., 17–19, 2013/2188(INI) (Jan. 8, 2014), available at http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-// EP//NONSGML%2BCOMPARL%2BPE-526.085%2B02%2BDOC%2BPDF%2BV0//EN, archived at http://perma.cc/KHA7-YNL2 (calling upon U.S. authorities to prohibit blanket mass surveillance activities and bulk processing of personal data).

[916] Voy. USA Freedom Act, H.R. 3361, 113th Cong. (2013), S. 1599, 113th Cong. (2013) (a bill jointly sponsored by U.S. Senator Patrick Leahy and U.S. Representative Jim Sensenbrenner purporting to end the program through which the NSA vacuums up the metadata generated in electronic communications).

[917] USA Patriot Act § 215, 50 U.S.C. § 1861 (2012) (regulating access to business records for foreign intelligence and international terrorism investigations).

[918] « The President's Review Group On Intelligence And Communications Technologies, Liberty And Security In A Changing World » (2013), available at http://www.white house.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf, archived at http://perma.cc/8FM4- QV77.

les autorités de sécurité et de répression basées uniquement sur des raisons justifiées [919]. Pourtant, le 8 avril 2014, quelques mois seulement après la proposition du président Obama, la Grande Chambre de la Cour de justice a franchi une étape fondamentale dans la protection des données, statuant que le régime juridique de l'UE pour la conservation des données, qui s'appuyait sur les sociétés privées traitant les métadonnées générées au cours de communications à des fins répressives, exactement comme prévu dans le plan Obama, avait violé le droit à la protection des données et à la vie privée consacré dans la Charte des droits fondamentaux de l'UE[920]. Ainsi la lutte contre le terrorisme et les formes graves de criminalité est un moyen pour étudier l'identité de l'Union européenne et sa politique étrangère en matière de protection des données personnelles. L'article 3 §2 du TFUE précise que « l'Union offre à ses citoyens un espace de liberté, de sécurité et de justice », le paragraphe 5 du même article, dispose : « l'Union affirme et promeut ses valeurs et ses intérêts et contribue à la protection de ses citoyens dans ses relations avec le reste du monde », ce qui implique une action externe de l'UE pour empêcher toute atteinte aux droits fondamentaux de ses citoyens lors du transfert des données vers des pays tiers[921].

Il a été souligné, à l'heure de la mondialisation, « il n'est plus de politique de l'Union qui n'ait une dimension externe. Il n'en va pas différemment pour l'Espace de liberté, de sécurité et de justice. (...) l'ELSJ ne peut se développer, comme espace sans frontières intérieures, qu'à la condition de pouvoir s'adosser (en quelque sorte à titre complémentaire, voire compensatoire) sur une dimension externe solidement établie »[922]. Avant le traité de Lisbonne plusieurs accords internationaux en matière de coopération pénale avaient été signés. Malgré l'absence de personnalité juridique de l'Union, c'est sur la combinaison des articles 24 (base légale pour conclure les traités internationaux en matière de PESC) et 38 de l'ex-TUE (base légale JAI)[923] que l'Union avait une sorte de titre de compétence externe *expresse*, distincte du principe de la compétence externe *implicite* qui prévalait au sein du pilier communautaire. Ces coopérations en matière pénale se sont d'ailleurs concentrées sur les aspects opérationnels et procéduraux de la coopération pénale (extradition, investigation, échange de données...) et non sur un rapprochement normatif[924]. Le Traité de Lisbonne a supprimé ces deux articles et a soumis

---

919 President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014) transcript available at http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-presi dent-review-signals-intelligence, archived at http://perma.cc/EJ7D-7CD2.

920 F. FABBRINI, *Fundamental right in Europe: Challenges and transformations in comparative perspective*, 2014, examining the European multilevel system for the protection of fundamental rights in comparison with the U.S. federal system.

921 E. P. COLE, « New challenges to the US Multinational Corporation in the European Economic Community », *Data Protection Laws*, in 17 N.Y.U J. INT'L L. & POL, 1995, p. 893.

922 H. LABAYLE, R. MEHDI, J.-S. BERGÉ « La dimension externe de l'espace de liberté, de sécurité et de justice », *RTDE*, 2014, p. 649. Voy. Également C. FLAESCH-MOUGIN, L. S. ROSSI (dir.), *La dimension extérieure de l'espace de liberté, de sécurité et de justice de l'Union européenne après le Traité de Lisbonne*, Bruylant, 2013, p. 113 et ss ; H. LABAYLE, « L'espace pénal européen et le monde : instrument ou objectif ? », *in* G. DE KERCHOVE et A. WEYEMBERGH (dir.), *Sécurité et justice : enjeu de la politique extérieure de l'Union européenne*, éd. De l'Université de Bruxelles, 2003, pp. 15-28.

923 Le Conseil européen de Tampere est souvent cité comme point de départ de l'action extérieure en matière pénale. Voy. M. CREMONA, « EU External Action in the JHA Domain : A Legal Perpective », *EUI Working Papers Law*, n°2008/24, pp. 1-31.

924 Pour aller plus loin dans l'étude des accords conclus en matière de coopération pénale voy. T. KONSTADINIDES, « EU Law and International Cooperation in Criminal Matters: A Tale of Legal Competence and Political Competency », *in* V.

l'action extérieure en matière pénale au cadre commun prévu par le TFUE. La politique externe en matière pénale de l'Union européenne (en matière de transfert de données personnelles lorsqu'elles sont utilisées à des fins répressives) est relativement récente. Le présent chapitre veut analyser la politique externe en matière pénale mise en place par l'Union européenne pour faire cohabiter sécurité publique et respect du droit fondamental à la protection des données personnelles. En effet, la sécurité intérieure de l'Union et la sécurité extérieure sont interdépendantes : l'Union européenne doit faire face à des menaces de tous types (terrorisme, crime organisé…) dont l'origine se situe loin de ses frontières et dont la gestion efficace suppose la mise en place de partenaires internationaux[925]. Ainsi, lorsque l'Union accepte de communiquer les données personnelles de ses citoyens dans le cadre de la lutte antiterroriste, elle concourt à assurer leur sécurité[926]. Il est possible de parler alors de dimension externe de l'Espace de liberté de sécurité et de justice qui relève de la politique étrangère de l'Union. Il paraît donc intéressant de se pencher sur les contraintes politiques et institutionnelles pesant sur l'élaboration d'accords entre l'Union européenne et les États tiers dans les relations externes. L'intervention de l'Union européenne pour assurer une protection « externe » sera analysée à travers l'affaire *Personal Name Record* (PNR), concernant le transfert de données des dossiers de passagers aériens vers les États-Unis afin de lutter contre le terrorisme et les formes graves de criminalité (section I) et à travers la mise en œuvre de la politique américaine anti-terroriste qui a mené l'Union européenne à conclure plusieurs accords « *Swift* »[927] avec les États-Unis finalisés aux transfert de données de messagerie financières dans la lutte contre le terrorisme (section II).

Ces deux accords « externes » concernent le transfert des données personnelles à des fins de sécurité et illustrent le difficile équilibre à atteindre entre lutte contre le terrorisme et protection des droits fondamentaux.

MITSILEGAS et a. (dir.) *Research Handbook on EU Criminal Law*, Edward Elgar Publishing, 2016, pp. 567-579 ; G. FOURNIER, « Coopération judiciaire de l'Union européenne en matière pénale : quelle contribution à un universalisme pénal ? », *in La dimension extérieure de l'espace de liberté, de sécurité et de justice de l'Union européenne après le Traité de Lisbonne*, Bruylant, 2013, pp. 457-486.

925 Voy. l'étude de N. CHICHE « Internet : Pour une gouvernance ouverte et équitable, étude du conseil économique, social et environnemental ». Disponible à l'adresse: https://www.lecese.fr/travaux-publies/internet-pour-une-gouvernance-ouverte-et-equitable. L'Internet devient une arme de pouvoir que de plus en plus de nations, d'entreprises ou de groupes - politiques ou religieux notamment - entendent pleinement utiliser pour asseoir leur puissance et modifier à leur profit les rapports de forces géopolitiques et économiques. Les exemples en la matière abondent de ce que l'on peut désormais considérer comme des formes nouvelles d'affrontement : le blocage des sites gouvernementaux de l'Estonie et de la Géorgie en 2007 et 2008, la destruction, en 2009/2010, dans le but de freiner le programme nucléaire de l'Iran, des systèmes de contrôles de centaines de centrifugeuses d'enrichissement de l'uranium par un virus sophistiqué « Stunex », le cyber-espionnage de programmes d'armement aux États-Unis en 2013, etc. Les câbles sous-marins qui constituent les principales dorsales du transport international de données sont eux aussi des cibles privilégiées pour l'espionnage numérique. L'ampleur et la sophistication des actes de cybercriminalité susceptibles, dans des scenarii apocalyptiques, de porter atteinte aux infrastructures vitales ou à des activités économiques ou militaires stratégiques risquent donc d'accentuer la vulnérabilité des États, des entreprises ou des autres organisations de la société civile.

926 Elle remplit les objectif prévu à l'article 67§3 TUE.

927 Voy. Décision Du Conseil du 13 juill. 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis aux fins du programme de surveillance du financement du terrorisme (2010/412/UE).

Section I. La politique étrangère de sécurité de l'Union européenne. La conclusion d'accords sur la surveillance des données de voyage « PNR »

123 Des approches opposées. Il est intéressant de souligner que le droit à la protection des données personnelles érigé à droit fondamental au sein de l'Union européenne, semble passer au second plan dans les systèmes juridiques d'États tiers comme aux États-Unis, où la priorité est donnée à la lutte contre le terrorisme et la sécurité publique. L'accord international conclu entre l'Union européenne et les États-Unis pour encadrer le transfert de données des passagers aériens, « *Passenger Name Records* » (ci-après « PNR ») à des fins de sécurité est l'exemple parfait de ces conceptions opposées. Cet accord a justifié la conclusion d'autres accords de la même nature entre l'Union européenne et d'autres États tiers mais qui paraissent plus équilibrés. Cela montre une marge de progrès dans le niveau de protection. Les données PNR sont recueillies par les transporteurs aériens au cours du processus de réservation de vol et comprennent, entre autres, les noms, adresses, détails de la carte de crédit et numéros de siège des passagers aériens. Les transporteurs aériens recueillent ces informations à leurs propres fins commerciales. L'UE a conclu des accords avec certains pays tiers (Australie, Canada et États-Unis) pour le transfert de données PNR afin de prévenir, détecter, enquêter et poursuivre des infractions terroristes ou des crimes transnationaux graves. En outre, l'Union a adopté la directive (UE) 2016/861[928] connue sous le nom de directive UE-PNR. Cette directive fournit un cadre juridique aux États membres de l'Union européenne pour le transfert des données PNR aux autorités compétentes d'autres pays tiers. En ce qui concerne les accords PNR entre l'Union européenne et les pays tiers, leur compatibilité avec les droits fondamentaux de la vie privée et de la protection des données consacrés dans la Charte des droits fondamentaux a été contestée. Lorsque, à la suite des négociations avec le Canada, l'UE a signé un accord sur le transfert et le traitement des données PNR en 2014, le Parlement européen a décidé de renvoyer l'affaire à la CJUE pour qu'elle évalue la légalité de l'accord avec le droit de l'UE, et en particulier avec les articles 7 et 8 de la Charte. Toutefois, suite aux attentats de Paris de janvier 2015[929] , l'adoption au niveau européen d'une directive PNR[930] montre la conviction de l'efficacité du dispositif PNR dans la lutte contre le terrorisme. Les accords PNR avec les États-Unis permettent l'étudier cette fois-ci le dialogue transatlantique en matière de sécurité (§1) et ses effets sur les autres négociations entre l'Union européenne et des pays tiers (§2).

928 Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime, OJ 2016 L 119.

929 Voy. Le communiqué du G29 du 5 février 2015, Déclaration sur la mise en place d'un système PNR européen.

930 Voy. la directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière, JO L 119 du 4/5/2016, p. 132-149 ; également l'avis rendu par la Cour relatif à l'accord PNR avec le Canada, CJUE, (Grande chambre), 26 juillet 2017, Avis 1/15 rendu en vertu de l'article 218, paragraphe 11, TFUE.

§1. Les accords « PNR » avec les États-Unis

124 Le fichier *Passenger Name Record* (PNR). Suite aux attaques terroristes du 11 septembre 2001, les États-Unis ont adopté une législation[931] imposant à l'ensemble des transporteurs aériens, assurant des liaisons au départ ou à destination des États-Unis, de communiquer les données contenues dans leurs systèmes de traitement des réservations des passagers aériens (PNR, *Passenger Name Record*)[932] au ministère américain de la Sécurité intérieure avant le départ des passagers. Les données PNR comprennent les noms, l'adresse, les informations sur la carte de crédit, numéros de sièges de passagers aériens et des renseignements additionnels quelconques comme des éventuels problèmes de santé, préférences alimentaires inspirées par motifs religieux etc.[933]. Ces renseignements peuvent se révéler particulièrement utiles pour lutter contre le terrorisme, mais peuvent porter atteinte aux données personnelles pour leur caractère sensible. Une fois collectées les informations, le CAPPS (*Computer Assisted Passenger Precreening System*) subdivisait, les voyageurs en deux groupes en séparant ceux pour lesquels était suffisant un contrôle de type général, ceux qui avaient besoin d'un *screening* plus approfondi et ceux pour lesquels il y avait une interdiction absolue d'embarquement. La législation américaine comportait des sanctions en cas de manquement de communication spontanée des données PNR de la part des compagnies aériennes au *Customs and Border Protection*. Les compagnies aériennes de presque tous les pays du monde se sont pliées à ces régulations du gouvernement américain et plusieurs États (si l'on pense à l'Australie, l'Angleterre, au Canada et à la Nouvelle Zélande), ont ensuite commencé à introduire dans leurs propres aéroports des systèmes de contrôle semblable au CAPPS. Les compagnies européennes qui refusaient de se soumettre, étaient menacées de se voir interdire l'atterrissage de leurs avions sur le sol américain[934]. Cette situation est à l'origine du contentieux entre les États-Unis et l'Union Européenne. Un accord entre l'Union européenne et les États-Unis a été alors élaboré afin de garantir un niveau adéquat de protection aux données personnelles transférées.

125 La contestation de l'absence de base légale pour la conclusion de l'accord. L'accord se fondait sur les décisions d'adéquation de la Commission prises sur la base de l'article 25§6 de la directive 95/46.

---

931 Voy. Aviation and Transportation security Act du 19 novembre 2001.

932 En 1996 la compagnie Northwest Airlines introduisait déjà sur les propres vols un Système Informatisé (CAPPS) pour surveiller les Voyageurs. Le CAPPS a été développé à travers une subvention fournie par le Federal Aviation Administration (FAA). Ce système devait comparer les données des voyageurs (PNR) Passenger name records, présents dans le Système de Réservation Informatisée de la compagnie aérienne avec ceux-là insérés dans une base de données contenant une no-fly list, une liste de personne considérés dangereux gérée par le FBI. Le système CAPPS a été fortement critiqué puisque n'a pas su empêcher l'attaque terroriste du 11 septembre 2001. Le gouvernement a réagi avec l'émanation d'une législation plus stricte avec le Transportation Security Act (»ATSA").

933 D. E. HASBROUCK, *What's in a Passenger Name Record (PNR)?*, disponible à l'adresse: http://hasbrouck.org/articles/PNR.html.

934 C. PATTON, *No man's land: the EU-US passenger name record agreement and what it means for the European Union's pillar structure,* in 40 George Washington International Law Review, 2008, p. 527.

Toutefois, cette base légale ne pouvait plus être maintenue en conséquence de l'arrêt d'annulation de la Cour de justice en 2006 pour défaut de base légale[935] puisque les législations américaines comme le « *Patriot Act* » ont révélé la possibilité que des données transférées aux États-Unis (pour des raisons commerciales) [936] soient appréhendées par les autorités américaines pour des finalités ultérieures et notamment pour des exigences de sécurité nationale. Ainsi le premier accord conclu en 2004 a été invalidé par la Cour de justice[937], et un nouvel accord a été négocié de manière provisoire à partir de 2007, puis rejeté par le Parlement européen en mai 2010 (A). De nouvelles négociations ont alors été menées entre l'UE et les États-Unis aboutissant à la conclusion d'un nouvel accord en 2012[938] (B).

A. L'invalidation de la « décision d'adéquation » de la Commission par la Cour de justice

126 Le raisonnement de la Cour de justice. Depuis juin 2001 la Commission Européenne, tout en reconnaissant la légitimité des intérêts de sûreté publique américaine, informait les autorités américaines du fait que les nouvelles dispositions en matière de transfert des données PNR étaient contraires à la législation communautaire et avec celle des États membres en matière de protection des données personnelles [939] . En février 2003, la Commission et la *Custom Border Protection* (ci-après CBP) arrêtaient une déclaration jointe grâce à laquelle la Commission aurait autorisé les compagnies aériennes européennes à transférer les données PNR au CBP [940] . À la déclaration était jointe un document prévoyant les engagements « *undertakings* »[941], assumés par le CBP, en vue de l'adoption de la part de la Commission, sur

---

935 CJCE, C-317/04 et C-318/04, 30 mai 2006. Par sa requête dans l'affaire C-317/04, le Parlement européen demande l'annulation de la décision 2004/496/CE du Conseil, du 17 mai 2004, concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure (JO L 183, p. 83 et rectificatif JO 2005, L 255, p. 168). Par sa requête dans l'affaire C-318/04, le Parlement demande l'annulation de la décision 2004/535/CE de la Commission, du 14 mai 2004, relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique (JO L 235, p. 11, ci-après la «décision d'adéquation»).

936 Le considérant 102 du RGPD prévoit le présent règlement s'entend sans préjudice des accords internationaux conclus entre l'Union et les pays tiers en vue de réglementer le transfert des données à caractère personnel, y compris les garanties appropriées au bénéfice des personnes concernées. Les États membres peuvent conclure des accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales dans la mesure où ces accords n'affectent pas le présent règlement ou toute autre disposition du droit de l'Union et prévoient un niveau approprié de protection des droits fondamentaux des personnes concernées.

937 Voy. l'arrêt de la Cour de justice du 30 mai 2006, aff. C-314/04 et C-318/04, Parlement européen c. Conseil et Commission.

938 Voy. l'Adoption en séance plénière le 19 avril 2012.

939 Communication de la Commission au Conseil et au Parlament concernant le tranfert des données PNR: »A Global EU Approach". http://ec.europa.eu/justice/policies/privacy/docs/adequacy/apis-communication/apis_en.pdf.

940 Voy. Joint statement approuvé à Bruxelles le 17 et il 18 février 2003.

941 Ces engagements comprennent 48 points, qui sont regroupés sous les titres suivants: «Fondement juridique du droit d'obtention des PNR»; «Utilisation des données de PNR par le CBP»; «Exigences relatives aux données»; «Traitement des données 'sensibles'»; «Méthode d'accès aux données de PNR»; «Stockage des données de PNR»; «Sécurité des systèmes

la base de l'art. 25, § 6, de la Directive 95/46, d'une décision sur l'adéquation du traitement des données effectué par le ministère de la Sécurité intérieure des États-Unis (Département of Homeland Security United States, ci-après DHS) « paquet PNR »[942] adopté le 14 mai 2004[943] et ayant donné lieu parallèlement à une décision du Conseil de l'UE du 17 mai 2004[944] approuvant la conclusion d'un accord entre la Communauté européenne et les États-Unis[945]. Cette négociation n'a pas été facile puisque la protection des données, érigée en droit fondamental au sein de l'Union européenne passait au second plan aux États-Unis, donnant priorité à la lutte contre le terrorisme[946]. Toutefois, quelques exigences de garantie fortement voulues par la Commission européenne ont été insérées dans les « *undertakings* » comme la réduction du nombre de données collectées, l'exclusion dans la liste PNR des données sensibles qui pouvaient permettre l'identification d'un voyageur sur la base de sa religion. Cependant, les concessions américaines sont demeurées insuffisantes, ainsi le numéro des données collectées est passé de 38 à 34. Le G29 a était saisi pour donner son avis à deux reprises, le 13 juin 2003[947] et le 29 janvier 2004 et il a exprimé de sérieux doutes sur le niveau de protection des données garanti par lesdits engagements. Les critiques du G29 concernaient notamment la finalité du transfert considéré comme incompatible avec la finalité commerciale originaire de leur récolte de la part des compagnies ou des agences de voyage, le défaut de proportionnalité des données transférées, ce transfert ne pouvait pas se justifier à la lumière des exceptions dont l'art. 26 de la directive 95/46 puisqu'il ne s'agissait pas d'un transfert exceptionnel mais systématique. D'autres critiques concernaient la durée de conservation et la méthode américaine « *pull* » impliquant un libre accès des autorités américaines au lieu d'une méthode « *push* » impliquant que les données pouvaient être envoyées aux autorités américaines sur leur demande dûment justifiée. Même le Parlement a exprimé des critiques en adoptant une

informatiques du CBP»; «Traitement et protection des données de PNR par le CBP»; «Transmission de données de PNR à d'autres autorités gouvernementales»; «Information, accès aux données et voies de recours pour les personnes concernées par les PNR»; «Respect des dispositions»; «Réciprocité»; «Révision et durée de validité de la déclaration d'engagement», et «Absence de création de droits ou de précédent». Voy. sur ce point l'avis du G29, Opinion 2/2004 on the Adequate Protection of Personal Data Contained in the PNR of Air Passengers to Be transferred to the United States' Bureau of Customs and Border Protection (US CBP)Adopted on 29 January 2004 consultabile su http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp87_en.pdf.

942 Décision du Conseil 2004/496/EC du 17 mai 2004 concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure et décision de la Commission 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique.

943 Décision de la Commission 2004/535/CE du 14 mai 2004 relative au niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens transférés au Bureau des douanes et de la protection des frontières des États-Unis d'Amérique. JO L 235 6 juillet 2004 p. 11-12.

944 Décision du Conseil 2004/496/EC du 17 mai 2004 concernant la conclusion d'un accord entre la Communauté européenne et les États-Unis d'Amérique sur le traitement et le transfert de données PNR par des transporteurs aériens au bureau des douanes et de la protection des frontières du ministère américain de la sécurité intérieure. JO 2005, L255, p. 168.

945 S. CLAVET, « Les consequences de l'accord PNR sur la protection des droits fondamentaux en Europe », *Droits fondamentaux*, n°8, 2010, p. 28.

946 A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États Unis. Entre souci de protection et volonté de coopération », *Revue trimestrielle de droit européen*, 2006 p.423.

947 Voy. l'Avis du G29, 4/2003 et l'Avis 2/2004, 29 january 2004.

résolution le 13 mars 2003[948]. Il estimait que la décision d'adéquation excédait les compétences conférées à la Commission par l'article 25 de la directive 95/46 et appelait la Commission à lui soumettre un nouveau projet de décision se réservant le droit de saisir la Cour de justice afin de vérifier la légalité de l'accord international pris sur la base de la décision d'adéquation de la Commission. Ainsi le Parlement a demandé l'avis de la Cour de justice[949] afin de savoir si l'accord violait les dispositions de la Directive 95/46[950]. Toutefois, la Commission ne tenant pas compte de l'avis du G29 ni de la résolution du Parlement (à l'époque l'avis du Parlement n'était pas nécessaire)[951], concluait l'accord PNR avec les États-Unis le 28 mai 2004[952]. Ainsi le Parlement retirait la demande d'avis de la Cour de justice et saisissait la Cour de justice de deux requêtes[953]. Dans l'affaire C-317/04 le Parlement demandait l'annulation de la décision n° 2004/496/CE du Conseil du 17 mai 2004 concernant la conclusion de l'accord PNR[954] et dans l'affaire C-318/04, le Parlement demandait d'annuler la décision 2004/535/CE du 14 mai 2004 de la Commission, concernant le niveau « adéquat de protection » des données transférées vers les États-Unis[955]. De plus, le Parlement avait demandé la procédure d'urgence, sur la base de l'art. 62 du règlement de procédure de la Cour de justice. Toutefois, sa demande avait été rejetée[956]. En revanche, considérant la connexion entre les affaires, elles ont été réunies[957]. Le 30 mai 2006, deux ans après la conclusion de l'accord PNR, la Cour de justice rendait sa décision[958]. Concernant l'affaire C-318/04 sur l'annulation de la décision d'adéquation de la Commission, le Parlement a invoqué quatre moyens d'annulation, tirés respectivement d'un

948 Voy. Résolution du Parlement 13 mars 2003 on transfer of personal data by airlines in the case of transatlantichttp://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B5-2003-0411+0+DOC+XML+V0//EN&language=ga.

949 Voy. Avis n° 1/04, 30 avril 2004.

950 Voy. l'article publié sur le N.Y Times de P. Meller, *Europe Asks Court to Rule on Air Security Pact*, 22 avril 2004.

951 Voy. l'article : EU-US PNR: « Council to ignore Parliament and go ahead with "deal" » disponible à l'adresse : http://www.statewatch.org/news/2004/may/06eu-us-nr-deal.htm.

952 Voy. le communiqué de presse : » European Commission External Relations, International Agreement on Passenger Name Records (PNR) Enters Into Force » (May 28, 2004), disponible à l'adresse : http://ec.europa.eu/comm/external_relations/us/news/ip04_694.htm.

953 Voy. l'arrêt de la Cour de justice du 30 mai 2006, aff. C-314/04 et C-318/04, Parlement européen c/ Conseil et Commission concernant le défaut de base juridique adéquate.

954 Voy.. JO, n° L 183, 20 maggio 2004, p. 83-85.

955 Voy., JO, n° L 235, 6 luglio 2004, p. 11-22. Pour la première fois le CEDP participait à une affaire devant la CJ pour soutenir la thèse du Parlement. Parallèlement, dans l'affaire C-318/04, le Royaume-Uni a été admis avec ordonnance du Président pour soutenir la Commission.

956 F. MARIATTE, « Rejet par la Cour des demandes de traitement accéléré des recours dans le dossier du transfert des données PNR », in *Revue Europe* n° 12, Décembre 2004, p 400.

957 Selon l'art. 43 du règlement de procédure de la Cour.

958 E. PEDILARCO, « Protezione dei dati personali: la Corte di giustizia annulla l'accordo Unione europea-Stati Uniti sul trasferimento dei dati dei passeggeri aerei », *Diritto pubblico comparato ed europeo* 2006 p.1225-1231. Voy. également P. De HERT, « Sur les données des dossiers passagers, la directive "vie privée" 95/46/CE et la non-adéquation de la législation européenne », *Revue européenne de droit de la consommation* 2007 p.223-242 ; E. PAHALAWAN-SENTIHES, « Coup d'arrêt aux transferts de données sur les passagers en partance pour les États-Unis », *Recueil Dalloz* 2006 IR. p.1560-1561 ; G. TIBERI, « L 'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia », *Quaderni costituzionali*, 2006 p.824-829.

excès de pouvoir, d'une violation des principes essentiels de la directive, d'une violation des droits fondamentaux et d'une violation du principe de proportionnalité. La Cour de justice a observé que l'art. 3 par. 2 de la Directive 95/46/CE excluait de son champ d'application le traitement de données à caractère personnel mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du Traité sur l'Union européenne, et, en tout état de cause, les traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État et les activités de l'État relatives à des domaines du droit pénal. La Cour de justice relève que, bien que les données PNR soient initialement collectées par les compagnies aériennes dans le cadre d'une activité qui relève du droit communautaire, à savoir la vente d'un billet d'avion qui donne droit à une prestation de services, le traitement des données qui est pris en compte dans la décision d'adéquation possède une nature tout autre[959], à savoir la lutte contre le terrorisme. Par conséquent, sans qu'il soit nécessaire d'examiner les autres moyens invoqués par le Parlement, la Cour annule la décision d'adéquation 2004/535 du 14 mai 2004 puisqu'elle ne pouvait pas se fonder sur la directive 95/46. Ainsi la Cour de justice suivant le raisonnement de l'Avocat général, selon lequel « le fait que les données PNR ont été collectées par des opérateurs privés à des fins commerciales et que ce sont ces derniers qui organisent leur transfert vers un États tiers dans un cadre institué par les pouvoirs publics et visant la sécurité publique ne peut pas se fonder sur la directive 95/46 et la Commission ne disposait pas, en vertu de l'article 25 de la directive n° 95/46, du pouvoir d'adopter une décision relative au niveau de protection adéquat de données à caractère personnel transférées dans le cadre et en vue d'un traitement exclu expressément du champ d'application de ladite directive »[960]. Concernant l'affaire C-317/04, le Parlement a avancé différents moyens d'annulation, tirés du choix erroné de l'article 95 CE comme base juridique de la décision 2004/496 et de la violation, respectivement, de l'article 300, paragraphe 3, deuxième alinéa, CE, de l'article 8 de la CEDH, du principe de proportionnalité, de l'exigence de motivation et du principe de coopération loyale. Le Parlement estimait que l'article 95 CE ne constituait pas, pour la décision 2004/496, une base juridique appropriée. La Cour de justice reprend ce raisonnement indiquant que la décision 2004/496 n'avait pas pour but l'établissement et le fonctionnement du marché intérieur mais avait pour finalité de légaliser le traitement de données à caractère personnel prescrit par la législation des États-Unis pour une finalité de lutte contre le terrorisme et de poursuite, d'enquête de la criminalité grave [961]. L'article 95 CE ne serait pas susceptible de fonder la compétence de la Communauté pour conclure un tel accord, puisque celui-ci vise des traitements de données exclus du champ d'application de la directive [962]. Ainsi la Cour de justice pour le même motif tiré de

---

959 En effet, cette décision, ne vise pas un traitement de données nécessaire à la réalisation d'une prestation de services, mais est considéré comme nécessaire pour sauvegarder la sécurité publique et à des fins répressives. Le transfert des données constitue un traitement ayant pour objet la sécurité publique et les activités de l'É tat relatives aux domaines du droit pénal et n'entre donc pas dans le champ d'application de la directive sur la protection des données personnelles.

960 Voy. les Conclusions de l'Avocat Général Philippe Léger aff.C-317/04 e tC-318/04 du 22.11.2005 § 73.

961 H. HIJIMANS, *Le troisième pilier dans la pratique : composer avec les faiblesses. L'échange d'informations entre les États membres*, Avis préalable en vue de la réunion de l'Association néerlandaise pour le droit européen, 7 février 2007, p.22.

962 CJUE, aff. jointes C-317/04 et C-318/04, Parlement européen c. Conseil de l'UE, 30 Mai 2006, para. 57, 58 et 59, dans lequel la Cour a statué que la décision d'adéquation et l'accord relatif au traitement des données sont exclus du champ d'application de la directive. La Cour de justice des Communautés européennes, réunie en grande chambre, a tranché un point de droit longuement débattu au sein des instances de l'Union européenne sur la base juridique des instruments de

l'incompétence au regard du Traité CE, annule la décision du Conseil[963] . Ce n'est pas la première fois que la Cour de justice se prononce sur le champ d'application *rationne materiae* de la Directive 95/46, à cet égard la Cour de justice dans son raisonnement rappelle l'affaire *Lindqvist*[964], en rappelant que l'art. 3 par. 2 de la directive 95/46 a un caractère purement exemplaire des traitements exclus du champ d'application. La Cour souligne que la finalité du traitement l'emporte sur la nature et l'origine des données[965], peu importe que les données soient collectées par les compagnies aériennes puisque la finalité de leur traitement est celle de lutte contre le terrorisme[966]. Il y a lieu de souligner que la Cour de justice, consciente des implications et obligations de la Communauté au niveau international et en raison du fait que l'accord cesse d'être applicable 90 jours après sa dénonciation, a imparti un délai expirant le 30 septembre 2006[967] afin de laisser le temps suffisant à la conclusion d'un nouvel accord entre l'Union européenne et les États-Unis, qui a vu le jour le 26 juillet 2007 pour une durée de sept ans. Toutefois, ce nouvel accord présentait plusieurs défauts[968] et il a été remplacé par un nouvel accord le 25 avril 2012[969]. Il a été observé que l'affaire PNR souligne les difficultés liées à l'ancienne division en pilier[970]. De plus, l'affaire présente beaucoup d'intérêt sous le profil de

rapprochement du droit pénal intervenant dans les matières communautaires. Un débat récurrent opposait jusqu'à présent la Commission européenne et les États membres sur le point de savoir si, lorsqu'un texte procède à une harmonisation des législations pénales nationales pour atteindre un objectif sectoriel précis pour lequel la Communauté dispose d'une compétence, la base juridique de ces dispositions pénales relève du « troisième pilier », relatif à la coopération policière et judiciaire pénale, en raison de leur contenu pénal, ou bien du « premier pilier », en raison de leur objectif sectoriel.

963 Voy. point 56-58 de l'arrêt.

964 Voy. point 52 de l'arrêt: « Il ne ferait pas de doute que le traitement des données PNR après le transfert à l'autorité américaine visée par la décision d'adéquation est effectué, et le sera, pour l'exercice d'activités propres aux États au sens du point 43 de l'arrêt du 6 novembre 2003, Lindqvist C-101/01 ».

965 F. FONTANELLI, *La Corte di Giustizia e il « Favor Communitatis". Il percorso della giurisprudenza della Corte di Giustizia delle Comunità Europee sul fondamento normativo degli atti della Comunità e dell'Unione*, in *Rivista Italiana di Diritto Pubblico Comunitario*, 2010, 1 p. 183 et s.

966 Les facteurs objectifs à prendre en compte pour choisir la base juridique comprennent notamment le but et le contenu de l'acte (Voy. Affaire C-491/01, British American Tobacco, en particulier les points 92 et 93). Si l'examen d'un acte de l'UE démontre qu'il poursuit une double finalité ou qu'il a une double composante et si l'une de celles-ci est identifiable comme principale ou prépondérante, tandis que l'autre n'est qu'accessoire, l'acte doit être fondé sur une seule base juridique, à savoir celle exigée par la finalité ou composante principale ou prépondérante (Voy. Affaire C-42/97, Parlement contre Conseil, points 39 et 40). À titre exceptionnel, s'il est établi que l'acte poursuit à la fois plusieurs objectifs, qui sont liés d'une façon indissociable, sans que l'un soit second et indirect par rapport à l'autre, un tel acte devra être fondé sur les différentes bases juridiques correspondantes (Voy. à cet égard l'affaire C-491/01, British American Tobacco, points 92 et 93, et l'affaire C-42/97, Parlement contre Conseil, point 38).

967 Cette lacune, résultant de la construction en pilier a été comblé par l'adoption de la décision-cadre du Conseil 2008/977/JAI du 27 décembre 2008 relative à la protection des données personnelles dans le cadre du troisième pilier, dont l'art. 15 exige que le transfert de ces données personnelles vers des États tiers ne puissent avoir lieu qu'à condition que ces derniers offrent une protection adéquate.

968 Notamment la liste des données et des destinataires pouvant y accéder étant augmentée, la durée de conservation allongée, l'accès aux données sensibles étant possible et le délai de conservation étant étendu à 15 ans minimum ainsi que le nombre trop important des dérogations admises.

969 Décision 2012/472/UE du Conseil du 26 avril 2012 relative à la conclusion de l'accord entre les États- Unis d'Amérique et l'Union européenne sur l'utilisation des données des dossiers passagers et leur transfert au ministère américain de la sécurité intérieure, JO 2012 L 215/4. Le texte de l'accord est joint à cette décision, JO 2012 L 215, p. 5–14.

970 L. SBOLCI, *Conflitti tra Istituzioni dell'Unione Europea e Accordi Interistituzionali*, in Rivista di Diritto Internazionale, 2007, p. 345 ; M. G. GARBAGNATI KETVEL, *La giurisprudenza della Corte comunitaria in materia penale: verso un ravvicinamento tra i pilastri dell'Unione Europea*, in *Diritto dell'Unione Europea*, 2007, 2 p. 399. Sous l'aspect de la base

la tradition juridique de l'Union européenne par rapport aux États-Unis en matière de droit à la protection des données personnelles. Il faut remarquer que la décision a été critiquée notamment pour avoir annulé l'accord sans trancher sur la question de savoir quelle aurait été la base juridique appropriée[971]. De plus, la Cour de justice n'a pas saisi l'occasion pour statuer sur la portée et de la dimension externe du droit à la protection des données personnelles, comme demandé par le Parlement. Il s'agit d'un arrêt qui est motif de frustration pour ce qui a été omis[972]. La conséquence de ce manque de clarté a ouvert la voie à une nouvelle négociation entre Union européenne et États-Unis, cette fois-ci ayant comme base juridique celle de l'ancien troisième pilier qui offre notamment des garanties moins efficaces par rapport à l'ex-premier pilier.

B. L'élaboration d'un nouvel accord PNR avec les États-Unis

127 Le conflit transatlantique. En juin 2006, la Commission, en réponse au jugement de la Cour de justice, a demandé au Conseil l'autorisation d'ouvrir des négociations visant à la conclusion d'un nouvel accord avec les États-Unis sur les transferts de données PNR sur la base de l'article 38 du Traité, puisque le troisième pilier a été présenté comme le seul cadre juridique approprié pour conclure un accord international sur les questions de sécurité publique et le droit pénal[973]. Ainsi un nouvel accord a été appliqué de manière provisoire à partir d'octobre 2006 avec une échéance au 31 juillet 2007[974]. Ce nouvel accord provisoire présentait les mêmes

juridique, cette décision a réveillé l'attention pour les conséquences possibles sur l'affaire mettant en cause la base juridique de la directive 2006/24/CE du Conseil et du Parlement Européen "concernant la conservation de données générales ou traité dans le cadre de la fourniture de services de communication". Dans cette affaire L'Irlande, soutenue par la Slovaquie, il avait saisi la CJ pour annulation contre cette directive, puisqu'elle ne visait pas à améliorer le fonctionnement du marché intérieur mais à favoriser la récolte de données exclusivement pour buts de sûreté publique et lutte au terrorisme. Avec grande surprise, la CJ ne suit pas le raisonnement de l'affaire PNR et statue sur la légitimité de base légale de l'art. 95 TCE.; Toutefois la directive 2006/24 a fait l'objet d'un affaire, tranché le 8 avril 2014 rendant invalide la directive sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications. Certes, les PNR ne sont pas ici directement concernés mais l'avis de la Cour sur la collecte massive de données est connu, la Cour a pu préciser par ailleurs dans son arrêt que « ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. ». La Cour soulève également qu'en termes de conservation de données, le législateur a excédé les limites qu'impose le respect du principe de proportionnalité.

971 Voy. l'avis du CEDP on the final report by the EU US High Level Contact Group on Information Sharing and Privacy and Personal Data protection § 22, www.edps.europa.eu.

972 V. MICHEL, « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration, note sous l'arrêt su 30 mai 2006, Parlement européen c. Conseil, aff. jtes C-317 et 318/04 », *Revue Trimestrielle Droit Européen*, 3/2006, p.535.

973 F. MARIATTE, « Transfert des données PNR et protection des données personnelles », *Europe n°* 12, Décembre 2006, comm. 359.

974 Voy. Press release US, Dept. of Homeland Security, Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Agreement with European Union (Oct. 6, 2006), available at

problèmes que le précèdent annulé par la Cour de justice, il se basait notamment toujours sur un système « *pull* »[975]. Par la suite, en juin 2007, un mois avant que l'accord temporaire expire, la Commission européenne et les États-Unis commençaient à négocier un accord définitif[976] et arrivent à la signature de l'accord le 23 juillet 2007 à Bruxelles et le 26 juillet 2007 à Washington avec échéance en juillet 2012. En vertu de l'accord définitif, les compagnies aériennes européennes devaient communiquer aux autorités américaines 19 types de données PNR. L'accord privilégiait un système « *push* » toutefois les autorités américaines avaient toujours le droit d'accéder directement aux systèmes de réservation des compagnies sur la base du mécanisme « *pull* » prévu dans le premier accord[977] . Finalement, le nouvel accord n'a attribué aucune marge d'appréciation aux entreprises dans la décision sur le type de données transférées, ni sur la durée et conditions de transfert. Cette situation a provoqué les critiques du président du CEDP, Peter Hustinx qui a observé : « *There is no limitation to what U.S. authorities are allowed to do with "the data" and "the absence of a robust legal mechanism that enables EU citizens to challenge the misuse of their personal information*" »[978]. De plus, la durée de conservation était de trois ans et demi selon l'accord PNR de 2004 et dans l'accord PNR de 2007 avait été augmenté à quinze ans. Enfin, aucune garantie n'a été fournie sur l'effacement des données inutiles ou non traitées[979]. L'accord a pris fin en 2012 et de nouvelles négociations ont alors eu lieu entre l'Union européenne et les États-Unis aboutissant à la conclusion d'un nouvel accord soumis à l'approbation du Parlement européen et entériné en avril 2012[980]. Entre temps, l'évènement majeur a été l'entrée en vigueur du traité de Lisbonne établissant un rôle plus accru du Parlement européen dans la procédure de conclusion d'accords internationaux avec un pouvoir de veto prévu à l'article 218 TFUE en ce qui concerne les accords internationaux dans les domaines rentrant dans la procédure législative ordinaire, y compris la conclusion d'accords en matière pénale (ex-troisième pilier). Ainsi le Parlement aurait pu exercer son contrôle démocratique, étant sur le même plan que le Conseil. Toutefois, nonobstant les critiques, le texte a été approuvé[981] en raison des considérations politiques et diplomatiques qui ont pris le pas sur les exigences de protection plus strictes de l'Union

---

http://www.dhs.gov/xnews/releases/pr_1160772588688.shtm; EU Further Loosens Data Protection and Privacy Rules to Fight Terrorism, INTERNET BUS. L. SERVS., Nov. 20, 2006.

975 Voy. Ad Interim Agreement Between the European Union and the United States Regarding the Transfer of Passenger Name Record Data, 72 Fed. Reg. 348 (Jan. 4, 2007).

976 Voy. U.S. Dept. of Homeland Security, « Statement by Homeland Security Secretary Michael Chertoff on Passenger Name Record Data », (5 luglio 2007), consultabile su http://www.dhs.gov/xnews/releases/pr_1183667401959.shtm.

977 F. MARIATTE, « Conclusion du nouvel accord UE/USA sur le transfert des données PNR », *Europe* n° 10, Octobre 2007, comm. 247.

978 Voy. la lettre de P. HUSTINX, *European Data Protection Supervisor, to Wolfgang Schauble, Minister for the Interior, 27 june* 2007, disponible à l'adresse: http://epic.org/privacy/pdf/hustinx-letter.pdf.

979 Déjà dans l'affaire Leander (CEDH, Leander c. Svezia, 26 mars 1987 §§ 19-22), la Cour de Strasbourg avait établi que la collecte et la transmission de renseignements personnels par les pouvoirs publics était en soi une ingérence conformément à l'art.

980 Commission des libertés civiles du parlement européen a donné son feu vert le 3 avril 2012. L'adoption en séance plénière a eu lieu le 19 avril 2012, par 409 voix contre 226.

981 L. GRARD, « Nouvelle actualité des accords PNR. - Sûreté du transport aérien contre sécurité juridique », *Revue de droit des transports* n° 3, Juillet 2012, repère 3.

européenne. Cela illustre le difficile dialogue transatlantique et la difficulté de l'équilibre à trouver entre lutte contre le terrorisme et protection des droits fondamentaux. Cependant, le nouvel accord de 2012 apporte des améliorations significatives. Il restreint les finalités pour lesquelles les informations peuvent être utilisées, telles que les formes graves de criminalité transnationale et le terrorisme et il établit la période pendant laquelle les données PNR peuvent être enregistrées : ainsi, toutes les données doivent être rendues anonymes à l'issue d'un délai de six mois. De plus, les personnes concernées ont un droit de recours administratif et judiciaire conformément au droit américain. Tout individu a également le droit d'accéder à ses propres données PNR et d'obtenir leur rectification par le ministère américain de la Sécurité intérieure, y compris la possibilité d'effacement si les informations sont incorrectes. L'accord, qui a pris effet le 1er juillet 2012, restera en vigueur pendant sept ans, jusqu'en 2019. Cependant, son adoption n'a pas mis fin aux critiques concernant l'insuffisance des garanties, en particulier la preuve que le stockage et le traitement des données PNR sont réellement nécessaires et proportionnées.

§2. Des conséquences sur le plan des autres négociations

128 Les données PNR considérées comme instrument nécessaire au travail des autorités répressives. Suite aux attentats du 11 septembre 2001, de Madrid en 2004 et de Londres en 2005, les États-Unis ont voulu adopter des lois sécuritaires basées sur le système du *Passenger Name Record*. L'Australie et le Canada ont voulu faire de même. Ainsi l'Union européenne a conclu des accords similaires avec l'Australie [982] et le Canada [983] . Les accords ont été définitivement adoptés en 2011 avec l'Australie, tandis que pour le Canada il s'agit d'un projet d'accord de 2014 qui a fait l'objet d'une critique par l'avocat général Mengozzi et confirmé par l'avis négatif de la Cour de justice. Ces évolutions témoignent que l'utilisation des données PNR est de plus en plus considérée comme un aspect nécessaire au travail des services répressifs. Or ce traitement de données à caractère personnel soulève d'importantes questions quant au respect de deux droits fondamentaux et la protection de la vie privée. En Europe, les droits fondamentaux au respect de la vie privée et à la protection des données à caractère personnel sont consacrés par l'article 8 de la Convention européenne des droits de l'homme (CEDH) et par les articles 7 et 8 de la Charte des droits fondamentaux de l'Union européenne. Ainsi toute limitation de l'exercice des droits et libertés reconnus par la Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. Compte tenu du fait que les régimes de protection des données dans les pays tiers peuvent différer de ceux qui sont en vigueur dans l'Union européenne, il est

982 Voy. JO L 213, 8.8.2008 p. 49.

983 Voy. JO L 91, 29.3.2006, p. 53, OJ L 91, 29.3.2006, p. 49 et JO L 82, 21.3.2006, p. 15.

important que pour tout transfert de données PNR en provenance d'États membres de l'Union européenne vers des pays tiers, ces derniers assurent un niveau adéquat de protection des données reposant sur une base juridique solide. En décembre 2011, le Conseil a approuvé la conclusion d'un nouvel accord entre l'Union européenne et l'Australie concernant le traitement et le transfert de données PNR[984] (A). Cet accord constitue une nouvelle étape du programme de l'Union européenne qui comprend des lignes directrices globales en matière de PNR[985]. Toutefois, la négociation d'un accord PNR avec le Canada[986] n'a toujours pas abouti à cause de l'avis négatif de la Cour de justice (B).

A. L'accord PNR avec l'Australie

129 Un accord « équilibré ». Le premier accord concernant ce type de données entre l'Union européenne et l'Australie a été signé en 2008. Il a ensuite été remplacé par un accord, signé en octobre 2011, qui est entré en vigueur au 1er juin 2012[987]. Ce nouvel accord renforce le cadre légal et juridique pour le transfert de données entre l'Union européenne et l'Australie [988]. L'accord restreint les finalités et prévoit notamment que les données peuvent être « conservées seulement pour la prévention et la détection d'infractions terroristes ou de formes graves de

---

984 Voy. Décision 2012/981/UE du Conseil du 13 décembre 2011 relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, JO 2012 L 186/3. Le texte de l'accord, qui remplace un précédent accord de 2008, est joint à cette décision, JO 2012 L 186, p. 4–16.

985 Voy. notamment la Communication de la Commission du 21 septembre 2010 relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, COM(2010) 492 final, Bruxelles, 21 septembre 2010 selon lequel les principes de base que le pays tiers demandeur devrait respecter en matière de protection des données à caractère personnel sont les suivants: limitation des finalités, la portée de l'utilisation des données par un pays tiers devrait être clairement et précisément définie dans l'accord et ne devrait pas dépasser ce qui est nécessaire compte tenu des objectifs à atteindre. Chaque accord devrait contenir une liste exhaustive des catégories de données PNR à transférer; catégories spéciales de données à caractère personnel (données sensibles): les données PNR révélant les origines raciales ou ethniques, les opinions politiques ou les convictions religieuses ou philosophiques, l'appartenance à un syndicat, l'état de santé ou la vie sexuelle d'une personne ne seront pas utilisées, sauf dans des circonstances exceptionnelles, lorsqu'il existe un risque de mort imminent et à condition que le pays tiers fournisse les garanties requises, par exemple en veillant à ce que ces données ne puissent être utilisées qu'au cas par cas, sur autorisation d'un haut fonctionnaire et uniquement aux fins prévues pour le transfert initial; sécurité des données: les données PNR doivent être protégées contre tout abus ou accès illégal au moyen de toutes les procédures et mesures techniques appropriées permettant de prévenir les risques pour la sécurité, la confidentialité ou l'intégrité des données; surveillance et responsabilité: un dispositif de supervision par un organisme public indépendant responsable de la protection des données et jouissant de véritables pouvoirs d'intervention et de répression doit être mis en place afin d'assurer la surveillance des autorités publiques utilisant les données PNR. Ces dernières seront responsables du respect des règles établies en matière de protection des données à caractère personnel et devraient être habilitées à recevoir les plaintes des particuliers relatives au traitement de leurs données PNR;transparence et information: chaque intéressé sera informé, au minimum, de la finalité du traitement des données à caractère personnel, de l'entité qui traitera ces données, conformément à quelles règles ou dispositions législatives, des types de tiers auxquels les données seront divulguées et des voies de recours disponibles;accès, rectification et suppression: chaque intéressé aura accès à ses données PNR et jouira, le cas échéant, du droit de demander la rectification ou la suppression de ces données; recours: chaque intéressé jouira d'un droit de recours administratif ou judiciaire effectif en cas de violation de sa vie privée ou des règles de protection des données, sans discrimination fondée sur la nationalité ou le lieu de résidence ; conservation des données: la période de conservation des données PNR ne devrait pas dépasser ce qui est nécessaire à la réalisation des tâches définies ; il devrait prévoir des restriction des transferts ultérieurs à des pays tiers.

986 L'Union européenne négocie actuellement un nouvel accord PNR avec le Canada, qui remplacera l'accord de 2006.

987 Voy. le communiqué de presse : « Signature de l'accord UE-Canada sur les données des dossiers passagers (données PNR », 25/06/2014) disponible à l'adresse : http://ww.consilium.europa.eu/uedocs/cms_data/docs/pressdata/fr/jha/143371.pdf

988 Accord UE-Australie sur le traitement des données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, disponible à l'adresse : http://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:22012A0714(01)&rid=3.

criminalité transnationale, ainsi que pour les enquêtes et les poursuites en la matière ». L'accord dispose que les données des passagers aériens sont traitées par le service australien des douanes et de la protection des frontières uniquement dans un objectif de prévention et de détection d'infractions terroristes avec une durée de conservation de 5 ans et demi. Pendant 3 ans, il n'y a que certains fonctionnaires expressément autorisés qui y ont accès, ensuite pendant la fin de la période, c'est-à-dire 2 ans et demi, les éléments d'identification individuelle sont effacés. L'accord interdit d'utiliser des données sensibles, le prix du billet, les modalités de paiement, le numéro de carte bancaire, les réservations d'hôtel et de voiture à l'arrivée et également des informations le plus généralement liées aux services demandés à bord tel que le choix d'un menu répondant à des exigences religieuses ou aux demandes d'assistance pour des raisons médicales. Concernant les garanties, l'accord prévoit un droit d'accès, de rectification et d'effacement des données pour les passagers. Les passagers disposent également d'un recours administratif et judiciaire effectif. Enfin, les données venant de l'UE ne pourront être transférées à des pays tiers que sous certaines conditions (au cas par cas, à certaines autorités publiques seulement, le destinataire doit offrir les mêmes garanties que l'accord, et le destinataire ne transfèrera pas ces données par la suite). Le CEDP a émis un avis positif[989] quant aux mesures de sécurité des données mises en place, ainsi qu'aux dispositions relatives aux organes de contrôle. Il a souligné que selon l'accord, toute personne peut saisir l'autorité australienne pour la protection des données ainsi que les autorités judiciaires australiennes, des garanties considérées comme essentielles. Le CEDP a également identifié une importante marge d'amélioration, notamment en ce qui concerne le champ d'application de l'accord, la définition du terrorisme, l'inclusion de certaines fins exceptionnelles et la durée de conservation des données PNR. Toutefois selon le CEDP, l'accord devait se fonder sur l'article 16 du TFUE et non sur l'article 82, paragraphe 1, lettre d), et 87, paragraphe 2, lettre a), conformément à la déclaration 21 annexée au traité de Lisbonne et dans le contexte plus large de la légitimité de tout système PNR, considéré comme la collecte systématique des données de passagers à des fins d'évaluation des risques. Toutes ces considérations ont été cependant ignorées. Les eurodéputés se sont montrés plus pessimistes. La majorité des interventions ont critiqué le flou qui entourent les accords. Ainsi lors de l'approbation du texte, les eurodéputés avaient évoqué l'absence d'une uniformité concernant les accords PNR. De plus, la Commission avait présenté en septembre 2010 une communication relative à la démarche globale en matière de transfert des données PNR aux pays tiers [990] . Cependant lorsqu'on regarde en détail la durée de conservation des données, celle-ci diffère selon les accords.

B. L'accord PNR échoué avec le Canada

989 Voy. l'avis sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (données PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières, OJ C 322/01, 23.12.2011, p.1 Avis consultable https://edps.europa.eu/sites/edp/files/publication/11-07-15_pnr_australia_fr.pdf.

990 Communication de la Commission européenne du 21 septembre 2010 : relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers COM/2010/0492 final.

130 Un accord jugé disproportionné. Le 18 juillet 2005, le Conseil a approuvé la négociation d'un accord entre la communauté européenne et le gouvernement canadien sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers, ci-après « l'accord de 2006 »[991]. Eu égard à cet engagement, la Commission européenne a adopté, sur le fondement de l'article 25, paragraphe 2, de la directive 95/46/CE, la décision d'adéquation 2006/253/CE[992], dont l'article 1er prévoyait que l'accord était considéré comme assurant un niveau de protection adéquat des données PNR transférées à partir des vols européens à destination du Canada. La décision 2006/253 ayant expiré au mois de septembre 2009, et la durée de validité de l'accord de 2006 étant liée à celle de cette décision [993], cet accord est donc également venu à échéance au mois de septembre 2009. Le 5 mai 2010, le Parlement a adopté une résolution sur le lancement des négociations sur des accords relatifs aux données des passagers aériens (PNR) avec les États-Unis, l'Australie et le Canada [994] . Dans cette résolution, le Parlement demandait notamment la mise en œuvre d'une approche cohérente pour l'utilisation des données PNR avec l'élaboration d'un ensemble unique de principes devant servir de base à la conclusion des accords avec les pays tiers. À cet égard, il invitait la Commission à présenter une proposition de modèle unique et un projet de mandat de négociation avec les pays tiers, tout en énonçant les conditions minimales devant être remplies[995]. Le 21 septembre 2010, la Commission a adopté trois propositions visant à autoriser l'ouverture des négociations avec les États-Unis, l'Australie et le Canada[996]. Par la suite, des accords ont été signés et conclus avec les États-Unis et l'Australie suite à l'approbation du Parlement[997]. Ces accords sont entrés en vigueur en 2012. Concernant le Canada, après la clôture des négociations, la Commission a adopté, le 19 juillet 2013, la proposition de décisions au Conseil relative à la signature et à la conclusion de l'accord envisagé. Toutefois, le CEDP s'est montré critique vis-à-vis du projet d'accord PNR avec le Canada par rapport au principe de nécessité et proportionnalité [998] . Ainsi il a rendu son avis sur cette proposition le 30 septembre 2013[999]. Dans cet avis, le CEPD soulevait une série d'interrogations quant à la nécessité et la proportionnalité des systèmes PNR, mettant en doute le choix de la base juridique

---

991 Voy. Décision 2006/230/CE du Conseil, du 18 juillet 2005, relative à la conclusion de l'accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données IPV/DP (JO 2006, L 82, p. 14).

992 Décision de la Commission du 6 septembre 2005, constatant le niveau de protection adéquat des données à caractère personnel contenues dans les dossiers des passagers aériens (DP) transférés à l'Agence des services frontaliers du Canada (JO 2006, L 91, p. 49).

993 Voy. Article 5 de l'accord de 2006.

994 JO 2011, C 81 E, p. 70.

995 Voy. § 7 et 9 de ladite résolution.

996 Voy. Respectivement SEC (2010) 1082, SEC(2010) 1083 et SEC(2010) 1084.

998 Voy. L'avis du CEDP 5/2015 disponible à l'adresse : https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf

999 Voy. L'avis sur ces propositions de décisions. Le texte intégral de cet avis, dont un résumé a été publié au Journal officiel de l'Union européenne (JO 2014, C 51, p. 12), est disponible sur le site Internet du CEPD, http://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-09-30_Canada_FR.pdf.

matérielle et sur les différentes dispositions de l'accord envisagé. De plus, l'Agence européenne des droits fondamentaux (FRA), le Groupe de travail de l'article 29 des autorités nationales chargées de la protection des données, le Service de recherche du Parlement européen (EPRS) et le Comité d'experts sur les migrations internationales, les réfugiés et les criminels, se sont exprimé dans le même sens estimant que le partage des données PNR ne respecte pas les critères de « nécessité et proportionnalité » puisque les avantages présumés n'ont jamais été testés et l'argument selon lequel cette collecte de données aiderait à prévenir le terrorisme ne repose pas sur des évidences[1000]. Toutefois, le 5 décembre 2013, le Conseil a adopté une décision relative à la signature de l'accord envisagé sans que des modifications souhaitées par le CEDP aient été apportées. Ainsi l'accord a été signé le 25 juin 2014 sous réserve de sa conclusion à une date ultérieure et le Conseil de l'Union européenne a demandé au Parlement européen d'approuver le projet de décision relative à la conclusion, au nom de l'Union[1001]. Le Parlement a alors décidé de saisir la Cour de justice afin de déterminer si l'accord était conforme aux traités et à la Charte des droits fondamentaux de l'Union européenne [1002] . Le Parlement européen demande notamment si, malgré les garanties inscrites dans l'accord, l'ingérence dans le droit fondamental à la protection des données est justifiée. On remarque que c'est la première fois qu'est demandé à la Cour de justice de se prononcer sur la compatibilité[1003] d'un projet d'accord international avec la Charte des droits fondamentaux de l'UE[1004]. Ainsi la Cour de justice suivant les conclusions de l'Avocat général Mengozzi a estimé que le projet d'accord PNR avec le Canada n'était pas compatible avec le droit de l'Union européenne. Cela aurait pu avoir un

---

1000 Voy. l'article disponible en ligne : http://www.politico.eu/wp-content/uploads/2017/07/EU-Canada-PNR.pdf.

1001 Ce projet de décision vise comme bases juridiques l'article 82, paragraphe 1, sous d), et l'article 87, paragraphe 2, sous a), TFUE, lus en combinaison avec l'article 218, paragraphe 6, sous a), v), TFUE1001.

1002 Le Parlement souhaite également savoir si l'accord envisagé doit se fonder juridiquement sur les articles 82 et 87 TFUE (coopération judiciaire en matière pénale et coopération policière) ou bien sur l'article 16 TFUE (protection des données à caractère personnel). À cet égard, l'avocat général répond que l'accord doit être conclu à la fois sur la base des articles 16 et 87 TFUE. En effet, l'accord envisagé poursuit deux objectifs indissociables et d'importance égale (à savoir d'une part la lutte contre le terrorisme et la criminalité transnationale grave – qui ressort de l'article 87 TFUE – et d'autre part la protection des données à caractère personnel – qui ressort de l'article 16 TFUE). Aux termes de l'article 218, paragraphe 11, TFUE, un État membre, le Parlement, le Conseil ou la Commission peut recueillir l'avis de la Cour sur la compatibilité d'un accord dont la conclusion est envisagée avec les traités. Conformément à la jurisprudence constante de la Cour, cette disposition vise à prévenir les complications qui résulteraient de contestations en justice relatives à la compatibilité avec les traités d'accords internationaux engageant l'Union. En effet, une décision judiciaire constatant éventuellement, après la conclusion d'un accord international engageant l'Union, que celui-ci est, au vu soit de son contenu, soit de la procédure adoptée pour sa conclusion, incompatible avec les dispositions des traités ne manquerait pas de créer, sur le plan non seulement interne de l'Union, mais également des relations internationales, des difficultés sérieuses et risquerait de porter préjudice à toutes les parties intéressées, y compris les États tiers [avis 2/13 (Adhésion de l'Union à la CEDH), du 18 décembre 2014, EU:C:2014:2454, points 145 et 146 ainsi que jurisprudence citée].

1003 La Cour doit se prononcer si l'accord est compatible avec l'article 16 TFUE et avec les articles 7, 8 et l'article 52, paragraphe 1, de la Charte.

1004 Sans qu'il soit besoin d'examiner de manière individuelle et exhaustive les 19 catégories de données PNR énumérées dans l'annexe à l'accord envisagé Il ne fait donc aucun doute, au regard de la jurisprudence de la Cour, que la transmission systématique des données PNR aux autorités publiques canadiennes, l'accès à ces données et l'utilisation et la conservation pour une durée de cinq ans de ces données par ces mêmes autorités publiques ainsi que, le cas échéant, leur transfert ultérieur au profit d'autres autorités publiques, y compris d'autres pays tiers, en vertu des stipulations de l'accord envisagé, sont des opérations qui entrent dans le champ d'application du droit fondamental au respect de la vie privée et familiale garanti par l'article 7 de la Charte ainsi qu'à celui « étroitement lié », mais néanmoins distinct, relatif à la protection des données à caractère personnel garanti par l'article 8, paragraphe 1, de la Charte et constituent une ingérence dans ces droits fondamentaux.

impact sur la mise en place d'une directive PNR pour l'Union européenne[1005] et sur le plan externe sur les autres négociations en cours entre l'UE et des États tiers. Toutefois, on observe que les attentats qui ont frappé l'Europe à partir de celui de janvier 2015 à Paris ont réactivé le débat quant à la nécessité de tels accords. Dans ses conclusions, l'Avocat général s'appuie très largement sur la jurisprudence de l'arrêt *Digital Rights Ireland*[1006] (annulant la directive « *Data Retention* » sur la conservation des données) et *Schrems*[1007] (condamnant tout stockage massif de données, contraire au principe de proportionnalité). Ainsi c'est la troisième fois que la Cour européenne a statué contre les dispositions relatives au stockage massif des données personnelles[1008]. Concernant les catégories de données visées par l'accord, l'Avocat général souligne que les 19 catégories de données PNR sont transmises aux autorités canadiennes à l'égard de tous les voyageurs empruntant une liaison aérienne entre le Canada et l'Union, sans qu'il existe un indice que le comportement de ces voyageurs puisse avoir un lien avec une activité terroriste ou de criminalité transnationale grave. À l'égard du caractère suffisamment précis de la finalité pour laquelle le traitement de données PNR est autorisé, il estime que l'accord envisagé doit être accompagné d'une liste exhaustive des infractions relevant de la définition des « formes graves de criminalité transnationale », prévue à l'article 3, paragraphe 3, de cet accord. De plus, en l'état actuel de sa rédaction, l'article 3, paragraphe 5, de l'accord envisagé est incompatible avec les articles 7, 8 et l'article 52, paragraphe 1, de la Charte, en ce qu'il permet, au-delà de ce qui est strictement nécessaire, d'élargir les possibilités de traitement de données PNR, indépendamment des finalités poursuivies par l'accord envisagé. Sur l'identification de l'autorité compétente en charge du traitement de données PNR, l'avocat général relève que l'accord n'est pas suffisamment clair et précis quant à l'identification de l'autorité chargée du traitement des données PNR, de manière à assurer la protection et la sécurité desdites données[1009]. Ainsi il conclut que l'accord dans l'état actuel ne peut pas être conclu[1010]. Le 26 juillet 2017, la Cour de justice en suivant les conclusions de l'Avocat général

1005 Proposition de directive du Parlement européen et du Conseil relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquê tes et les poursuites en la matière, COM(2011) 32 final, Bruxelles, 2 février 2011. En avril 2011, le Parlement européen a demandé à la FRA de remettre un avis sur cette proposition et sur sa conformité avec la Charte des droits fondamentaux de l'Union européenne. Voy. : FRA (2011), Avis 1/2011 – Données des dossiers passagers, Vienne, 14 juin 2011.

1006 Arrê t C-293/12 & C-594/12, de la Cour du 8 avril 2014, Digital Rights Ireland, la Cour de justice déclare la directive sur la conservation des données invalide).

1007 Arrê t de la Cour du 6 octobre 2015, Schrems C-362/14, la Cour déclare invalide la décision de la Commission constatant que les États-Unis assurent un niveau de protection adéquat aux données à caractère personnel transférées).

1008 Voy. Les affaires *Digital Rights* et *Schrems* prèc.

1009 Dans ces conditions, et ainsi que l'a relevé M. l'avocat général Mengozzi au point 316 de ses conclusions, l'article 10 de l'accord envisagé ne garantit pas de manière suffisamment claire et précise que la surveillance du respect des règles prévues par cet accord, relatives à la protection des personnes physiques à l'égard du traitement des données PNR, sera effectuée par une autorité indépendante, au sens de l'article 8, paragraphe 3, de la Charte.

1010 L'avocat général conclu et répond à l'avis du Parlement déclarant que l'acte du Conseil portant conclusion de l'accord envisagé entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers (PNR), signé le 25 juin 2014, doit être fondé sur l'article 16, paragraphe 2, premier alinéa, et l'article 87, paragraphe 2, sous a), TFUE, lus en combinaison avec l'article 218, paragraphe 6, sous a), v) TFUE. Ainsi l'accord envisagé, pour être compatible avec l'article 16 TFUE et les articles 7, 8, et l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne, doit prévoir que: les catégories de données PNR des passagers aériens soient libellées de manière claire et précise et que les données sensibles soient exclues du champ d'application de l'accord; les infractions relevant de la définition des formes graves de criminalité transnationale soient énumérées de manière exhaustive dans l'accord; de plus, l'accord devrait identifier de manière

a confirmé dans son avis[1011] que l'accord UE / Canada sur la collecte des données des voyageurs aériens violait la législation européenne. Comme souligné par la Cour de justice, si l'existence d'une base légale, de l'intérêt légitime et le respect du contenu essentiel ne font pas défaut, le projet d'accord PNR n'échappe pas pour autant au contrôle de proportionnalité et de stricte nécessité. Ainsi l'accord est incompatible avec les articles 7, 8 ainsi qu'avec l'article 52, paragraphe 1, de la Charte des droits fondamentaux de l'Union européenne en cela qu'il n'exclut pas le transfert des données sensibles depuis l'Union européenne vers le Canada ainsi qu'il ne limite pas l'utilisation et la conservation de ces données[1012]. Selon la Cour, pour être compatible avec le droit de l'Union européenne et en particulier avec la Charte des droits fondamentaux l'accord devrait : déterminer de manière claire et précise les données des dossiers passagers à transférer depuis l'Union européenne vers le Canada ; prévoir que les modèles et les critères utilisés dans le cadre du traitement automatisé des données des dossiers passagers seront spécifiques et fiables ainsi que non discriminatoires ; prévoir que les bases de données utilisées seront limitées à celles exploitées par le Canada en rapport avec la lutte contre le terrorisme et la criminalité transnationale grave ; soumettre, hormis dans le cadre des vérifications relatives aux modèles et aux critères préétablis sur lesquels sont fondés les traitements automatisés des données des dossiers passagers, l'utilisation de ces données par l'autorité canadienne compétente pendant le séjour des passagers aériens au Canada et après leur départ de ce pays, de même que toute communication desdites données à d'autres autorités, à des conditions matérielles et procédurales fondées sur des critères objectifs ; subordonner cette utilisation et cette communication, sauf cas d'urgence dûment justifiés, à un contrôle préalable effectué soit par une juridiction soit par une entité administrative indépendante, dont la décision autorisant l'utilisation intervient à la suite d'une demande motivée de ces autorités, notamment dans le cadre de procédures de prévention, de détection ou de poursuites pénales ;

---

claire et précise l'autorité chargée du traitement des données PNR, de sorte à assurer la protection et la sécurité de ces données; le nombre de personnes ciblées devrait être délimité, de sorte que ne soient concernées que les personnes sur lesquelles pèse un soupçon raisonnable de participation à une infraction terroriste ou de criminalité transnationale grave. L'accord devrait ainsi indiquer de manière motivée les raisons objectives justifiant la nécessité de conserver toutes les données des dossiers passagers pour une période maximale de cinq ans.

1011 Voy. l'Avis 1/15 de la Cour de justice (grande chambre) 26 juillet 2017. La demande d'avis soumise à la Cour par le Parlement européen est formulée comme suit : « L'accord envisagé [entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers] est-il compatible avec les dispositions des traités (article 16 TFUE) et la charte des droits fondamentaux de l'Union européenne (articles 7, 8 et article 52, paragraphe 1) en ce qui concerne le droit des personnes physiques à la protection des données à caractère personnel ? L'article 82, paragraphe 1, second alinéa, sous d), et l'article 87, paragraphe 2, sous a), TFUE constituent-ils la base juridique appropriée de l'acte du Conseil [de l'Union européenne] portant sur la conclusion de l'accord envisagé ou cet acte doit-il se baser sur l'article 16 TFUE ? ».

1012 Selon une jurisprudence constante de la Cour, le choix de la base juridique d'un acte de l'Union, y compris celui adopté en vue de la conclusion d'un accord international, doit se fonder sur des éléments objectifs susceptibles de contrôle juridictionnel, parmi lesquels figurent la finalité et le contenu de cet acte (arrêts du 6 mai 2014, Commission/Parlement et Conseil, C 43/12, EU point 29, ainsi que du 14 juin 2016, Parlement/Conseil, C 263/14, point 43 et jurisprudence citée). Si l'examen d'un acte de l'Union démontre qu'il poursuit deux finalités ou qu'il a deux composantes et si l'une de ces finalités ou de ces composantes est identifiable comme étant principale tandis que l'autre n'est qu'accessoire, l'acte doit être fondé sur une seule base juridique, à savoir celle exigée par la finalité ou la composante principale ou prépondérante. À titre exceptionnel, s'il est établi, en revanche, que l'acte poursuit à la fois plusieurs objectifs ou a plusieurs composantes qui sont liés de façon indissociable, sans que l'un soit accessoire par rapport à l'autre, de telle sorte que différentes dispositions des traités sont applicables, une telle mesure doit être fondée sur les différentes bases juridiques correspondantes (arrêt du 14 juin 2016, Parlement/Conseil, C 263/14, point 44 et jurisprudence citée). Toutefois, le recours à une double base juridique est exclu lorsque les procédures prévues pour l'une et l'autre de ces bases sont incompatibles (arrêt du 6 novembre 2008, Parlement/Conseil, C 155/07, point 37 et jurisprudence citée). Selon l'avis de la CJUE, la décision du Conseil relative à la conclusion, au nom de l'Union, de l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers doit être fondée conjointement sur l'article 16, paragraphe 2, et sur l'article 87, paragraphe 2, sous a), TFUE.

limiter la conservation des données des dossiers passagers après le départ des passagers aériens à celles des passagers à l'égard desquels il existe des éléments objectifs permettant de considérer qu'ils pourraient présenter un risque en termes de lutte contre le terrorisme et la criminalité transnationale grave ; soumettre la communication des données des dossiers passagers par l'autorité canadienne compétente aux autorités publiques d'un pays tiers à la condition qu'il existe soit un accord entre l'Union européenne et ce pays tiers équivalent à l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, soit une décision de la Commission européenne, au titre de l'article 25, paragraphe 6, de la directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, couvrant les autorités vers lesquelles la communication des données des dossiers passagers est envisagée ; prévoir un droit à l'information individuelle des passagers aériens en cas d'utilisation des données des dossiers passagers les concernant pendant leur séjour au Canada et après leur départ de ce pays ainsi qu'en cas de divulgation de ces données par l'autorité canadienne compétente à d'autres autorités ou à des particuliers, et garantir que la surveillance des règles prévues par l'accord entre le Canada et l'Union européenne sur le transfert et le traitement de données des dossiers passagers, relatives à la protection des passagers aériens à l'égard du traitement des données des dossiers passagers les concernant, est assurée par une autorité de contrôle indépendante. Ainsi l'avis de la Cour de justice obligera l'Union européenne à renégocier l'accord avec le Canada afin d'assurer sa conformité aux droits fondamentaux garantis par la Charte (sur des points d'inégale difficulté technique). En conséquence, l'accord de 2006 entre l'Union européenne et le Canada sur les PNR restera en vigueur jusqu'à ce qu'un nouvel accord puisse le remplacer. Si la Cour de justice valide le système PNR vis-à-vis de l'objectif d'intérêt général relatif à la sécurité publique elle souligne que l'intérêt général à la sécurité ne l'emporte pas sur le droit fondamental à la protection des données personnelles. Nous pouvons constater que la conclusion d'un accord PNR avec le Canada peut avoir des conséquences tant sur le plan interne à l'Union européenne (1) que sur le plan de futures négociations avec des États tiers (2).

1) Des conséquences sur le plan interne

La conclusion d'accords entre l'Union et des États tiers concernant les données PNR a fait naître un débat au sein même de l'Union européenne. Le Royaume-Uni avait déjà mis en place un système PNR, tandis que d'autres États comme la France depuis 2008 utilisaient les données PNR à titre expérimental. La Commission reconnaissant la nécessité de disposer des données PNR dans le cadre de la prévention du terrorisme et des formes graves de criminalité et de la lutte contre ces phénomènes, avait présenté une proposition de décision-cadre relative à l'utilisation des données des dossiers passagers à des fins répressives. À la suite de l'entrée en vigueur du traité de Lisbonne, la Commission a proposé de remplacer cette proposition par une directive portant le même intitulé, qui devait obliger les transporteurs aériens à transmettre aux États membres les données PNR. En effet, pour désorganiser les réseaux terroristes et criminels, il est essentiel de pouvoir suivre les déplacements. Ainsi dans le contexte de lutte contre le terrorisme l'UE a voulu adopter une directive PNR en avril 2016. Cette adoption a été réclamée

par la France et plusieurs États depuis les attentats de Paris de janvier 2015. Les attentats de Bruxelles et Berlin ont par la suite aussi contribué à son adoption par les parlementaires. L'élaboration de la directive PNR a donné lieu à des débats enflammés entre le Parlement et les États membres, les eurodéputés exigeant des garanties sur la protection des données recueillies. Un compromis politique sur le PNR avait été trouvé en décembre 2015 entre les négociateurs du Parlement et des États membres mais le vote du texte a pris du retard en raison de réticences des groupes parlementaires socialistes, libéraux et Verts, qui demandaient que le texte sur la protection des données personnelles soit voté en même temps [1013] . Ainsi les colégislateurs ont achevé leurs travaux concernant l'établissement d'une directive encadrant le système européen de dossiers passagers (PNR), pour les passagers des compagnies aériennes, qui devrait être totalement compatible avec la Charte des droits fondamentaux tout en fournissant un instrument efficace au niveau de l'UE. Toutefois le fait que le système PNR ne soit pas centralisé au niveau de l'Union européenne a fait l'objet de vives critiques[1014].

2) Des conséquences sur le plan externe

L'accord PNR entre l'Union européenne et le Canada a été considéré comme le moins restrictif de tous les accords PNR de l'Union européenne. Afin de respecter l'avis de la Cour de justice, l'Union européenne devrait immédiatement suspendre les transferts des données PNR avec l'Australie et les États-Unis et renégocier des accords PNR dans le respect des droits fondamentaux. La Nouvelle-Zélande et la Corée du Sud utilisent également des données PNR, mais ces pays n'ont pas conclu d'accord avec l'Union européenne. Il est probable que dans les années à venir la tendance se confirme et que de plus en plus de pays adoptent des systèmes PNR. Plusieurs pays ont également adopté une législation PNR à titre expérimental comme l'Afrique du Sud, l'Arabie Saoudite et le Japon. Le 14 juillet 2015, les négociations sur un accord UE-Mexique concernant le transfert de données PNR ont été officiellement lancées[1015]. Les projets ont été débattus le 15 avril 2015 en session plénière et le 4 juin 2015 en commission des libertés civiles. Ainsi tout projet d'accord PNR avec le Mexique devra prendre en compte le contenu de l'avis de la Cour de justice sur l'accord PNR UE-Canada. Une fois conclu, il ne pourrait entrer en vigueur qu'avec l'accord du Parlement européen lequel pourrait saisir la Cour de justice pour donner son avis.

1013 Adoptée le 27 avril 2016 et publiée au JO de l'Union européenne du 4 mai 2016 la nouvelle directive 2016/681 devra être transposée dans la loi nationale de chaque État membre au plus tard le 25 mai 2018.

1014 En effet les données PNR seront collectées par des « unités d'informations passengers » (UIP) crées dans chaqque États membre. Ces données peuvent s'echanger parmi les UIP des États membres e Europol.

1015 Le Conseil a donné son mandat à la Commission le 23 juin 2015.

Section II. La politique étrangère de sécurité de l'Union européenne. La conclusion d'accords sur la surveillance des données financières

131 La lutte contre le terrorisme. L'analyse menée jusqu'ici a permis d'observer que dans la tradition de l'Union européenne, la protection des données personnelles est un droit fondamental. Cela s'explique par des raisons historiques puisque le continent européen a connu plusieurs régimes totalitaires dans lesquels les données personnelles ont été l'instrument de contrôle des individus. Aujourd'hui le risque est lié aux formes de contrôle exercés par les nouvelles technologies, que ce soit dans le secteur privé (avec l'exemple des géants du web qui peuvent manipuler nos choix, grâce au profilage de la personne) que dans le secteur public (avec l'exemple de l'État qui, avec le prétexte de garantir la sécurité, collecte et traite les données des citoyens et peut exercer une forme de contrôle). Le danger est alors dans les finalités des usages des données personnelles. L'utilisation des données personnelles est un domaine où différentes conceptions s'opposent. Ce domaine est en effet marqué par une forte opposition entre l'approche américaine, davantage libérale et la conception européenne, plus paternaliste[1016].Ainsi en Europe, la vision politique est marquée par une philosophie kantienne de « la Paix perpétuelle », dans un monde régi par le droit et les institutions. La sécurité est perçue comme un « devoir » de l'État, et doit se concilier avec la liberté (à travers la protection des droits fondamentaux). La protection des droits fondamentaux constitue le cœur de la politique sécuritaire de l'Union européenne, jouissant d'un ancrage constitutionnel dans la Charte des droits fondamentaux. Au contraire, selon le politologue Robert Kagan [1017] , l'approche américaine serait marquée par la vision du monde de Thomas Hobbes et de John Locke, où « la sécurité est considérée comme l'objet même de l'engagement en société », ce qui légitime l'usage de la force et la restriction aux droits et libertés fondamentales[1018]. Or, ces deux conceptions sont porteuses d'une connotation très forte, susceptible d'influer sur la détermination des enjeux liés au droit à la protection des données personnelles. Ainsi l'expression « *privacy* » est utilisée dans les pays de culture anglo-saxonne et implique la protection de la vie privée. Pour revenir à la formulation originelle de Warren et Brandeis, celle de « *right to privacy* »[1019], la *privacy* n'est pas un droit privé subjectif, comme le droit de

---

1016 Sur la conception américaine de la protection des données personnelles v. J.-B. RULE, « La protection des données personnelles aux États-Unis. La réaction à la directive européenne », *RFAP*, n° 89, 1999, pp. 95 et s. ; Y. DETRAIGNE., A.-M. ECOFFIER, *Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques*, préc., sp. pp. 51-53. Plus générale sur l'opposition entre la conception américaine et celle européenne de la vie privée v. J. Q. WHITMAN, *The two western cultures of privacy : dignity versus liberty*, 2003-2004, 113 *Yale L. J.*, p. 1151.

1017 Voy. R. KAGAN, *Puissance américaine, faiblesse européenne*, Disponible à l'adresse: http://www.lemonde.fr/international/article/2002/07/26/puissance-américaine-faiblesse-europeenne-par-robert-kagan_285878_3210.html#3hyM7vKbMKbfUqPB.99

1018 M. GAUCHET, *La démocratie contre elle-même*, Gallimard, Collection Tel, 2002, p. 215.

1019 S.D. WARREN and L. D. BRANDIES, *The right to privacy*, Harvard Law Review, Dec. 15, 1890, Vol. 4, No. 5 pp. 193-220.

propriété, le droit de créance ou même le droit sur son image : elle appartient plutôt à la catégorie des droits publics subjectifs, des libertés protégées contre des ingérences extérieures [1020] . Dans cette conception manque l'idée d'autodétermination informative, de disposer de ses propres informations présente dans les pays de *civil law.* Dans la culture de *civil law*, comme dans l'Union européenne, on utilise l'expression « droit des données personnelles » ou « droit à la protection des données personnelles » pour renvoyer à un droit subjectif consacré comme un droit fondamental et qui présente un caractère autonome vis-à-vis de la vie privée. De plus, l'Union européenne et les États-Unis se distinguent par leur conception divergente des droits fondamentaux. Ces différences d'approches, sont aggravées par une hiérarchisation différente des priorités dans le débat sécurité / liberté et l'adoption par les États-Unis de législations priorisant la lutte contre le terrorisme. Ce n'est pas le but de ce travail de présenter une analyse détaillée de la législation américaine sur la protection des données personnelles puisqu'il existe aux États-Unis, à côté du système juridique fédéral, différents ordres juridiques (égal au nombre d'États fédérés). De plus, une analyse de toutes les législations ne présenterait aucun intérêt, puisque les accords sur les transferts des données personnelles avec l'Union européenne ont été conclus par le gouvernement fédéral. Cependant, rien n'empêche d'apporter des considérations générales sur la façon dont le droit à la protection de données personnelles est conçu dans la loi fédérale américaine et dans d'autres pays afin de comprendre la spécificité de la protection offerte par le modèle de protection de l'Union européenne. Aux États-Unis, la réglementation en matière de protection des données est sectorielle [1021] et il n'existe aucun régulateur américain spécifiquement en charge de la protection des données. Toutefois, les attentats du 11 septembre 2001, ont accéléré la coopération sécuritaire et des instruments spécifiques à la lutte anti-terroriste ont été mis en place, non sans conséquence pour la protection des données personnelles des citoyens européens. En effet, l'impératif de sécurité nationale suppose que des mesures extraordinaires soient adoptées et rend légitimes de nombreux sacrifices à la protection de données. Le programme de surveillance du financement du terrorisme dit *Terrorist Finance Traking Program* (ci-après TFTP), relève d'un aspect spécifique du terrorisme, c'est-à-dire prévenir, enquêter et détecter les activités de financement du terrorisme[1022]. Ainsi le terrain des choix politiques en matière de sécurité offre un prisme intéressant pour mener l'analyse de la spécificité du model européen. Dans la précédente section, il a été illustré que l'accord PNR portait atteinte aux données personnelles. Ici nous analyserons l'affaire *Swift*[1023] (§1) comme

---

1020 N. WESLEY HOHFELD, « Fundamental Legal Conceptions as Applied in Judicial Reasoning and Other Legal Essays, New Haven », *Yale University Press*, 1923, p. 43-49.

1021 On peut citer le Federal Credit Act pour le secteur bancaire, les Privacy Act et Freedom of Information Act pour le secteur public, le Telecommunication Act dans le domaine de la santé, le COPPA pour la protection des enfants et le CAN-SPAM en matière de marketing et lutte contre le spam.

1022 Voy. l'Accord entre l'Union européenne et les États-Unis sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO L 195 du 27 Juillet 2010.

1023 L'organisme financier belge SWIFT, transférait au Département Américain du Trésor des informations relatives aux transactions financières traitées afin que les États-Unis effectuent des croisements entre des transactions financières et des individus suspectés de financement du terrorisme. Ce transfert, qui est resté secret entre 2001 et 2006 a été révélé par deux journaux américains et vivement critiqué par le Parlement européen, Voy. Parlement européen, Résolution du 14 février 2007 sur SWIFT, l'accord PNR et le dialogue transatlantique sur ces questions, P7_TA(2007)0039, Strasbourg, JO C 287 du 29

un nouvel épisode de friction entre l'Union européenne et les États-Unis. Le débat entre sécurité et liberté est loin d'être épuisé. Face aux pressions sécuritaires, l'Union européenne montre sa détermination à maintenir l'équilibre entre sécurité publique et protection des données personnelles (§2).

§1. La création du *Terrorist Finance Traking Program (*« TFTP »)

132 Une opération secrète. Suite aux attaques terroristes du 11 septembre 2001, les États-Unis ont élaboré un certain nombre de mesures législatives visant à renforcer la sécurité nationale en réponse à la menace du terrorisme. En effet, la facilité avec laquelle les terroristes du 11 septembre avaient utilisé le système bancaire afin de mettre en place leur activité, a mis en lumière la nécessité lutter contre le financement du terrorisme. Deux semaines après les attaques, le président américain Bush adoptait *l'Executive Order* 13224 ayant comme but : « *Blocking Property and Prohibiting Transactions With Persons Who Commit, Threaten To Commit or Support Terrorism* »[1024]. L'*Executive Order*, autorisait le Président à exercer les pouvoirs de l'« *International Emergency Economic Powers Act »* afin de congeler les biens des personnes soupçonnées de terrorisme et grâce au Titre III du Patriot Act, le gouvernement pouvait obliger les institutions financières à coopérer avec l'autorité publique et dans le cas échéant, le gouvernement aurait pu ordonner le gel de leurs activités comme prévu par *l'Executive Order* 13224. Le Département du Trésor américain, de concert avec la CIA, sur la base de l'*Executive Order*, commençait le « *Terrorist Finance Tracking Program »* (TFTP) et il émettait des « *Administrative Subpoenas* » (sommations) vis-à-vis des institutions financières sur le territoire américain afin de les obliger à fournir tous les renseignements sur les transactions bancaires. Ceci dit, au niveau mondial, les transactions financières transitent à travers un circuit géré par une société établie au Belgique, dénommées *Society for Worldwide Interbank Financial Télécommunication* (ci-après *Swift*) ayant des filiales entre autres aux États-Unis. A l'époque des faits, la Société de télécommunications interbancaires mondiales (*Swift*) traitait les flux financiers de plus de 8000 banques dans le monde, transmettait les données en sa possession aux autorités américaines agissant dans le cadre de leur programme de lutte contre le terrorisme (*Terrorist Finance Tracking Programme*, TFTP) et opérait avec un « centre jumeau » situé aux États-Unis. Ce dernier avait reçu une demande de communication de données de la part du ministère américain des finances aux fins d'une enquête liée au terrorisme[1025]. Le 23 juin 2006, le *New York Times*[1026], le *Los Angeles Times* et le *Wall Street*

novembre 2007; Résolution du 6 juillet 2006 sur l'interception des données des virements bancaires du système Swift par les services secrets américains, P6_TA(2006)0602, Strasbourg, JO C 303 du 13 décembre 2006.

1024 Voy. la Loi du 26 octobre 2001, initiée par George Bush et adoptée par le Congrès américain. Elle vise notamment à lutter contre le terrorisme en renforçant les pouvoirs des agences gouvernementales de renseignement et d'enquête, telles la CIA, le FBI ou la NSA. https://www.state.gov/j/ct/rls/other/des/122570.htm.

1025 Voy., dans ce contexte, groupe de travail Article 29, Avis 14/2011 sur les questions de protection des données relatives à la prévention du blanchiment de capitaux et du financement du terrorisme, WP 186, Bruxelles, 13 juin 2011 ; groupe de travail Article 29, Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT), WP 128, Bruxelles, 22 novembre 2006 ; Commission belge de la protection de la vie privée (2008), « Contrô le et procédure de recommandation initiées à l'égard de la société Swift scrl », décision, 9 décembre 2008.

Journal publiaient la nouvelle concernant le *Terrorist Finance Tracking Program* (TFTP), ainsi les Européens découvraient que les États-Unis utilisaient secrètement depuis 2001 des données bancaires personnelles stockées via le réseau *Swift* (*Society for Worldwide Interbank Financial Télécommunications*) [1027] . Suite à la polémique soulevée en Europe quant à l'atteinte aux données personnelles, un accord a été conclu en 2010[1028] entre l'UE et les États-Unis afin de donner une base légale aux échanges de données bancaires transatlantiques, et assurer par la même un niveau satisfaisant de protection des données à caractère personnel. Le Parlement européen a rejeté un premier accord temporaire le 11 février 2010. Un second accord a alors été proposé, négocié, conclu, puis finalement accepté par le même Parlement le 8 juillet 2010. À cause des lacunes en matière de protection des données, cet accord a fait l'objet d'un certain nombre d'améliorations, par exemple il est prévu que les autorités européennes via Europol puissent évaluer la pertinence des demandes américaines, qu'un représentant de l'UE soit présent à Washington afin de contrôler l'utilisation des données, ou enfin que les Européens puissent bénéficier de procédures judiciaires de réparation sur le sol américain [1029] . Il faut souligner que si les Institutions européennes s'étaient inquiétées de la situation[1030], l'opinion publique n'avait pas été autant choquée d'apprendre que les données bancaires de tous les citoyens européens avaient été espionnées depuis cinq ans avec la complicité des banques[1031]. En octobre 2006, le G29 a émis un avis selon lequel le transfert du circuit *Swift* vers les États-Unis devait respecter la législation belge et donc la directive 95/46 puisque la société *Swift* avait son siège au Belgique[1032]. *Swift* et les banques avaient violé la législation UE en matière de protection de données personnelles. Il a observé que selon l'art. 6 de la Directive les données personnelles doivent être traitées avec loyauté et de manière légitime ; elles doivent être recueillies pour des buts spécifiques, explicites et légitimes et ne peuvent être traitées pour des buts incompatibles avec ceux pour lesquelles elles ont été recueillies. Dans cette optique le transfert de données par le circuit *Swift* vers le Département du Trésor américain, faisait l'objet d'un « traitement autre » incompatible avec les buts commerciaux pour lesquels les données avaient été recueillies au sens de la directive. La jurisprudence de la CJ avait déjà affirmé dans l'affaire *Rechnungshof/Lauermann* que la communication de données collectées pour finalités

1026 E. LICHTBLAU et J. RISEN, « Bank data is sifted by US in secret to clock terror », 22 juin 2006, *New York Time*s. Cette révélation suivait de peu celle relative au programme de surveillance PRISM.

1027 M.A. LEDIEU, *L'adoption de la résolution sur les données des passagers et l'affaire Swift*, Communication Commerce électronique n° 4, Avril 2007, alerte 79.

1028 Accord du 28 juin 2010, suite à la décision du Conseil du 24 juin 2010, Décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, 11222/1/10.

1029 http://www.europaforum.public.lu/fr/actualites/2010/07/pe-swift/index.html.

1030 Voy. la Resolution du parlement on the interception of bank transfer data form the Swift systeem by the US secret services, avec laquelle il demandait aux États membres de vérifier qu'il n'y avait pas de lacunes législatives au niveau national et que la législation européenne en matière de protection des données couvrît également les banques centrales.

1031 M.A. LEDIEU, « Surveillance des transferts bancaires européens par les autorités américaines : vers une remise en cause des garanties négociées », in Communication Commerce électronique n° 10, Octobre 2009, alerte 124.

1032 Voy. Press release on the Swift case following the adoption of the Article 29 Working Party opinion on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunications"(SWIFT) http://ec.europa.eu/justice/policies/privacy/news/docs/PR_Swift_Affair_23_11_06_en.pdf aggiornato al 25.09.2012.

économiques et leur successive transmission à des tiers, y compris les autorités publiques, constituait « une ingérence au sens de l'art. 8 CEDH » et que des éventuelles dérogations devaient se justifier à la lumière de l'art. 13 de la directive 95/46 et de l'art. 8 §2 CEDH[1033]. De même, le G29 a souligné que ni la société *Swift*, ni les institutions financières n'avaient informé les responsables de traitement du transfert des données, comme prescrit aux articles. 10 et 11 de la directive 95/46. Ce transfert ne pouvait pas être justifié au regard de l'article 25 de la directive, puisque les États-Unis n'offraient pas un niveau de protection adéquat, ni ne pouvait tomber sous les exceptions de l'art. 26. De plus les mesures de contrôle mises en place par *Swift* ne pouvaient remplacer en aucun cas l'activité de l'autorité de contrôle indépendante prévue à l'art. 28 de la directive. Le G29 a rappelé le principe selon lequel même la lutte contre le terrorisme ne peut pas justifier une atteinte aux droits fondamentaux d'une telle ampleur[1034]. Constatant les violations, le G29 a appelé la société *Swift* et les institutions financières à prendre des mesures nécessaires pour remédier à l'illégalité des traitements[1035]. Ainsi la société *Swift* a arrêté de collecter les données dans son siège aux États-Unis et effectuait leur back up uniquement dans ses serveurs en Suisse et aux Pays-Bas. Le 27 juillet 2009, les 27 ministres des Affaires étrangères des États membres ont donné mandat à la Commission européenne pour négocier un accord intérimaire avec les États-Unis afin d'offrir une base légale nécessaire à garantir une protection adéquate des données[1036] *Swift*. On observe que la différence avec le scandale Prism est le fait qu'ici les données étaient transférées de manière volontaire de la part de *Swift* aux États-Unis pour une finalité de *back up*, sans que les règles de base de la directive 95/46, relatives aux transferts de données soient respectées. La conclusion d'un accord intérimaire qui réglait le flux de données financières était nécessaire, puisqu'une fois que les données des citoyens européens parviennent sur le sol américain, elles sont traitées selon la législation américaine pour la protection des données. Or, la protection des données aux États-Unis n'est pas inspirée d'une conception générale et chaque secteur est réglementé par des règles de protection des données qui lui sont propres. Ainsi, aucune régulation particulière n'est prévue pour le domaine pénal. Le texte de référence pour la protection des données personnelles est le *Privacy Act* de 1974, qui régit la protection des données en général. Cela pose trois problèmes au regard de la coopération transatlantique: premièrement, il ne protège que les citoyens américains, deuxièmement, le principe de finalité n'est pas reconnu par le *Privacy Act* et de nombreuses dérogations à ce principe sont possibles (même si le consentement de la personne concernée n'est pas obtenu, les données peuvent être utilisées à des fins différentes que celles pour lesquelles elles avaient été collectées) et enfin, aucun principe général n'existe aux États-Unis pour la durée de conservation des données. La conception européenne de protection des données dans l'accord TFTP nous permet d'étudier la mise en œuvre de l'approche européenne entre protection des droits fondamentaux et sécurité et ses limites. Nous

1033 CJUE, Rechnungshof/Lauermann, affaires jointes C-465/00, C-138/01 et C-139/01 20 mai 2003,Voy. §68.

1034 Voy. Avis. 10/2006 G29: On the processing of personal data by the society for worldwide interbank financialtelecommunication : http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp128_en.pdf.
1035 G29, WP 128, Avis 10/2006du 22 novembre 2006, p. 26.

1036 Voy. Décision 2010/412/UE du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, JO 2010 L 195, p. 3 et 4. Le texte de l'accord est joint à cette décision, JO 2010 L 195, p. 5–14.

verrons que l'UE n'est pas totalement parvenue à « exporter » son approche. Pour mener cette analyse, il faut tout d'abord rappeler les modifications apportées à l'accord entre ses versions de novembre 2009 (A) et de juillet 2010 (*Swift* II) qui ont permis d'obtenir le feu vert du Parlement européen (qui avait préalablement rejeté le texte) [1037] et approuver un texte de compromis (B).

A. Le premier accord « TFTP »

133 Les criticités du premier accord. Suite aux réserves exprimées par le G29[1038] et par le Parlement européen[1039], un dialogue transatlantique et des engagements entre la Commission européenne et le Conseil de l'UE d'une part et le Trésor américain d'autre part ont été initiés en 2007. Suite à l'avis favorable du juge Bruguière, un accord a été signé le 30 novembre 2009[1040]. Cet accord a été signé la veille de l'entrée en vigueur du traité de Lisbonne, il a donc échappé à la procédure de codécision. Cependant sa mise en œuvre, le 1er février 2010 pour une durée de 9 mois, a nécessité le vote d'un avis conforme du Parlement. La doctrine a critiqué un tel accord, ainsi que la procédure utilisée par la Commission et le Conseil pour échapper au nouveau pouvoir de codécision du Parlement[1041]. En effet, l'accord a été conclu en dépit de critiques du Parlement [1042] pour permettre aux États-Unis de continuer à accéder aux informations bancaires du réseau *Swift* dans le cadre de la lutte contre le terrorisme. Selon le texte de l'accord, l'UE permettrait à *Swift* de partager le nom, numéro de compte, adresse, numéro national d'identification et d'autres données personnelles avec les autorités américaines dans le cas de suspicion où la personne en question serait impliquée dans une activité terroriste. La demande d'information devait être limitée au strict nécessaire afin d'éviter que les données soient transférées de manière généralisée. Toutefois, si le fournisseur n'était pas capable pour des raisons techniques d'évaluer quelles données étaient pertinentes il avait l'obligation de transmettre toutes les données sans distinction. La durée de la conservation aux États-Unis était de cinq ans. L'accord *ad interim* du 30 novembre 2009 était lacunaire sous plusieurs aspects. Tout d'abord la transmission des données ne faisait pas l'objet d'un but déterminé permettant

1037 Parlement européen, Résolution législative du Parlement européen du 11 février 2010 sur la proposition de décision du Conseil relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme, P7_TA(2010)0029, Strasbourg, JO C 341 du 16 décembre 2010.

1038 Voy. WP 128, Avis 10/2006 du 22 novembre 2006, p. 22.

1039 Voy. La Resolution du Parlement européen du 6 juillet 2006 sur l'interceptation des données des virements bancaires du système Swift par les services secrets americains.

1040 Voy. Cons. UE, déc. n° 2010/16/PESC/JAI, 30 nov. 2009, relative à la signature, au nom de l'Union européenne, de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis d'Amérique aux fins du programme de surveillance du financement du terrorisme : JOUE n° L 8, 13 janv. 2010, p. 9 à 16.

1041 E. DE BUSSER, « EU data protection in transatlantic cooperation in criminal matters: Will the EU be serving its citizens an American meal ? », *Utrecht Law Review*, 2010, Volume 6, Issue 1p. 5.

1042 Voy. Résolution du Parlement du 17 septembre 2009.

un contrôle sur son opportunité[1043] , il prévoyait seulement la communication des paquets d'informations relatives à la série de transactions. De même, il faisait défaut sous le profil du principe de proportionnalité qui constitue une condition essentielle pour permettre une ingérence dans les droits fondamentaux. Ainsi, comme établi par la jurisprudence de la CEDH, « le pouvoir de surveiller en secret les citoyens n'est tolérable d'après la Convention que dans la mesure strictement nécessaire à la sauvegarde des institutions démocratiques (...). Les États contractants ne disposent pas pour autant d'une latitude illimitée pour assujettir à des mesures de surveillance secrète les personnes soumises à leur juridiction (...). Dans le contexte de l'article 8, cela signifie qu'il faut rechercher un équilibre entre l'exercice par l'individu du droit que lui garantit le paragraphe 1 et la nécessité, d'après le paragraphe 2, d'imposer une surveillance secrète pour protéger la société démocratique dans son ensemble des transferts massifs et indifférenciés de données ne satisfont certainement pas à cette exigence »[1044]. Cet accord devait entrer en vigueur en 2010 pour une durée de neuf mois en attendant que la Commission fasse une proposition pour la négociation en vue d'un accord permanent. Cet accord n'a pas vu le jour à cause du rejet le 4 février 2010 par la Commission pour les libertés civiles du Parlement et le CEDP, de son initiative, a envoyé une lettre à la Commission en soulignant à quel point le texte portait atteinte au droit à la protection des données personnelles. Selon le CEDP, rien ne laissait supposer que de telles mesures constituaient une ingérence nécessaire et proportionnée par rapport à d'autres moyens de contrôle déjà mis en place, de plus, il n'y avait aucune raison de limiter la protection des données personnelles, puisque contrairement à l'accord PNR, le responsable de traitement était installé dans l'UE et la législation européenne aurait dû s'appliquer dans son ensemble. Ainsi le 11 février 2010, la session plénière du Parlement rejetait l'accord TFTP. La motivation du rejet du Parlement portait sur le fait que l'accord n'offrait pas une protection satisfaisante, en particulier compte tenu de la prévision des transferts massifs de données et de l'absence de toute forme de contrôle par une autorité judiciaire indépendante, ainsi la légitimité des demandes de transmission du Département du Trésor des États-Unis ne pouvait pas être appréciée[1045]. Cet accord provisoire ayant une durée prévue de neuf mois, la Commission devait donc faire une proposition pour la négociation d'un mandat en vue d'un accord permanent. Cet accord n'a jamais vu le jour du fait que le Parlement a fait usage de son droit (acquis avec le traité de Lisbonne, art. 218 §6 TFUE) de refuser de donner un avis conforme[1046]. Un nouveau mandat de négociations a abouti à un nouvel accord signé par les États-Unis et l'UE le 28 juin 2010.

1043 A. PRÜM « Bataille politique autour de Swift : la lutte contre le terrorisme doit compter avec le respect de la vie privée », in Revue de Droit bancaire et financier n° 3, Mai 2010, p.9.

1044 A. PRÜM, précité p. 11-13.

1045 R. TURNER, *European Parliament Rejects Swift deal for sharing bank data with the US*, disponible sur le site http://www.dw.de/european-parliament-rejects-swift-deal-for-sharing-bank-data-with-us/a-5239595-1.

1046 Voy. La Recommandation A7-0013/2010 du parlement européen du 5 février 2010.

B. Le nouvel accord « TFTP »

134 Un accord plus équilibré. Suite au droit de veto par le Parlement, la Commission a publié, le 15 Juin 2010, une nouvelle proposition de décision relative à la conclusion d'un nouvel accord, baptisé « TFTP II »[1047]. Cette proposition, en plus de contenir le fruit des négociations avec les États-Unis présentait quelques-unes des indications du Parlement européen et visait à répondre aux préoccupations relatives à la protection des données personnelles. Selon la nouvelle proposition, la validité et la légitimité des demandes de transfert des États-Unis seraient évalués par Europol. De plus, il était envisagé la création d'un système européen équivalent au TFTP, afin de surmonter la nécessité d'un accord séparé avec les États-Unis avec l'application de mêmes règles. Le CEDP, dans son avis consultatif sur la proposition de décision relative à la conclusion du TFTPII[1048] , avait reconnu que le projet contenait des améliorations par rapport à l'accord intérimaire TFTP. Cependant, il a saisi l'occasion pour réitérer la nécessité de parvenir à un accord global avec les États-Unis en matière de protection des données personnelles dans le cadre de la coopération policière et judiciaire en matière pénale qui devrait remplacer les accords *ad hoc* déjà existants (PNR et TFTP)[1049]. Concernant le principe de proportionnalité, le CEPD a remarqué que, malgré les demandes du Parlement européen, la nouvelle proposition permettrait toujours le transfert massif de données. Un nouveau mandat de négociations a abouti le 28 juin 2010 à la signature de l'accord entre l'Union européenne et les États-Unis. Nonobstant les critiques, le 8 Juillet 2010, le Parlement européen a approuvé le nouvel accord TFTP II ce qui a permis son entrée en vigueur le 1er Août 2010[1050]. Cinq jours plus tard, le 13 Juillet 2010 le Conseil a finalement approuvé l'accord[1051]. La version finale de l'accord prévoit que les informations d'abord stockées sur le territoire de l'UE par les fournisseurs de services de communication financière peuvent faire l'objet de transferts vers le Département du Trésor des États-Unis sur demande et dans le seul but de prévention, d'enquête et poursuites du terrorisme et de son financement art. 1 et 3). Contrairement aux dispositions du TFTP I, la définition de terrorisme est calquée sur celle de la décision-cadre 2002/475 / JAI. L'art. 4 de l'Accord prévoit que les demandes du Département du Trésor américain soient analysées par Europol, à l'inverse ce qui avait été proposé par le CEDP, lequel aurait voulu une analyse de la part d'une autorité judiciaire. En effet Europol n'est pas une autorité de contrôle indépendante mais une prolongation de la police des États membres ayant un intérêt dans la collecte des données. Europol doit recevoir une copie de chaque demande du ministère

---

1047 Voy. 2010/412/: Décision du Conseil du 13 juillet 2010 relative à la conclusion de l'accord entre l'Union européenne et les États-Unis d'Amérique sur le traitement et le transfert de données de messagerie financière de l'Union européenne aux États-Unis aux fins du programme de surveillance du financement du terrorisme.

1048 Voy. l'avis du CEDP du 22 juin 2010, JO 2010/C/ 355/02.

1049 Voy. Avis du CEDP, du 22 juin 2010, JO 2010/C/ 355/02, points 7 et 8.

1050 L'accord Swift est valable pendant cinq ans jusqu'en août 2015. Il se prolongera automatiquement pour des périodes successives d'un an, sauf si l'une des parties informe l'autre, au moins six mois à l'avance, de son intention de ne pas prolonger l'accord.

1051 http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/fr/ecofin/115800.pdf.

américain des Finances et vérifier si les principes de l'accord *Swift* sont respectés[1052]. S'ils le sont, la société *Swift* est tenue de remettre directement les données financières au ministère américain des Finances. Le ministère doit alors enregistrer les données financières dans un environnement physique sécurisé de sorte que seuls des analystes enquê tant sur le terrorisme ou son financement puissent y accéder et les données financières ne doivent pas être interconnectées avec une quelconque autre base de données. De manière générale, les données financières reçues de *Swift* doivent être supprimées au plus tard cinq ans après leur réception. Les données financières qui sont pertinentes pour des enquê tes ou poursuites particulières peuvent ê tre conservées aussi longtemps qu'elles sont nécessaires pour les enquê tes ou poursuites en question. Des observateurs indépendants, notamment une personne nommée par la Commission européenne, contrô lent la conformité avec les principes de l'accord *Swift*. Les personnes concernées ont le droit d'obtenir confirmation de l'autorité européenne de protection des données compétente du respect de leur droit à la protection des données à caractère personnel et notamment le droit à la rectification, à l'effacement ou au verrouillage de leurs données collectées et enregistrées par le ministère américain. Toutefois, les droits d'accès des personnes concernées peuvent faire l'objet de certaines limitations légales. Lorsqu'un accès est refusé, la personne concernée doit être informée par écrit du refus et de son droit à former un recours administratif ou judiciaire aux États-Unis. Ainsi, un premier contrôle effectué en 2010 par l'Autorité de contrôle conjointe d'Europol, a mis en exergue le fait que les justifications écrites fournies étaient insuffisantes. Un second contrôle en 2012 a souligné les progrès, notamment dans la modification de la procédure consistant à attribuer un rôle formel et spécifique au délégué à la protection des données en ce qui concerne les injonctions de produire du Trésor américain. Quant au contenu de l'accord, dans l'article 5, les autorités américaines s'engagent à respecter les garanties quant à la sécurité et l'intégrité des données collectées, en particulier les données doivent être stockées dans un environnement sûr, séparées des autres données et non interconnectées avec d'autres bases de données. L'art 6 prévoit d'ailleurs un système de révision annuel de la part du Département du Trésor afin de déterminer les données qui ne sont plus nécessaires. Nonobstant les avancées de l'accord, de nouvelles préoccupations ont émergé en 2013 lorsque le Parlement a demandé la suspension de l'accord[1053], sans que cela n'ait eu d'effet. Les négociations transatlantiques témoignent d'un contexte diplomatique complexe. L'accord TFTP (*Terrorist Finace Tracking Programme*, programme de surveillance du financement du terrorisme) a révélé des divergences dans les approches en matière de protection des données. Si la doctrine européenne a critiqué l'accord TFTP, la doctrine américaine a critiqué l'attitude de l'Union Européenne, en soulignant comment celle-ci a cherché à imposer son modèle de protection. Ceci témoigne du difficile équilibre à trouver entre protection des données et lutte contre le terrorisme[1054]. Deuxièmement, l'accord est en mesure de frapper les citoyens européens puisque leurs données sont traitées sans leur consentement et

---

1052 L'autorité de contrô le commune d'Europol a effectué des vérifications sur les activités menées par Europol dans ce domaine, dont les résultats sont disponibles à l'adresse : http://europoljsb.consilium. europa.eu/reports/inspection-report.aspx?lang=en.

1053 Voy. la Recomandation du Parlement du 23 octobre 2013 sur la souspension de l'accord TFTP 2013/2831.

1054 G. ERCHOVE et A. WEYEMBERGH *Sécurité et justice : enjeu de la politique extérieure de l'Union européenne*, Bruxelles, Institut d'É tudes Européennes, É ditions de l'Université de Bruxelles, 2003, p. 195.

sans qu'ils soient au courant. Le ministère américain des Finances peut transférer des informations issues des données reçues de *Swift* à des organismes chargés de l'application de la loi, de sécurité publique ou de lutte contre le terrorisme, aux États-Unis ou à l'étranger, exclusivement pour la prévention ou la détection du terrorisme et de son financement ou pour les enquêtes ou poursuites en la matière. Lorsque le transfert sortant de données financières concerne un citoyen ou un résident d'un É tat membre de l'UE, tout partage des données avec les autorités d'un pays tiers requiert le consentement préalable des autorités compétentes de l'É tat membre concerné. Des exceptions sont possibles lorsque le partage des données est essentiel pour prévenir un danger grave et immédiat pour la sécurité publique, ce qui dans un contexte de lutte contre le terrorisme semble être plutôt la règle que l'exception [1055] . Au contraire, selon la doctrine européenne, l'accord *Swift* aurait mis en évidence un esprit de coopération insuffisant des États-Unis vis-à-vis de l'UE. En vérité, à l'époque du scandale *Swift*, il existait au niveau international des systèmes efficaces de coopération et de lutte contre le terrorisme qui pouvaient être mis en place dans le respect de la souveraineté des pays adhérents. Une bonne partie de la doctrine européenne reste ancrée à l'idée que la lutte contre le terrorisme ne devrait jamais être utilisée comme un prétexte pour limiter les droits fondamentaux[1056]. Ainsi l'accord *Swift* a montré des défaillances véritables dans le système de protection mis en place par la Directive 95/46/CE, qui se révèle être un instrument normatif insuffisant pour faire face aux enjeux et défis pour la protection des données personnelles[1057]. Les politiques de l'ELSJ sur la protection des données personnelles placent le citoyen au cœur de cet espace. Toutefois encore aujourd'hui, le rôle central est joué par la Commission, cela ne reflète pas la prise en considération des enjeux pour la protection des données personnelles. La meilleure réalisation des objectifs est le contrôle du juge européen, lequel n'hésite pas à remettre en cause les normes juridiques relatives à l'utilisation des données personnelles. L'accord signé avec les États-Unis n'étant pas réciproque, il ne profite qu'aux États-Unis, ce qui alimente la vision d'une Union européenne fragile sur le plan international. Même si la réforme lancée en janvier 2012 n'a pas eu d'impact sur l'accord « TFTP » signé en 2010, il est probable qu'un nouvel accord voit le jour. Est soulignée la nécessité de conclure un accord général en matière de coopération judiciaire et pénale comme en matière commerciale avec l'accord « *Privacy Shield* » qui a permis le transfert de données personnelles entre entreprises européennes et américaines.

§2. La spécificité du modèle de protection européen

1055 Voy. S. KIERKEGAARD, « Cloud State Surveillance: Dark Octopus Tentacle Clouds from the Atlantic », in M. GUPTA (eds) *Handbook of Research on Emerging Developments in Data Privacy*, IGI Publication. New York, 2014.

1056 M. GAUTIER, « Lutte contre le terrorisme et droits fondamentaux : le droit international sous la surveillance de la CJCE », *JCP G*., nov. 2008, p.45-46.

1057 Voy. S. KIERKEGAARD, précité.

135 L'approche de l'Union européenne dans la lutte contre le terrorisme. Si la jurisprudence *Kadi*[1058] a tempéré la politique de lutte contre le terrorisme menée par les États-Unis trop attentatoire aux droits fondamentaux, elle n'a pas entraîné d'infléchissement de la politique législative. Ainsi la nouvelle directive relative à la lutte contre le terrorisme présentée au lendemain des attentats de Paris, le 2 décembre 2015, et dont il faut souligner qu'elle n'a été accompagnée d'aucune étude d'impact (ce qui serait justifié selon la Commission par l'urgence), s'inscrit dans le droit chemin de la décision-cadre 2002/475/JAI telle que révisée en 2008 (que la directive a remplacé). Il faut rappeler que la décision-cadre avait été vivement critiquée notamment car elle imposait, à côté des « infractions terroristes » et des « infractions liées à un groupe terroriste », l'incrimination d'« actes préparatoires » se trouvant très en amont de la réalisation d'infractions terroristes[1059]. De plus, la Commission européenne a présenté le 17 avril 2018 dans un communiqué de presse une proposition de règlement dit « *e-evidence* »[1060], afin de rendre plus facile et plus rapide pour les autorités policières et judiciaires

1058 Une remarquable complexité caractérise les rapports entre les systèmes juridiques nationaux, régionaux et international, notamment au sujet de la mise en œuvre des résolutions adoptées au sein du Conseil de sécurité de l'Organisation des Nations unies (ci-après l'ONU), dans le cadre de la lutte contre le terrorisme. En effet, ces dernières ont pour effet de créer une présomption de culpabilité des personnes ou entités soupçonnées de participer à des activités terroristes, laquelle ne peut être renversée devant une juridiction nationale ou régionale, qu'au risque pour les États, de méconnaître les obligations qui leur incombent en leur qualité d'États parties à l'ONU. Dans l'arrêt *Kadi* de 2008, la Cour de justice de l'Union européenne a souligné l'importance des garanties procédurales qui doivent être consacrées dans lesdites résolutions, en annulant le règlement n° 881/2002, fondé sur la résolution 1390 (2000), pour violation du principe de protection juridictionnelle effective. En ce qui concerne la Cour européenne des droits de l'homme (ci-après la Cour EDH), l'on se rappelle de l'arrêt *Bosphorus* de 2005, où était en cause la violation par l'Irlande de la Convention européenne des droits de l'homme (ci-après la CEDH), en raison de l'exécution des obligations prévues dans le règlement n° 990/93, lui-même fondé sur la résolution onusienne 820 (1993). Au lieu d'apprécier la portée de la violation alléguée, la Cour EDH a préféré établir la présomption selon laquelle la protection des droits de l'homme dans l'Union européenne est équivalente à celle garantie par la CEDH. L'on a alors cru que l'arrêt *Bosphorus* a créé un précédent dans la jurisprudence de la Cour EDH, notamment pour les affaires où celle-ci serait amenée à apprécier la violation de la CEDH, engendrée par l'exécution des engagements internationaux des États parties à cette dernière. L'arrêt *Nada c. Suisse*, rendu en grande chambre le 12 septembre 2012, montre que la Cour EDH semble abandonner sa position dans l'arrêt *Bosphorus* pour suivre le raisonnement tenu par la Cour de justice dans l'arrêt *Kadi*.

1059 Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil, JOUE L 88/6 du 31/03/2017. La révision de 2008 introduit les incriminations de « provocation publique à commettre une infraction terroriste », le « recrutement » et l' « entraînement » pour le terrorisme, ainsi que la complicité de ces infractions et la tentative de les commettre.

1060 Voy. COM(2018) 225 final, disponible à l'adresse: https://ec.europa.eu/info/sites/info/files/placeholder.pdf Selon le projet, qui devra franchir toutes les étapes du processus législatif avant les élections du Parlement européen en 2019, la Commission européenne propose ainsi la mise en place des mécanismes suivants :la création d'une injonction européenne de production: elle devrait permettre à une autorité judiciaire d'un État membre de demander des preuves électroniques (telles que des courriels, des SMS ou des messages échangés dans des applications) directement auprès d'un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre, indépendamment de la localisation des données; ce prestataire sera alors tenu de répondre dans un délai de 10 jours, et dans les 6 heures en cas d'urgence (contre 120 jours pour la décision d'enquête européenne existante ou 10 mois pour une procédure d'entraide judiciaire) ; la création d'une injonction européenne de conservation, permettant d'empêcher l'effacement de données : elle devrait permettre quant à elle à une autorité judiciaire d'un État membre de contraindre un prestataire offrant des services dans l'Union et établi ou représenté dans un autre État membre à conserver certaines données afin que ladite autorité puisse demander ces informations ultérieurement par voie d'entraide judiciaire ou au moyen d'une décision d'enquête européenne ou d'une injonction européenne de production ; les mécanismes précédents doivent être assortis de la mise en place de garanties solides ainsi que de voies de recours: les deux types d'injonctions ne peuvent être émis que dans le cadre de procédures pénales, et toutes les garanties procédurales de droit pénal sont applicables. Les nouvelles règles garantissent l'intervention d'autorités judiciaires et posent des exigences supplémentaires pour l'obtention de certaines catégories de données. Elles comportent également des garanties concernant le droit à la protection des données à caractère personnel. Les prestataires de services et les personnes dont les données sont demandées bénéficieront de plusieurs garanties, parmi lesquelles la possibilité, pour le prestataire de services, de demander un examen si, par exemple, l'injonction constitue une violation manifeste de la charte des droits fondamentaux de l'Union européenne; une disposition du projet de règlement apparaît ensuite comme correspondant à l'effet extraterritorial du *Cloud Act*américain : il est en effet prévu de contraindre les prestataires de services à désigner un représentant légal dans l'Union. De la sorte, tous les prestataires qui proposent leurs services dans l'Union européenne seraient soumis à des obligations identiques,

l'obtention de preuves électroniques situées dans le *cloud* des fournisseurs de services afin d'enquêter, de poursuivre et de condamner des criminels et des terroristes, indépendamment de la localisation de ceux-ci sur le territoire européen, ce qui devrait concerner aussi des États tiers avec un effet d'extraterritorialité. Ce projet s'inscrit encore une fois dans un contexte de conflit transatlantique [1061]. En effet, le règlement « *e-evidence* » apparaît comme une réponse au « *Cloud Act* » promulgué par le Président américain Donald Trump le 23 mars 2018 [1062]. Toutefois, le projet de règlement européen *e-privacy* ne concerne pas seulement les métadonnées de communications (comme dans la directive 2006/24/CE invalidée par la Cour de justice dans l'arrêt *Data Retention*), mais aussi « le contenu des données », à savoir contenu des mails, vidéos, images, son, etc. Si le législateur européen tend ces dernières années à privilégier la sécurité et la lutte contre la criminalité, le difficile équilibre à atteindre entre sécurité et respect de la vie privée est assuré par la jurisprudence de la Cour de justice (A) et de la Cour européenne des droits de l'homme (B).

même si leur siège est situé dans un pays tiers. Le représentant légal dans l'Union désigné nécessairement par le prestataire de services assurerait ainsi la réception, le respect et l'exécution des décisions et injonctions émises par les autorités compétentes des États membres à des fins de collecte de preuves en matière pénale ; enfin, et cette disposition semble correspondre aux attentes des fournisseurs de service, comme l'affaire Microsoft le montre aux États-Unis, il est prévu de par ce nouveau texte de procurer une sécurité juridique aux entreprises et aux prestataires de services : actuellement, les autorités répressives sont tributaires du bon vouloir des prestataires de services à leur remettre les preuves dont elles ont besoin. Avec le nouveau règlement, s'il est adopté, les autorités et prestataires de services bénéficieront d'une plus grande sécurité juridique grâce à la mise en œuvre de règles identiques pour tous en matière de fournitures de preuves électroniques.

1061 Voy. la lettre de la Commission européenne dans l'affaire Microsoft auprès de la Cour Suprême américaine qui a porté à l'adoption du Cloud Act disponible à l'adresse : https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf. « Selon l'Union européenne, du point de vue du droit international public, lorsqu'une autorité publique demande à une société établie dans sa propre juridiction de produire des données électroniques stockées sur un serveur situé dans une juridiction étrangère, les principes de territorialité et de courtoisie en droit international public sont engagés, et les intérêts et les lois de cette juridiction étrangère doivent être pris en compte ».

1062 Pour aller plus loin Voy. : « Le projet de règlement « *E-evidence* » (preuves électroniques) présenté par la Commission européenne : un « Cloud Act » européen », disponible à l'adresse : http://www.gdr-elsj.eu/2018/04/24/droits-fondamentaux/le-projet-de-reglement-*e-evidence*-preuves-electroniques-presente-par-la-commission-europeenne-un-cloud-act-europeen/. Voy. The White Book: USA v. Microsoft: Quel Impact?, CEIS & The Chertoff Group White Paper (2017). Le point de départ se trouve dans une banale procédure judiciaire aux États-Unis dans une affaire de trafic de stupéfiants. Un juge américain a en effet ordonné en 2013 à la société Microsoft de lui livrer les emails d'un suspect, situés dans le *cloud*, le serveur étant en Irlande. Microsoft s'y est toutefois refusée, car la loi américaine de 1986 fondant l'injonction du juge (*Stored Communications Act*, SCA) n'avait pas d'effet extraterritorial selon elle. La Cour d'appel a confirmé ce point de vue, estimant que la loi SCA ne s'appliquait qu'aux données stockées sur le territoire des États-Unis. Le gouvernement américain a alors saisi la Cour Suprême en octobre 2017, cette dernière étant censée rendre son jugement en juin 2018. Entre temps, le Président américain Donald Trump a pris toutefois le juge de vitesse, en incluant le *Cloud Act* (*clarifying lawful overseas use of data act*) dans le projet de loi fédérale sur le budget 2018, soit 32 pages noyées dans plus de 2000 pages … Le Congrès avait déjà tenté à deux reprises de modifier la loi SCA de 1986, mais sans succès (projets de « Loi sur l'accès aux données stockées à l'étranger », LEADS Act, de 2015 et loi sur la protection des communications internationales, ICPA, en 2017). Cette importante loi a ainsi été adoptée sans examen spécifique, profitant de l'adoption globale de la loi de finances. Le Cloaud Act donne un cadre légal à la saisie par des agences gouvernementales (renseignement) ou des forces de police, d'emails, documents et communications électroniques localisés dans des serveurs de sociétés américaines à l'étranger (*cloud*). Doté clairement d'un effet d'extraterritorialité, il se présente comme une alternative extrêmement simplifiée au processus actuellement en vigueur quant au partage d'informations, basé sur le traité d'assistance mutuelle (MLAT : *mutual legal assistance treaty*). Dès lors qu'il permet aux différentes autorités intéressées un accès à tous les emails, conversations en ligne, photos et vidéos sur Facebook, Snapchat etc., il pose question quant à la protection des droits fondamentaux (protection des données à caractère personnel) du point de vue européen. La doctrine a remarqué comme le droit international offre aux États différentes possibilités leur permettant de trouver des solutions mutuellement acceptables, respectueuses de leur souveraineté et compatibles avec la protection des droits de l'homme au problème important de l'accès des services de justice aux preuves numériques lors d'une enquête pénale. Les États ont donc le choix entre un unilatéralisme hasardeux, prôné par le gouvernement américain devant la Cour Suprême, et la voie multilatérale qui a montré son efficacité à maintes reprises dans l'histoire du droit international.

A. La surveillance dans la jurisprudence de l'Union européenne.

136 La pondération entre droit fondamental à la protection des données et sécurité. L'arrêt *Digital Rights Ireland* marque l'affirmation d'une protection européenne des données personnelles, dans le contexte de l'espionnage de l'Europe par les États-Unis[1063]. Il s'agissait pour la Cour de justice d'arbitrer entre l'objectif de lutte contre le terrorisme et le respect de la vie privée. En effet, il a été observé que la directive 2006/24 est une « directive antiterrorisme »[1064] même si elle a été adoptée sur la base légale de l'ex-premier pilier, pour assurer le fonctionnement du marché intérieur. Ainsi la Cour de justice a précisé : « l'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique »[1065]. La Cour de justice établit tout d'abord que la rétention de données prévue par la directive 2006/24 constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 (vie privée) et 8 (protection des données personnelles) de la Charte qui s'avère « d'une vaste ampleur », « particulièrement grave » et « susceptible de générer dans l'esprit des personnes concernées (...) le sentiment que leur vie privée fait l'objet d'une surveillance constante »[1066]. Ainsi dans cette affaire, la Cour de justice annule dans son intégralité et avec effet *ex tunc* la directive 2006/24/CE sur la conservation de données notamment en raison de l'absence de critères objectifs permettant de délimiter l'accès des autorités compétentes aux métadonnées (données de communication, sans le contenu des communications) dont elle imposait la conservation aux opérateurs de services de télécommunication[1067]. Or, de tels critères auraient dû être définis afin de garantir qu'un tel accès ne soit possible qu'en lien avec l'objectif légitimement poursuivi de lutte contre les infractions graves et la criminalité[1068].

1063 CJUE (Grande chambre), 8 avril 2014, *Digital Rights Ireland Ltd*, aff. jointes C-293/12 et C-594/12. Sur ce point M.-L. BASILIEN-GAINCHE, « Une prohibition européenne claire de la surveillance électronique de masse », *La Revue des droits de l'homme*, 14 mai 2014, disponible à l'adresse : http://revdh.revues.org/746 ; également S. PEYROU, « La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel », RTDE, 2015, n°1, p. 117.

1064 V. N.VANDYSTADT, « Cour de justice : une directive antiterrorisme sur la sellette », *Europolitics*, n°4846, mardi 8 avril 2014, p. 8.

1065 C-293/12, *op. cit.*, pt 41. La détermination de l'objectif était particulièrement délicate puisque la Cour qui avait déjà eu à connaître de la directive 2006/24/CE avait considéré que son objectif « principal » était de protéger le bon fonctionnement du marché intérieur, et ainsi que la base légale appropriée était l'article 95 TCE (aujourd'hui 114 TFUE) dans son arrêt de Grande chambre *Irlande c/Parlement et Conseil* du 10 février 2009 2009 (C-301/06). L'avocat général parle ainsi de « dualité fonctionnelle » pour distinguer les différents objectifs de la directive. Voy. les conclusions de l'avocat général P. CRUZ VILLALÓN présentées le 12 décembre 2013, *in* C-293/12.

1066 CJUE, C-293/12, *op. cit.*,§ 37, voy. Également les conclusions de l'avocat général, pts 52 et 72.

1067 F. FERRETTI, « Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States », *Harvard Human Rights Journal* / Vol. 28, p.65-95, disponible à l'adresse : http://harvardhrj.com/wp-content/uploads/2009/09/human-rights-in-the-digital-age.pdf

1068 CJUE, Digital Rights Ireland Aff. C-293/12 et C-594/12, 8 avril 2014, § 60.

137 Les mesures nationales de conservation des données. L'affaire *Tele2 Sverige.* La Cour de justice a rappelé le raisonnement de l'arrêt *Digital Rights* dans l'affaire *Tele 2 Sverige*. Ici elle a précisé que l'invalidation de la directive 2006/24 avait une incidence dans les législations nationales de conservation des données[1069]. En effet, l'article 15 paragraphe 1 de la directive 2002/58/CE introduisait une disposition permettant aux États membres d'adopter des mesures imposant la conservation des données en vue de garantir la sécurité nationale, la défense et la sécurité publique. Dès lors, la Cour a affirmé que lesdites mesures nationales sont soumises au respect de la Charte des droits fondamentaux de l'Union européenne, et notamment ses articles 7 et 8[1070]. Elle donne des critères permettant d'apprécier la conformité d'une mesure nationale de conservation des données de communication et de localisation traitée par les fournisseurs de services de télécommunications électroniques avec le droit de l'Union : la mesure ne doit pas imposer une conservation « généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés » ; l'accès des autorités aux données conservées doit être limité « aux seules fins de lutte contre la criminalité » et soumis « à un contrôle préalable par une juridiction ou une autorité administrative indépendante » et les données doivent être conservées sur le territoire de l'Union européenne.

138 La nécessité de l'existence d'un recours effectif comme garde-feu. La Cour de justice s'est exprimée également de façon radicale sur la surveillance d'État dans l'arrêt *Schrems contre DPC Irlande*[1071]. Dans cette affaire elle a affirmé que l'existence d'un recours effectif auprès d'une juridiction ou d'une autorité indépendante capable de superviser la surveillance secrète des télécommunications, constitue un élément essentiel pour prévenir les abus d'une telle mesure. Par conséquent elle a annulé l'accord *Safe Harbor* puisque les États-Unis n'assuraient pas un niveau jugé adéquat de protection aux données personnelles transférées depuis l'Union européenne en raison de l'absence de recours juridictionnel pour les citoyens européens face aux programmes de surveillance des agences de renseignement américaines, dont le caractère massif et indiscriminé avait été révélé par Edward Snowden[1072]. Le Règlement général sur la protection des données (RGPD) ouvre de multiples possibilités pour engager une action en justice en cas d'atteinte aux données personnelles. Recours devant l'autorité de controle, action au pénal, assignation au civil. Lorsqu'elle estime que ses droits n'ont pas été respectés, une personne peut effectuer un recours RGPD devant l'autorité de contrôle de : l'État membre dans lequel se trouve sa résidence habituelle; son lieu de travail; le lieu où la violation aurait été commise. La personne concernée peut aussi effectuer ce recours en mandatant un organisme, une organisation ou une association à but non lucratif, dont les

1069 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15

1070 CJUE 21 décembre 2016 « Tele2 Sverige » Aff. C-203/15 et C-698/15, §. 73-78.

1071 Voy. le Chapritre I sur le trasfert dans les échanges commerciaux. CJUE 6 octobre 2015 « Schrems contre DPC Irlande » Aff. C-362/14.

1072 CJUE 6 octobre 2015 « Schrems contre DPC Irlande » Aff. C-362/14 §89.

objectifs statutaires doivent d'être d'intérêt public, et qui doit être actif dans le domaine de la protection des droits et des libertés des personnes concernées.

B. La surveillance dans la jurisprudence de la CourEDH

139 L'invocabilité de l'intérêt légitime à la sûreté de l'État, à la défense, ou à la sécurité publique. La CourEDH effectue un contrôle de l'ensemble des activités de surveillance d'État à des fins de sécurité et de police, sur la base de l'article 8 de la CEDH protégeant le droit à la vie privée. Au contraire, le contrôle de la Cour de justice ne peut avoir à connaître que des affaires relevant du domaine de compétence de l'Union[1073]. La CourEDH dans sa jurisprudence relève qu'une limitation du droit à la vie privée répond à l'intérêt légitime à la sûreté de l'État, à la défense, ou la sécurité publique. Toutefois, telles limitations doivent être prévues par la loi. Ainsi, dans l'affaire *Malone contre Royaume-Uni*[1074], la CourEDH a rappelé que la surveillance de la correspondance et les écoutes téléphoniques doivent être prévues par la loi, ce qui, en l'espèce, n'était pas le cas en raison de dispositions partielles et peu claires. Toutefois, plus tard, en 2010, dans l'affaire *Kennedy contre Royaume- Uni*[1075], la CourEDH a validé le régime britannique d'interception des télécommunications en raison de dispositions législatives suffisamment claires. La question de l'intérêt à agir a amené des divergences de jurisprudence.

En effet, comme rappelé au point 164 de l'arrêt *Roman Zakharov contre Russie*[1076] : « selon la jurisprudence constante de la Cour, la Convention ne reconnaît pas l'*actio popularis* et la Cour n'a pas normalement pour tâche d'examiner dans l'abstrait la législation et la pratique pertinentes, mais de rechercher si la manière dont elles ont été appliquées au requérant ou l'ont touché a donné lieu à une violation de la Convention ».
Selon la CourEDH, les mesures de surveillance secrète constituent l'exception puisque depuis l'arrêt *Klass et autres c. Allemagne* [1077] « un individu peut, sous certaines conditions, se prétendre victime d'une violation entraînée par la simple existence de mesures secrètes ou d'une législation permettant de telles mesures, sans avoir besoin d'avancer qu'on les lui avait réellement appliquées »[1078]. Cet arrêt a permis pour la première fois à la CourEDH d'affirmer

1073 En effet, dans l'arrêt Digital Rights Europe du 8 avril 2014, la CJUE a été amenée à analyser la compatibilité des programmes de surveillance de la National Security Agency des États-Unis au regard du droit européen à la protection des données. L'absence de garantie pour les citoyens européens des garanties minimales de protection de leur vie privée face aux programmes de surveillance de masse de la NSA ayant pour conséquence l'absence d'équivalence dans la protection des données entre les États-Unis et l'Union européenne, la CJUE a alors annulé la décision « *Safe Harbor* » permettant sous certaine condition le transfert de données personnelles depuis l'UE vers les États-Unis. De ce fait, matériellement, la CJUE ne s'est prononcée que sur une décision de l'Union relevant des compétences communautaires de celle-ci, mais a tout de même été amenée à énoncer un certain nombre de principes encadrant la surveillance d'État sur la base de la Charte des droits fondamentaux de l'Union européenne et de la Convention européenne des droits de l'homme.

1074 CEDH, Malone contre Royaume-Uni,, req. n° 8691/79, 2 août 1984, § 79.

1075 CEDH, Kennedy c. Royaume-Uni, req. n°26839/05, 18 mai 2010.

1076 CEDH, Roman Zakharov contre Russie, req. n° 47143/06, 4 décembre 2015 § 164.

1077 CEDH, Klass e. a. contre RFA, req. n° 5026/71, 6 septembre 1978.

qu'en matière de surveillance secrète, la charge de la preuve reposait sur l'État dont la mesure était attaquée. Par la suite, il y a eu deux conceptions de la qualité de victime dans des affaires de surveillance secrète qui se sont développées en parallèle et de façon contradictoire : dans certaines affaires, la CourEDH a considéré qu'il ne fallait pas interpréter l'arrêt *Klass et autres c. Allemagne* de façon extensive et ouvrir une possibilité de recours à toute personne souhaitant introduire un recours général contre une législation instaurant une surveillance généralisée des télécommunications[1079]. Dans *Kenney contre Royaume-Uni* [1080], la CEDH a confirmé qu'en matière de surveillance secrète, il fallait déroger à l'approche générale déniant aux particuliers le droit de se plaindre *in abstracto* d'une législation. En effet, elle a estimé qu'il fallait éviter que « le caractère secret de pareilles mesures ne conduisît [...] à ce qu'elles fussent en pratique inattaquables et qu'elles échappassent au contrôle des autorités judiciaires nationales et de la Cour »[1081] . La différence des approches adoptées par la CourEDH depuis l'arrêt *Klass et autres c. Allemagne* l'a amenée à préciser et unifier son approche dans l'arrêt *Roman Zakharov contre Russie*[1082], qu'elle cite désormais dans ses arrêts en lieu et place de l'arrêt *Klass e.a. contre Allemagne*[1083]. A partir de l'affaire *Roman Zakharov c. Russi*e, elle adopte l'approche issue de l'arrêt *Kennedy contre Royaume-Uni*, selon laquelle un requérant peut se prétendre victime d'une violation entraînée par la seule existence de mesures de surveillance secrète à condition que la législation attaquée puisse toucher le requérant[1084]. Par ailleurs, la CourEDH tient désormais compte de l'existence et effectivité de recours internes. En effet, la possibilité d'un recours interne est une garantie contre le pouvoir discrétionnaire dont dispose l'exécutif en matière de surveillance d'État. Dans l'affaire *Szabó and Vissy contre Hongrie*, elle a jugé que l'obligation d'autorisation par un membre de l'exécutif autre que le ministre de l'Intérieur (en l'espèce le ministre de la Justice) des demandes de mise sur écoute, formulées par les services de renseignement ou de police compétents, ne remplit pas le critère d'indépendance indispensable pour garantir la stricte nécessité d'une telle mesure[1085], surtout en l'absence de toute possibilité de recours judiciaire.

140 Les garanties de fond visant à justifier la surveillance. L'affaire *Szabó and Vissy contre Hongrie*. Dans l'arrêt *Szabó and Vissy contre Hongrie,* la CourEDH a rappelé un principe déjà affirmé dans *Dumitru Popescu c. Roumanie*[1086] : lorsque l'autorisation de procéder à des écoutes n'est pas octroyée par une autorité indépendante de l'exécutif, ces mesures doivent

1078 CEDH, Klass e. a. contre RFA, req. n° 5026/71, 6 septembre 1978 §. 34 à 38 (la jurisprudence Klass et autres ayant été amendées par la décision Roman Zakharov contre Russie, l'étude de ces conditions n'a cependant plus qu'un intérêt d'ordre historique).

1079 CEDH, Roman Zakharov contre Russie, Aff. 47143/06, 4 décembre 2015 §167 et 168.

1080 CEDH, Kennedy contre Royaume-Uni, Aff.n° 26839/05, 18 mai 2010.

1081 CEDH, Kennedy contre Royaume-Uni, Aff. 26839/05, 18 mai 2010,§ 124 et CEDH, Roman Zakharov contre Russie Aff. n° 47143/06, 4 décembre 2015 § 169.

1082 CEDH, Roman Zakharov contre Russie, Aff. n°47143/06, 4 décembre 2015, §170.

1083 CEDH, Šantare et Labaņ ikovs contre Lettonie, Aff. n°34148/07, 31 mars 2016, § 53.

1084 CEDH, Roman Zakharov contre Russie, Aff. n°47143/06, 4 décembre 2015 § 171.

1085 CEDH, Szabó and Vissy contre Hongrie, Aff. n°37138/14, 12 janvier 2016, § 75.

1086 CEDH, Dumitru Popescu c. Roumanie, Aff. n° 71525/01, 26 avril 2007.

pouvoir être contestées devant un juge ou une autre forme d'autorité indépendante[1087]. Si de telles garanties ne sont pas apportées, cela constitue une violation de l'article 3 CEDH. Cependant, selon la CourEDH, des mécanismes de contrôle *ex post* peuvent aussi justifier d'un allègement des procédures *ex ante* [1088] . La collecte de données, y compris dans le cadre d'enquêtes pénales, doit respecter le principe de limitation des finalités : seules les données personnelles nécessaires à l'objet de l'enquête doivent être collectées et conservées[1089]. Ce principe implique aussi que la surveillance ne soit pas une surveillance de masse. Les mises sur écoute doivent correspondre bel et bien aux nécessités d'une enquête et doivent être ciblées[1090]. De plus, la CourEDH a énoncé le principe de proportionnalité consistant à vérifier, avant la mise en œuvre d'une mesure de surveillance, si une mesure moins invasive de la vie privée de la personne concernée permettrait d'atteindre la finalité poursuivie. Si tel est le cas, la solution alternative moins intrusive devra toujours être préférée[1091].

1087 CEDH, Dumitru Popescu contre Roumanie, n° 49234/99, 26 avril 2007, § 70-73.

1088 CEDH, Kennedy contre Royaume-Uni, n°26839/05, 18 mai 2010, § 167, cité par : CEDH, Szabó and Vissy contre Hongrie, Aff. 37138/14, 12 janvier 2016, § 77.

1089 CEDH, Robathin c. Autriche n° 30457/06, 3 juillet 2012, § 52.

1090 CEDH, Szabó et Vissy c. Hongrie n° 37138/14, 12 janvier 2016 et CEDH 4 décembre 2015 Zakharov contre Russie, n° 47143/06.

1091 CEDH, Uzun c. Allemagne, n°35623/05, 2 septembre 2010, § 78.

CONCLUSION DU CHAPITRE II

Après avoir étudié l'échange des données dans un but économique, il a été possible de souligner à quel point l'échange des données pour des finalités de coopération pénale peut sembler problématique sur le plan du respect des droits et libertés.

L'analyse du présent Chapitre peut se résumer à deux aspects : la protection des droits fondamentaux (notamment la protection des données à caractère personnel)[1092] et les relations entre l'Union européenne et les pays tiers, principalement avec les États-Unis. Ainsi il est possible d'affirmer que l'espace pénal européen constitue à la fois un instrument pour l'Union afin d'exporter son modèle dans le monde et un objectif.

La dimension « sécuritaire » externe s'impose comme un outil de contrôle social et de crédibilité de l'Union en tant qu'instance de pouvoir. Toutefois, le succès de la politique sécuritaire de l'Union européenne dépend largement de la coopération avec les partenaires internationaux[1093]. Ainsi les divergences conceptuelles et politiques entre Union européenne et États-Unis ont mené à un « conflit transatlantique ». Le chapitre a mis en évidence les résultats obtenus ces derniers années grâce à une véritable politique législative étrangère de l'Union européenne[1094]. Ainsi le cadre harmonisé du droit fondamental à la protection des données personnelles a un effet extraterritorial et constitue un modèle pour certains pays tiers. Cependant, la politique sécuritaire de l'Union européenne a été plusieurs fois pointée du doigt [1095] , ces critiques trouvent leur base dans l'absence d'une véritable politique pénale supranationale. En effet, il a été observé que la construction du droit pénal de l'Union a été une démarche «*casuistique*», *intuitive*, se traduisant par un « *empilement institutionnel et normatif sans harmonie d'ensemble »*, par une approche « *ad hoc et éclectique »*[1096]. De plus, dans les deux affaires (PNR et *Swift*) l'administration américaine en opposition avec l'ordre de droit européen, a imposé aux entreprises de se faire remettre des informations qui violent la vie privée des citoyens. Cela est exemplaire de la thèse de Carl Schmitt, selon laquelle «est souverain,

---

[1092] Voy. Maria Tzanou, *The Added Value of Data Protection as a Fundamental Right in the EU Legal Order in the Context of Law Enforcement* (2012) (unpublished Ph.D. thesis, European University Institute).

1093 D. FAYON, « Géopolitique d'Internet, Qui gouverne le monde ? », *Economica*, mars 2013.

1094 Voy. la Thèse de L. FAVERO, *La dimension externe de la protection des données à caractère personnel dans le droit de l'Union eur*opéenne, Soutenue le 27-05-2013 à Strasbourg en cotutelle avec l'Università degli studi (Bologne, Italie), dans le cadre de École doctorale Droit, science politique et histoire (Strasbourg), en partenariat avec Centre d'études internationales et européennes (Strasbourg) (équipe de recherche Sous la direction de Fabienne Kauff-Gazin et de Lucia Serena Rossi.

1095 Voy. Notamment D. BIGO, *Liberty, whose Liberty ? The Hague Programme and the Conception of Freedom,* in S. CARRERA et T. BALZACQ (dir.), *Security versus Freedom. A challenge for Europe's future*, Ashgate Publishing, 2006, pp. 35-44; S. DE BIOLLEY, *Liberté et sécurité dans la construction de l'espace européen de justice pénale : cristallisation de la tension sous présidence belge* in G. DE KERCHOVE et A. WEYEMBERGH (dir.), *L'espace pénal européen : enjeux et perspectives*, éd. de l'Université de Bruxelles 2003, pp. 169-198 ; A. WEYEMBERGH, *L'espace pénal européen : "épée" des droits fondamentaux dans l'Union européenne* », in *Les droits de l'homme, bouclier ou épée du droit pénal ?*, 2007., pp. 175-209 ; A. WEYEMBERGH, *L'impact du 11 septembre sur l'équilibre sécurité/liberté dans l'espace pénal européen*, in E. BRIBIOSA et A. WEYEMBERGH (dir.), Lutte contre le terrorisme et droits fondamentaux, Bruylant, 2002, pp. 153-195.

1096 J.A.E. VERVAELE, « Harmonised Union policies and the harmonisation of substantive criminal law », *in* F. GALLI et A. WEYEMBERGH (dir.), *Approximation of substantive criminal law in the EU. The way forward*, éd. de l'Université de Bruxelles, 2013, pp. 43-71, sp. p. 57.

celui qui décide d'une situation exceptionnelle »[1097]. Dans l'accord PNR et *Swift*, le pouvoir exécutif américain réaffirme son droit de disposer des données personnelles des ressortissants européens. Le rôle de l'Union européenne se limite à en aménager l'exercice[1098]. Afin de montrer sa bonne volonté, l'autorité américaine, dans une démarche unilatérale, concède des « garanties » formelles, qu'elle peut unilatéralement modifier ou supprimer. Le défi pour l'Union européenne est de garantir le juste équilibre entre la protection de la vie privée avec la sécurité qui figurent parmi ses valeurs et principes, tant sur le plan interne que sur le plan externe. La réponse de l'Union européenne doit donc être globale et reposer sur un ensemble cohérent de mesures combinant dimension intérieure et dimension extérieure pour resserrer les liens entre, d'une part, Justice et Affaires intérieures et, d'autre part, la politique de sécurité et de défense commune. Ainsi l'accord spécial conclu entre l'Union européenne et les États-Unis pour encadrer des transferts de données des passagers aériens (PNR) à des fins de sécurité a justifié la conclusion d'autres accords de la même nature avec d'autres États tiers. De plus, l'adoption au niveau européen d'une directive PNR montre la conviction de l'efficacité du dispositif PNR dans la lutte contre le terrorisme mais il ne faut pas oublier que le débat sur l'opportunité de la directive PNR a été réactivé suite aux attentats de Paris de janvier 2015[1099]. Toutefois, l'avis contraire de la Cour de justice vis-à-vis d'une nouvelle conclusion d'accord PNR avec le Canada marque un changement d'orientation. Ainsi la jurisprudence de la Cour de justice en matière de protection des données personnelles dans sa dimension externe confirme le rôle stratégique que ce droit représente pour l'Union européenne. Il serait possible même de parler d'arrêts politiques, qui anticipent les choix du législateur et lui donnent des indications dans l'élaboration des actes juridiques[1100]. L'affaire *Schrems* a sûrement influencé la décision Zakharov[1101] et la décision Szabo [1102] dans lesquelles la CourEDH insiste sur les garanties accordées aux citoyens européens contre les abus de la surveillance secrète. Il est possible de constater que malgré les efforts, face aux pressions sécuritaires, tant l'accord PNR que l'accord *Swift* sont le fruit d'un compromis. Afin d'assurer un système européen complet de sécurité, l'Union européenne doit travailler à une plus grande cohérence et uniformité pour assurer la meilleure protection des données possibles en adéquation avec sa lutte contre le terrorisme.

1097 C. SCHMITT, *Théologie politique*, Gallimard, Paris, 1988, p. 15.

1098 J.-C. PAYE, La fin de l'État de droit, La Dispute, Paris 2004, p.156-160.

1099 Voy. le communiqué du G29 du 5 février 2015, Déclaration sur la mise en place d'un système PNR européen.

1100 Si l'on pense par exemple à l'affaire *Google Spain* et la codification du droit à l'oubli dans le nouveau règlement 679/2016, au champ d'application territorial élargi du règlement ou encore à l'avis négatif de la Cour de justice vis-à-vis de l'accord pnr avec le Canada.

1101 Cour. EDH, Gr. Ch., 4 décembre 2015, Zakharov c. Russie, Req. N°47143/06. L'affaire concernait un journaliste et éditeur qui avait pris une action en justice affirmant que ses communications téléphoniques avaient été soumis aux fins d'empêcher l'écoute clandestine des activités terroristes. En conséquence d'un ordre de gouvernement, en fait, les opérateurs de télécommunications ont été obligés d'installer des dispositifs qui permettent la captation communications par l'Agence pour la sécurité nationale en l'absence d'une mesure d'autorité judiciaires dans les deux ensembles de procédures, cependant, l'éditeur a été les résultats Bente échoué car il n'a pas été en mesure de prouver qu'il avait effectivement subi les conséquences de la mise en œuvre d'un système de surveillance de masse. La Grande Chambre estime que dans ce cas, il y avait une violation du droit consacré par l'art. 8 de la Convention. Selon la Cour, l'existence d'une menace de caractère massif suffit à envisager la violation du droit à la vie privée consacré par l'art. 8 de la Convention.

1102 Cour EDH, 5e sect., 12 janvier 2016, Szabo c. Hongrie, Req.n°37138/14.

Cependant, le *Cloud Act* américain a manifestement pour objet de produire un effet extraterritorial. Selon cette logique, des données personnelles situées par exemple sur le sol français et concernant des citoyens français pourraient être adressées aux autorités répressives américaines, sur simple demande de celles-ci au fournisseur de services américain disposant d'un *datacenter* sur le territoire français. Dès lors, le risque de mimétisme [1103] semble aujourd'hui se concrétiser par la présentation du projet de règlement européen *e-evidence*. Le sujet est donc loin d'être épuisé, et l'avenir du traitement des données en matière pénale est relativement incertain. Ilsemble que seule l'action politique de la Cour de justice peut mener à l'affirmation du modèle européen sur la scène internationale, ce qui fait réfléchir sur l'effectivité du modèle.

1103 T. CHRISTAKIS, « Data, Extraterritoriality and the Need for International Law Solutions to Transatlantic Law Enforcement Issues, Legal Opinion on the Microsoft Ireland Case », *CEIS & The Chertoff Group White Paper 2017*, disponible à l'adresse : https://ceis.eu/wp-content/uploads/2017/12/Whitepaper_EN_WEB.pdf.

CONCLUSION DU TITRE II

L'analyse a permis de souligner les divergences conceptuelles et politiques entre Union européenne et États-Unis qui ont mené à un « conflit transatlantique », d'une part dans le secteur privé[1104] avec l'approbation de l'accord sur le transfert des données dit « *Safe Harbor* », annulé et remplacé par le « *Privacy Shield* », d'autre part, dans la coopération pénale avec la mise en œuvre d'accords visant à lutter contre le terrorisme (accords PNR et *Swift*). Cette analyse a permis de vérifier le niveau de protection offert aux données personnelles dans leur dimension externe et de qualifier l'action de l'Union européenne comme une politique étrangère ayant comme but d'exporter son standard de protection. Encore une fois c'est la Cour de justice qui a permis une juste pondération entre d'une part, des intérêts économiques et les exigences de sécurité publique et de l'autre, la protection des droits fondamentaux. Ainsi à l'échelle mondiale, l'Europe constitue une sorte de « village gaulois » dans la mesure où son modèle de protection reste très spécifique voir maximaliste[1105]. Dans sa dimension externe, l'Union européenne face à la multiplication des transferts des données personnelles [1106], a élaboré une réglementation juridique spécifique qui ne cherche pas à supprimer les risques liés à la multiplication de l'utilisation des données personnelles, mais plutôt à les maîtriser[1107]. En principe, pour pouvoir transférer les données vers un État tiers la condition d'un niveau « adéquat » de protection dans le pays destinataire est requise. Néanmoins, il existe des dérogations permettant le transfert de données à caractère personnel dans des circonstances spécifiques, même lorsque ni un niveau de protection adéquat ni des garanties appropriées ne sont en place. Le règlement 679/16 a reproduit ce schéma, ce qui montre son efficacité. Toutefois, l'Union européenne cherche à exporter son modèle de protection, cela se heurte à des divergences conceptuelles qui dérivent d'une approche différente. En effet, si certains États ont compris l'enjeu démocratique du problème et se sont munis d'une réglementation spéciale, qu'il s'agisse d'Israël, de l'Argentine ou de l'Inde, d'autres comme la Chine, la Nouvelle-Zélande, l'Australie et les États-Unis[1108] ne disposent à ce jour d'aucune protection spécifique. Ainsi aux États-Unis, le *Privacy Act* de 1974 ne concerne que les données traitées par le gouvernement fédéral, ce qui rend cette législation dépourvue de portée générale puisqu'elle ne s'applique pas aux États fédérés [1109]. De plus, la Constitution fédérale ne prévoit pas

---

1104 J. REIDENBERG, « E-Commerce and Trans-Atlantic Privacy », in *38 Hous. L. Rev.*2001, p. 717-728 (2001); F. BIGNAMI, G. RESTA « Transatlantic Privacy Regulation: Conflict and Cooperation », *in Law and Contemporary Problems*, 2015, p.231-266.

1105 G. DESGENS -PASANAU, *La protection des données personnelles*, LexisNexis, 2016, p.200.

1106 Voy. dans la doctrine américaine A. F. WESTIN, *Privacy and Freedom*, Atheneum, 1970, p.487 ; Dans la doctrine française G. BRAIBANT, *La protection des droits individuels au regard du développement de l'informatique*, RIDC, 1971, pp. 793 et s. ; B. CHENOT (dir.), *Rapport de la Commission informatique et libertés*, La Documentation française, 1975, 106 p. ; F. GALLOUEDEC -GENUYS, H. MAISL, *Le secret des fichiers*, Ed. Cujas, 1976, p.328.

1107 A. TURK, *La vie privée en péril. Des citoyens sous contrôle*, Odile Jacob, Paris, 2011, p. 272.

1108 Dans ce dernier pays, les données à caractère personnel sont présumées utilisables tant que la personne ne s'y est pas explicitement opposée.

expressément la protection des données personnelles, cette dernière est garantie par le biais d'une législation sectorielle et fragmentaires avec des différences entre le secteur public et privé (et notamment à travers la *self-regulation* des entreprises)[1110]. A la différence du cadre juridique de l'UE, il n'existe au niveau fédéral aucun organe de contrôle indépendant visant à assurer la protection des données personnelles[1111].

****

CONCLUSION DE LA PARTIE I

L'analyse de l'existence d'une politique interne et externe en matière de données personnelles a apprécié le degré de protection offerte par l'Union européenne et sa cohérence entre la protection offerte au niveau interne, et celle offerte au niveau externe. Toutefois, si l'Union européenne a réservé au droit à la protection des données personnelles une attention particulière dans sa dimension interne[1112], il en ressort que dans sa dimension externe son effectivité connaît des limites. Dans le droit de l'Union européenne, la protection des données à caractère personnel est un droit fondamental, proclamé, et garanti par l'article 8 de la Charte des droits fondamentaux et désormais inscrit au rang de source primaire grâce au Traité de Lisbonne. L'Union européenne dispose également d'une législation substantielle en la matière, dont la directive 95/46/CE a constitué le cœur. Toutefois, la mise en œuvre de la directive 95/46 dans chaque État membre a donné lieu à des différences significatives qui se traduisent par la pratique de *forum shopping*, consistant pour certaines entreprises internationales à établir leur siège dans l'État de l'Union européenne disposant de la législation la moins contraignante. Cette hétérogénéité a posé un problème d'insécurité juridique pour les personnes qui ne disposent pas du même niveau de protection et pour les entreprises internationales qui devaient concilier des règlementations nationales contradictoires[1113]. La refonte de la législation tient d'une part, à garantir la meilleure exploitation possible du marché numérique et d'autre part à garantir un niveau élevé de protection des données personnelles. Nos sociétés sont de plus en plus numérisées. Le rythme des développements technologiques et la façon dont les données personnelles sont traitées affectent chacun de nous chaque jour et de toutes sortes de manières

1109 P. SCHWARTZ, « Data Processing and Government Administration: The Failure of the American Response to the Computer », in L.J. HASTING, Disponible à l'adresse : http://scholarship.law.berkeley.edu/facpubs/987 http://scholarship.law.berkeley.edu/facpubs/987.

1110 J.Q. WHITMAN, « The Two Western Cultures of Privacy: Dignity Versus Liberty », 113 *Yale L. J.*, 2014, p. 115.

1111 P.M. SCHWARTZ, « The EU-U.S. Privacy Collision: A Turn to Institutions and Procedures », in *126 Harvard L. Rev.* 1966, 1974-1979 (2013).

1112 Toutefois cette cohérence n'est pas totale puisque on remarque la permanence de deux instruments juridiques un pour ce qui relève du marché intérieur et l'autre pour l'ELSJ.

1113 CJUE, *Google Spain* SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12, 13 mai 2014.

à la lumière de ces changements. Les cadres juridiques de l'Union européenne (UE) et du Conseil de l'Europe qui protègent la protection de la vie privée et des données personnelles ont récemment été revus. Ainsi la directive 95/46/CE a été remplacée par le nouveau règlement 679/16. À cet égard depuis la constitutionnalisation de la Charte des droits fondamentaux de l'Union européenne, la Cour de justice a joué un rôle décisif dans l'évolution de ce droit. Dans des arrêts historiques elle a montré une tendance très nette à l'émancipation de son raisonnement vis-à-vis de celui de la CourEDH qui l'a pourtant longtemps inspirée. Désormais la Cour de justice peut s'appuyer sur une Charte de rang primaire et assurer la protection du droit fondamental à la protection de la vie privée. Ainsi la Cour de justice, avec ses dernières décisions *Google Spain*[1114] , *Data Retention*[1115] et *Schrems*[1116] , a marqué le passage d'une dimension économique à une dimension constitutionnelle du droit à la protection des données personnelles [1117] en faisant prévaloir le droit fondamental à la protection des donnée personnelles sur d'autres intérêts économiques et sécuritaires. C'est dans ce contexte que le législateur est intervenu avec un chantier de réformes qui a abouti à l'adoption du règlement 679/16 et de la directive 680/16. Le mérite est sans doute l'uniformisation des législations et une meilleure protection pour les personnes grâce à des principes renforcés et à des nouveaux droits. Toutefois des critiques peuvent déjà être soulevées quant au fait du choix de garder deux instruments législatifs séparés pour les matières relevant de l'ex-premier pilier et l'ex-troisième pilier. Une fois assuré la protection des données dans la dimension interne, l'Union européenne est intervenue à l'échelon externe puisque le partage d'informations sur les personnes s'accélère et s'amplifie[1118]. Le transfert des données vers des pays tiers est encadré par des règles strictes et par la conclusion d'accords internationaux. Le but est d'assurer un niveau de protection « adéquat » au données personnelles lorsqu'elles sont transférées. Les raisons du transfert sont tant de nature économique que politique. Toutefois, les pays tiers ont une approche plus souple et très peu d'entre eux sont considérés par la Commission européenne comme disposant d'un niveau de protection « adéquat » au standard européen. Encore une fois, c'est la Cour de justice qui, suivant le *trend* de l'affaire *Digital Rights Irelan*d[1119], a établi un équilibre entre protection des données personnelles et intérêt général à la sûreté nationale[1120].

1114 CJUE, *Google Spain* SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12, 13 mai 2014.

1115 CJUE, Digital Rights Ireland Ltd c. Minister for Communications, aff. Jointes C-293/12 e C-594/12, 8 avril 2014

1116 CJUE, Gr.Ch, Maximilian Schrems c. Data Protection Commissioner Ireland, aff. C-362/14, 6 octobre 2015.

1117 G. FINOCCHIARO, *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems*, In Diritto dell'informazione e dell'informatic, 2016, p. 383 et s.

1118 D. BIGO, R.B.J. WALKER, « Le régime du contre-terrorisme global », in D. BIGO, D. BONELLI, L. DELTOMBE D., (dir.), *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, Paris, La Découverte, 2008, p. 13-35.

1119 CJUE, aff. jointes C-293/12 et C-594/12, Digital Rights Ireland, Seitlinger e a. 8 avril 2014. l est remarquable de noter que la Cour de Strasbourg a, elle aussi, opéré une condamnation stricte de la surveillance de masse dans son arrêt Zakharov de décembre 2015 et son arrêt Szabo de janvier 2016, tout en élargissant le statut de « victime » en matière de surveillance.

1120 Dans sa communication au Parlement européen et au Conseil relative au fonctionnement de la sphère de sécurité du point de vue des citoyens de l'Union et des entreprises établies sur son territoire COM(2013) 847 final, la Commission avait déjà conclu que «l'accès à grande échelle des agences de renseignement aux données que des entreprises certifiées au titre de la

Afin d'assurer les rapports commerciaux et établir une politique étrangère basée sur le flux de données personnelles, l'Union européenne et les États-Unis ont conclu des accords tant dans le secteur privé que dans le secteur public au point de faire parler de *Brussels effect*[1121]. Toutefois, les révélations d'Edward Snowden dans le scandale *Prism* ont montré la fragilité de tel accord puisque les autorités américaines pouvaient accéder aux données des citoyens européens détenues par les sociétés américaines et notamment les GAFAM (Google, Amazon, Facebook, Microsoft). La Cour de justice est alors intervenue comme véritable gardienne des droits fondamentaux dans l'affaire *Schrems*, invalidant la décision de la Commission et l'accord du Conseil sur lesquels se basait le *Safe Harbor* [1122] en imposant un niveau de protection substantiellement équivalent à celui de l'Union.

L'affaire *Schrems* a eu des conséquences économiques car elle a obligé l'Union européenne et les États-Unis à renégocier rapidement un nouvel accord avec des plus amples garanties pour les données personnelles. C'est dans ce contexte que l'accord *Privacy Shield* a vu le jour. Ainsi les standards européens en matière de protection des droits fondamentaux (protection des données) imposent certaines limites et garanties, notamment celles d'un « niveau de protection adéquat » ou « substantiellement équivalent » comme l'a indiqué la Cour de justice. Cette véritable politique étrangère de l'Union européenne est l'expression de son identité. A travers

---

sphère de sécurité transfèrent aux États Unis soulève de graves questions sur la continuité de la sauvegarde des droits des citoyens européens en matière de protection des données lorsque des données les concernant sont transférées aux États Unis». Voy. sur ce point M. SCHEININ, *The Essence of Privacy, and Varying Degrees of Intrusion*, disponible à l'adresse : www.verfassungsblog.de, 7 ottobre 2015; R. MILLER, *Schrems v. Commissioner: A Biblical Parable of Judicial Power* »,ivi, 7 ottobre 2015; C. KUNER, *The Sinking of Safe Harbor* , 8 october 2015, disponible à l'adresse : https://verfassungsblog.de/the-sinking-of-the-safe-harbor-2/; O. LYNSKEY, *Negotiating the Data Protection Thicket: Life in the Aftermath of Schrems*, 9 ootber 2015, disponible à l'adresse : https://verfassungsblog.de/negotiating-the-data-protection-thicket-life-in-the-aftermath-of-schrems-2/; S. PEERS, *The party's over: EU data protection law after the Schrems Safe Harbor judgment*, disponible à l'adresse *:* www.eulawanalysis.blogspot.it, 7 october 2015; S. RODOTA, *Internet e privacy, c'è un giudice in Europa che frena gli Usa*, 1 octobre 2015, disponible à l'adress : in www.repubblica.it,; M. BASSINI, O. POLLICINO, *La Corte di giustizia demolisce il safe harbor e ridisegna i confini del diritto alla privacy in ambito transnazionale*, 7 octobre 2015, disponible à l'adresse www. diritto24.ilsole24ore.com.

1121 A. BRADFORD, « The Brussels Effect », 107 *N.W. U. L. Rev.* 1, 2012, p. 22-26.

1122 L'accord *Safe Harbor* se basait sur une autocertification des entreprises américaines qui voulaient adhérer à la « sphère de sécurité ». Pour autocertifier son adhésion à la 'sphère de sécurité', une organisation peut remettre au ministère américain du commerce (ou à la personne désignée par celui-ci) une lettre signée d'un cadre de ladite organisation contenant au moins les informations suivantes: le nom de l'organisation, son adresse postale, son adresse électronique, ses numéros de téléphone; une description des activités de l'organisation relativement aux informations à caractère personnel en provenance de l'Union européenne; une description des dispositions de protection de la vie privée appliquées par l'organisation auxdites informations, précisant: a) le lieu où le texte de ces dispositions peut être consulté par le public; b) la date de mise en œuvre de ces dispositions; c) le service à contacter en cas de plainte, pour des demandes d'accès et pour toute autre question relevant de la 'sphère de sécurité'; d) le nom de l'instance réglementaire spécifique qui est chargée de statuer sur les plaintes déposées, le cas échéant, contre l'organisation pour pratiques déloyales ou frauduleuses et pour infraction aux lois ou aux réglementations régissant la protection de la vie privée (et qui est mentionnée dans l'annexe aux principes); e) l'intitulé de tout programme relatif à la protection de la vie privée auquel participe l'organisation; f) la méthode de vérification (par exemple, en interne ou par des tiers) [...] et g) l'instance de recours indépendante qui pourra instruire les plaintes non résolues. Le 27 novembre 2013, la Commission a adopté la communication au Parlement européen et au Conseil, intitulée « Rétablir la confiance dans les flux des données entre l'Union européenne et les États Unis d'Amérique » [COM(2013) 846. Comme indiqué au point 2, de la communication « les données à caractère personnel des citoyens de l'Union transférées aux États Unis dans le cadre de la sphère de sécurité peuvent, en effet, être consultées et traitées par les autorités américaines d'une manière incompatible avec les motifs pour lesquels elles avaient été initialement collectées dans l'Union et avec les finalités de leur transfert vers les États Unis» et que « la majorité des entreprises américaines du secteur de l'Internet, qui semblent être plus directement concernées par les programmes de surveillance, sont certifiées dans le cadre de la sphère de sécurité». En outre, elle a indiqué, à ce même point 2, que «les données à caractère personnel des citoyens de l'[Union] transférées aux États Unis dans le cadre de la sphère de sécurité peuvent, en effet, être consultées et traitées par les autorités américaines d'une manière incompatible avec les motifs pour lesquels elles avaient été initialement collectées dans l'Union et avec les finalités de leur transfert vers les États Unis» et que «la majorité des entreprises américaines du secteur de l'Internet, qui semblent être plus directement concernées par les programmes de surveillance, sont certifiées dans le cadre de la sphère desécurité».

la protection des données personnelles, l'Union européenne a su imposer sa souveraineté au-delà de ses frontières. L'Internet est devenu un espace qui symbolise le brouillage des frontières entre les territoires, entre le privé et le public, entre la loi et le marché. La question de la gouvernance internationale représente donc un défi pour l'identité de l'Union européenne.

PARTIE II. UNE ARTICULATION COMPLEXE DU RÉGIME DE PROTECTION

141 Le régime de protection. À l'origine, la CEE, instituée avec le Traité de Rome de 1957, n'avait pas pour vocation la protection des droits fondamentaux. C'est avec l'affaire *Stauder*[1123] que la Cour de justice a affirmé le principe selon lequel les droits fondamentaux font partie du droit communautaire en tant que principes généraux[1124] dont elle assure le respect[1125]. La portée de cette jurisprudence a été précisée dans l'affaire *Internationale Handelgesellshaft* où la Cour précise que pour dégager ces principes protecteurs des droits fondamentaux, elle recourt à deux sources d'inspiration : d'une part, les traditions constitutionnelles communes aux États membres [1126] ; d'autre part, les accords internationaux de protection des droits de l'homme[1127]. Parmi tous les traités internationaux dont la Cour a déclaré s'inspirer, le plus important est la Convention européenne des droits de l'homme. Dès 1970, la Cour de justice a décidé que les droits fondamentaux feraient partie des principes généraux du droit qu'elle se devait de sauvegarder et qu'elle s'inspirerait, pour ce faire, des traditions constitutionnelles communes aux États membres. En conséquence, aucune mesure incompatible avec les droits fondamentaux ne saurait être légitime[1128]. Ainsi les droits fondamentaux sont devenus une préoccupation majeure pour la Cour de justice. Parallèlement à la CourEDH, la Cour de justice a cherché à arbitrer dans les rapports conflictuels dérivant de la mise en œuvre de l'intérêt général ou du respect d'autres droits fondamentaux comme la liberté d'expression, la propriété intellectuelle ou encore la liberté d'entreprendre et le droit à la protection des données personnelles. Le droit positif de l'Union européenne avec l'inscription de l'article 8 de la Charte dans le droit primaire, a offert un nouvel instrument juridique pour répondre aux atteintes dérivant de l'utilisation des données personnelles et a inauguré une phase d'autonomisation du raisonnement de la Cour de justice qui s'affranchit de toutes références à l'art. 8 de la CEDH (Titre I). De plus, le droit positif de l'Union européenne a donné l'impulsion à l'institution d'autorités administratives indépendantes au sein des États membres, dotées d'une mission de régulation et de contrôle quasi juridictionnel (Titre II).

1123 C'est l'article 19 §1 TUE qui confie à la Cour la charge d'assurer le respect du droit dans l'interprétation et l'application des traités. La Cour a développé largement le recours aux principes généraux du droit, dans les nombreux domaines où cela lui est apparu nécessaire pour compléter les sources écrites.

1124 Il s'agit de règles non écrites appliquées par le juge. Ces principes généraux ont une valeur supérieure aux normes du droit dérivé et aussi aux accords internationaux conclus par l'Union. Leur respect s'impose non seulement aux institutions et organes de l'Union mais aussi aux États membres lorsqu'ils procèdent à l'exécution du droit de l'Union.

1125 Les traités originaux des Communautés européennes ne contenaient pas de référence aux droits de l'homme ou à leur protection. À mesure que la Cour de justice des Communautés européennes de l'époque était saisie d'affaires invoquant des violations des droits de l'homme dans des domaines relevant de la compétence du droit de l'UE, celle-ci a développé une nouvelle approche. Pour offrir une protection aux individus, elle a intégré les droits fondamentaux dans les principes généraux du droit européen. Selon la CJUE, ces principes généraux reflètent le contenu de la protection des droits de l'homme prévue par les constitutions nationales et les traités sur les droits de l'homme en particulier la CEDH. La CJUE a déclaré qu'elle garantirait la conformité du droit de l'UE à ces principes. En reconnaissant que ses politiques pouvaient avoir un impact sur les droits de l'homme et dans le souci de veiller à ce que les citoyens se sentent protégés de l'UE, en 2000 a été proclamé la Charte des droits fondamentaux de l'Union européenne. La Charte avait une portée politique mais avec l'entrée en vigueur du traité de Lisbonne le 1er décembre 2009, elle a acquis force obligatoire.

1126 CJCE, Internationale Handelgesellshaft, aff. 11/70, 17 dec. 1970.

1127 CJCE, Nold, aff. 4/73, 14 mai 1974.

1128 CJUE, ERT, §41.

TITRE I. LA SYSTÉMATISATION D'UNE PROTECTION JURIDICTIONNELLE

142 Une protection duale. Le droit à la protection des données à caractère personnel en Europe est un droit qui se caractérise par un fort niveau d'harmonisation, tant par le droit issu de la Convention européenne des droits de l'homme que par le droit de l'Union européenne. Une jurisprudence assez extensive s'est d'ailleurs développée, afin de préciser les différentes normes supranationales applicables, comme l'article 8 de la Convention européenne des droits de l'homme, la convention 108 du Conseil de l'Europe, la directive 95/46/CE ou encore l'article 8 de la Charte des droits fondamentaux. L'étude de la protection juridictionnelle des données personnelles par l'Union européenne et par la Convention européenne des droits de l'homme, révèle de nombreuses similitudes. L'analogie dans les mécanismes de protection est le fruit d'une démarche jurisprudentielle consistant en une recherche de cohérence normative et de l'utilisation de méthodes interprétatives similaires. Le « dialogue des juges »[1129] permet de mettre en corrélation les mécaniques respectives des différents ordres juridiques et donc constitue un élément du décloisonnement maîtrisé des ordres juridiques européens [1130] . Ce dialogue a entraîné un rapprochement juridique entre l'Union européenne et la Convention européenne des droits de l'homme. Ce rapprochement se concrétise aujourd'hui à travers la future adhésion de l'Union européenne à la Convention européenne des droits de l'homme[1131]. Ainsi les dispositions de la CEDH doivent être prises en compte « dans le but d'interpréter » les dispositions correspondantes de la Charte. En particulier, l'article 6, paragraphe 3, du TUE dispose que « les droits fondamentaux garantis par la Convention européenne pour la protection des droits de l'homme et des libertés fondamentales et résultat des traditions constitutionnelles communes aux États membres constituent des principes généraux du droit de l'Union ». De plus, la Charte elle-même exige que, dans la mesure où elle contient « des droits qui

1129 Le résultat de ce dialogue est flagrant à travers la lecture de l'article 6§2 du Traité d'Amsterdam qui se voit aujourd'hui concrétisé par le Traité de Lisbonne et la Charte des droits fondamentaux.

1130 L. BURGORGUE-LARSEN, « De l'internationalisation du dialogue des juges », in *Mélanges en l'honneur du Président Bruno Genevois, Le dialogue des juges*, Dalloz, Paris, 2009, p. 105 : « le dialogue peut permettre d'assurer la cohérence de systèmes dont les principes de fonctionnement sont similaires, on retrouve alors ici la logique de systèmes, c'est l'idéal systémique ».

1131 Voy. B. BONNET, « Repenser les rapports entre ordres juridiques », *Lextenso*, Paris, 2013, p. 23. L'auteur a observé que « l'imbrication complète, et semble-t-il irréversible de plusieurs systèmes de droit, qui se situent désormais non plus dans des rapports de primauté mais des rapports de systèmes ». Par conséquent, « la hiérarchie des normes, au sens classique du terme, n'existe plus, ou tout du moins (…) elle n'est qu'alternative ou multiple ». Certes, la Cour européenne des droits de l'homme rappelle de manière récurente que « les actes de la Communauté européenne ne peuvent être attaqués en tant que tels devant la Cour, car la Communauté en tant que telle n'est pas Partie contractante » voy. CEDH 18 février 1999, « Matthews c/ Royaume-Uni, §32 ; C.E.D.H., 30 juin 2005, « Bosphorus », §152. Cependant, de nombreux éléments démontrent que la Cour européenne s'est inscrite dans une logique de reconnaissance du droit de l'Union européenne, en effet, le juge de Strasbourg reconnaît non seulement la nature « sui generis » de l'Union européenne mais il l'établit également en tant que « système juridique propre » (Matthews c/ Royaume-Uni [GC] », précité, §48 et §36), Voy. également C.E.D.H., 30 juin 2005, « Bosphorus », §150. Du point de vue de la jurisprudence conventionnelle, les arrêts « Matthews » et « Bosphorus » consacrent donc cette spécificité de l'Union européenne non seulement à l'égard d'autres organisations internationales mais également à l'égard des droits nationaux. L'affaire Bosphorus marque la volonté du juge de Strasbourg d'élargir mais également d'approfondir son contrôle sur les actes émanant de l'Union européenne pour néanmoins en établir une protection équivalente. L'arrêt explicite les rapports pouvant exister entre la Convention européenne des droits de l'homme et le droit dérivé de l'Union européenne en précisant les liens pouvant exister entre ces ordres juridiques mais surtout en établissant une présomption de protection équivalente des droits fondamentaux.

correspondent aux droits garantis par la CEDH, la signification et la portée de ces droits sont les mêmes que celles prévues par CEDH ». Toutefois, le droit à la protection des données personnelles (tant au niveau de l'UE que du Conseil de l'Europe) ne peut être exercé de manière absolue[1132]. Il est susceptible d'être restreint lorsqu'il entre en conflit avec d'autres intérêts individuels également protégés ou des contraintes collectives relevant de l'intérêt général[1133] et avec les droits d'autrui. La Cour de justice de l'Union européenne a d'ailleurs clairement affirmé que : « les droits fondamentaux ne constituent pas des prérogatives absolues et doivent être pris en considération au regard de leur fonction dans la société »[1134] . La doctrine a également mis en évidence la nécessité de dépasser toute approche absolutiste des droits fondamentaux[1135]. Dans la jurisprudence de la Cour de justice, il est possible d'observer une « instrumentalisation » du droit de la Convention européenne des droits de l'homme au service du droit de l'Union européenne, qui comporte l'établissement d'une présomption de protection équivalente des droits fondamentaux[1136]. Nous verrons dans un premier temps que le droit fondamental à la protection des données personnelles n'est pas une prérogative absolue, et qu'il peut faire l'objet de restrictions tant d'un point de vue formel que matériel. Ainsi il doit être mis en balance et concilié avec d'autres intérêts légitimes, que ce soit l'intérêt général ou les libertés d'autrui[1137]. Dans un premier temps, le raisonnement du juge de l'Union européenne était calqué sur celui de la CourEDH (Chapitre I). Toutefois, avec l'entrée en vigueur du traité de Lisbonne on peut souligner un processus d'autonomisation progressive du juge de l'Union vis-à-vis de la CEDH. La Charte des droits fondamentaux est ainsi devenue la principale

---

1132 E. MILLARD, *Effectivité des droits de l'homme*, in J. ANDRIANTSIMBAZOVINA, H. GAUDIN, J.-P. MARGUENAUD, S. RIAL, F. SUDRE (dir.), *Dictionnaire des droits de l'homme*, PUF, coll. Quadrige – Dicos Poche, 2008, p. 277 et s.

1133 D. LOCHAK, « Les bornes de la liberté » , *Pouvoirs, revue française d'études constitutionnelles et politiques*, n°84, 84 - La liberté, p.15-30. Consulté le 2017-08-13, disponible à l'adresse : : http://www.revue-pouvoy.s.fr/Les-bornes-de-la-liberte.htmlp. P.16 : « La liberté de chacun a pour bornes la liberté d'autrui d'un côté, le bien commun de l'autre : tel est le paradigme fondamental dans lequel s'énonce la problématique classique des restrictions aux libertés ».

1134 CJUE, Eugen Schmidberger, Internationale Transporte und Planzü ge c. République d'Autriche, C-112/00, 12 juin 2003, Rec. p. I 05659, § 80. Pour l'application au droit à la protection des données personnelles v. CJUE, G. Ch., Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, aff. C-92/09 et C-93/09, Rec. I-11063, 9 novembre 2010, § 48.

1135 A.REMEDEM, *La protection des droits fondamentaux par la Cour de justice de l'Union européenne*, Droit Université d'Auvergne - Clermont-Ferrand I, 2013. Français , disponible à l'adresse : https://tel.archives-ouvertes.fr/tel-01168308/document; A. VIALA, *Droits fondamentaux (Garanties procédurales)*, in D. CHAGNOLLAUD, G. DRAGOr (dir.), *Dictionnaire des droits fondamentaux*, Dalloz, 2006, pp. 287 et s., spéc. p. 298-299.

1136 F. SUDRE, *L'apport du droit international et européen à la protection communautaire des droits fondamentaux*, Société française pour le Droit international, colloque de Bordeaux , in *Droit international et droit communautaire. Perspectives et réalités*, Paris, Pédonne, 2000, pp. 169 et s. L. SCHEECK parle d'« intrusions réciproques » in L. Scheeck, « L'amplification de la résonance et la réduction de la dissonance ? Les effets de la relation entre les cours européennes sur l'intégration européenne, in W.D. EBERWEINet Y. SCHEMEIL, (éds.), *Normer le monde : énonciation et réception des normes internationales*, L'Harmattan, 2009, pp. 277-308, spéc. pp. 280 et s ; V. Constantinesco évoque une « vampirisation » du droit de la Convention par la Cour de justice in V. CONSTANTINESCO, *Le renforcement des droits fondamentaux dans le Traité d'Amsterdam, in Le Traité d'Amsterdam, réalités et perspectives*, Pedone,1999, Paris, p. 33.

1137 La doctrine distingue la conciliation de la limitation des droits fondamentaux, la première correpondant à l'hypothèse d'un conflit de droits fondamentaux, la seconde à l'hypothèse d'une confrontation d'un droit fondamental à un impératif d'intérêt général. Voy. B. MATHIEU, M. VeERPERAUX (dir.), *L'intérêt général, norme constitutionnelle*, Dalloz, coll.Cahiers constitutionnels de Paris 1, 2007, spéc p. 474-475.

référence pour évaluer la conformité du droit dérivé de l'Union européenne au droit fondamental à la protection des données personnelles proclamé par la Charte[1138]. De plus, la jurisprudence de la CJUE a établi que la CEDH « ne constitue pas, tant que l'Union européenne n'y a pas adhéré, un instrument juridique qui est officiellement intégré au droit de l'Union européenne »[1139] (Chapitre II).

CHAPITRE I. UNE DOUBLE PROTECTION JURIDICTIONNELLE

144 Le dialogue des juges. La protection des données à caractère personnel s'est développée à partir du droit à la vie privée, consacré par l'article 8 de la Convention de 1950. Du point de vue de la CEDH, le droit à la protection des données personnelles « joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la CEDH. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article »[1140]. Or, depuis l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Convention européenne des droits de l'homme a intégré le droit de l'Union, aux côtés de la Charte des droits fondamentaux de l'Union européenne. De plus, la Charte lie les institutions de l'Union ainsi que les États membres dans l'exécution du droit de l'Union, et comprend comme la CEDH une disposition relative à la protection de la vie privée (art.7), mais aussi un article qui protège spécifiquement les données personnelles dans son article 8[1141]. Toutefois, les références au droit à la vie privée à l'article 1er de la Convention 108, ainsi que dans le préambule et à l'article 1er de la directive 95/46/CE attestent que le droit à la protection des données est étroitement lié au droit à la vie privée. Bien que consacré comme un droit fondamental, le droit à la protection des données personnelles n'est pas une prérogative absolue, mais doit être mis en balance et concilié avec d'autres intérêts légitimes, que ce soit ceux de la

1138 Voy. Les recents affaires de la CJ, en particulièr Digital Rights Ireland and Schrems illustrent ce propos. Voy. également CJEU, aff. C-199/11, Otis and Others, paragraph 47, aff. C- 398/13 P, Inuit Tapiriit Kanatami and Others c. Commission, paragraph 46.

1139 Voy. CJUE, C 617/10, Åkerberg Fransson, § 44. C 398/13 P, Inuit Tapiriit Kanatami and Others v Commission, § 45, C-601/15 PPU J.N. v Staatssecretaris van Veiligheid en Justitie, §45, aff. Jointes C-203/15 and C-698/15, Tele2 Sverige AB, §127-129.

1140 CEDH, S. et Marper contre Royaume-Uni. Req. 30562/04 et 30566/04, § 103, 4 décembre 2008.

1141 M. ROCCATI, *Droit de l'Union et protection des données à caractère personnel*, Les cahiers de la fonction publique, 2014, p.36-38.

société dans son ensemble, comme des intérêts publics, ou des intérêts privés[1142]. Le présent chapitre a pour objet l'analyse de la conciliation entre le droit à la protection des données personnelles avec l'intérêt général et d'autres droits fondamentaux[1143]. Les limites à l'exercice des droits se posent dans la stricte mesure où ceux-ci sont nécessaires et proportionnés pour préserver l'équilibre de la vie en société. Cet équilibre est assuré par le juge. C'est au jugequ'il revient de soupeser, au cas par cas, les exigences antinomiques pour concilier le plus équitablement possible l'exercice de deux droits potentiellement antagonistes. Ainsi, la liberté de chacun a pour bornes la liberté d'autrui d'une part et le bien commun de l'autre[1144]. Un juste équilibre doit être maintenu entre les exigences de l'intérê t général de la communauté et la sauvegarde des droits fondamentaux des individus. Cela peut comporter un conflit de droits qui ne peuvent pas se réaliser intégralement et simultanément[1145] puisqu'il n'existe aucun droit pouvant s'exercer sans limites ; aucune liberté n'est absolue. Il faut se demander quelles limites, quelles bornes à l'exercice du droit à la protection des données personnelles sont légitimes et nécessaires dans une société démocratique[1146]. L'article 52 §1 de la Charte, exige que les limitations à l'exercice de droits soient prévues par la loi. De plus, une ingérence au droit à la vie privée et à la protection des données personnelles peut être validée et acceptée par les deux Cours, mais à condition qu'elle parvienne à passer le test de proportionnalité[1147]. L'article 52, paragraphe 3, de la Charte prévoit un mécanisme de cohérence entre la Charte des droits fondamentaux et la CEDH, en disposant que le sens et la portée des droits contenus dans ces deux textes, sont les mêmes que ceux que leur confère la CEDH. L'interdépendance de ces droits transparaît aussi dans la jurisprudence de la Cour de justice de l'Union européenne. Lorsqu'elle applique les critères de nécessité et de proportionnalité dans les affaires sur la protection des données, la Cour a pour longtemps privilégié une lecture conjointe des articles 7 et 8 de la Charte bien que le droit à la vie privée soit inscrit dans la Charte (article 7) et dans la CEDH (article 8), le droit à la protection des données à caractère personnel en tant que tel est un droit fondamental distinct dans la Charte (article 8)[1148]. De plus, le droit de l'Union peut

---

[1142] D. SHELTON, *Remedies and the Charter of Fundamental Rights of the European* Union, in S. PEERS, A. WARDS, The european Charter of foundamental right : politics, Law and policy, 2004, p.349 ; A.TORRES PEREZ, *Conflicts of rights in the European Union : a theory of supranational adjudication,* Oxford Studies in European Law, 2009, p. 23.

1143 L'art. 8 de la CEDH et l'art. 52.1 de la Charte parlent de « droit d'autrui ». P. DUCOULOMBIER, « Conflit et hiérarchie dans la jurisprudence de la Cour européenne des droits de l'homme », in L. POTVIN-SOLIS (dir.), *La conciliation des droits et libertés dans les ordres juridiques européens*, Broché, 2012, p. 319 et s.

1144 On trouve les prémisses de ce paradigme libéral à l'art 4 de la Déclaration des droits de l'homme lorsqu'elle énonce que « la liberté consiste à pouvoir faire tout ce qui ne nuit pas à autrui ».

1145 F. SUDRE, « Les conflits de droits. Cadre général d'approche dans la jurisprudence de la Cour européenne des droits de l'homme », in L.POTVIN-SOLIS (dir.), *La conciliation des droits et libertés dans les ordres juridiques européens*, Bruxelles, Bruylant, coll. Colloques Jean Monnet, 2012, spéc p. 237.

1146 Manuel de droit européen en matière de protection des données, préparé conjointement par l'Agence des droits fondamentaux de l'Union européenne et le Conseil de l'Europe, en association avec le greffe de la Cour européenne des droits de l'homme, Luxembourg, Office des publications de l'Union européenne, 2014.

1147 Voy. Opinion 01/2014 of the Article 29 Working Party on the application of necessity and proportionality concepts and data protection within the law enforcement sector, 27 february 2014.

davantage fournir une protection plus étendue (article 52 (3) de la Charte). D'une part, le droit au respect de la vie privée dans l'article 7 de la Charte correspond directement à l'article 8 de la CEDH. D'autre part, le droit à la protection des données personnelles est inscrit dans la Charte, mais ne figure pas expressément parmi les droits correspondant à un droit protégé par la CEDH conformément à l'article 52 (3) de la Charte[1149].Toutefois, la note explicative de l'article 8 de la Charte prévoit que ce droit a été fondé, entre autres, sur l'article 8 de la CEDH. Par conséquent, la jurisprudence de la Cour européenne des droits de l'homme en vertu de l'article 8 de la CEDH est pertinente, pour déterminer si une limitation est conforme à la Charte [1150] . Il existe également un dialogue constant entre la Cour de justice et la Cour européenne des droits de l'homme, observé dans de nombreuses références dans la jurisprudence des deux juridictions[1151]. L'imperatif de cohérence doit être appréndé dans une logique horizontale permettant d'assurer la coexistance des deux ordres juridiques distincts et autonomes[1152]. Ainsi dans les deux ordres spècifiques, les restrictions au droit à la protection des données personnelles doivent être justifiées. Non seulement il faut que les restrictions soient prévues et connues par les destinataires mais aussi qu'elles soient conformes au principe de proportionnalité. Outre ces deux conditions relatives à la prévisibilité et à la proportionnalité des restrictions, une troisième condition relative à l'interdiction d'atteinte au contenu essentiel du droit fondamental est parfois invoquée comme « limite aux limites ». Cela implique l'existence d'un noyau dur intouchable au sein de chaque droit fondamental qui ne saurait jamais être atteint, quel que soit le but légitime poursuivi[1153]. Cette interdiction est consacrée dans la Charte des droits fondamentaux de l'Union européenne[1154]. Les restrictions au droit à la protection des données personnelles visent d'une part à préserver l'intérêt public de la société, d'autre part à protéger les intérêts privés d'autrui. Ainsi la CourEDH et la Cour de justice ont été amenées à arbitrer des rapports conflictuels qu'il s'agisse des limites d'une surveillance généralisée au regard de la vie privée, des rapports entre les libertés d'expression, la propriété intellectuelle ou encore la liberté d'entreprendre. En tout état de cause, les restrictions au droit

1148 Voy. l'Avis du Groupe Article 29 n. 4/2007 sur le concept de données personnelles p. 7 et s.

1149 Voy. les explications de la Charte et de l'article 52.

1150 Voy. CJUE, C 617/10, Åkerberg Fransson, § 44, C 398/13 P, Inuit Tapiriit Kanatami et Autres c. Commission, § 45, C-601/15 PPU J.N. v Staatssecretaris van Veiligheid en Justitie, § 45 et les aff. Jointes C-203/15 et C-698/15, Tele2 Sverige AB, §127-129.

1151 Voy. CJCE affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke, paragraphe 59 ; affaires jointes C 293/12 et C 594/12, Digital Rights Ireland, paragraphe 35 ; affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB paragraphes 119, 120 et CEDH Zakharov c. Russia, 4 Decembre 2015 et 12 Janvier 2016, paragraphe 23.

1152 D. DERO-BUGNY, « La cohèrence dans le système européen de protection des droits fondamentaux », *mélanges en l'honneur de Claude Blumann, Bruxelles, Bruylant 2*015, p.109 et s.

1153 P. MEYER-BISCH (dir.), *Le noyau intangible des droits de l'homme*, éd. universitaire de Fribourg, 1991, pp. 53-56.

1154 L'article 52 paragraphe 1 de la Charte des droits fondamentaux de l'Union européenne interdit de porter atteinte au « contenu essentiel » des droits fondamentaux. Pour un commentaire de cet article v. L. BURGORGUE LARSEN, *Article II-112*, in L. BURGORGUE -LARSEN, A. LEVADE, F. PICOD (dir.), *Traité établissant une Constitution pour l'Europe. Commentaire article par article. Partie II La Charte des droits fondamentaux de l'Union*, Bruxelles, Bruylant, p. 658, spèc. p. 668-670.

à la protection des données personnelles doivent être prévisibles et proportionnées. Elles doivent être justifiées d'un point de vue formel mais aussi à travers un contrôle de type matériel, le juge doit vérifier si l'ingérence est nécessaire dans une société démocratique à travers un contrôle de proportionnalité (section I) et à travers la pondération avec les droits d'autrui (section II).

Section I. La légitimité de l'ingérence selon un contrôle formel et matériel

145 Les restrictions possibles. Le droit fondamental à la protection des données n'est pas une prérogative absolue, il doit être mis en balance et concilié avec d'autres intérêts légitimes. La doctrine a parlé de « limitations »[1155] ou de « restrictions »[1156] , le paragraphe 2 de l'art. 8 mentionne le terme « ingérence » et il semble correct de qualifier ce terme comme une « restriction » du droit à la protection des données personnelles[1157]. Le droit à la protection des données à caractère personnel fait partie des droits protégés par l'article 8 de la CEDH qui garantit le respect de la vie privée et familiale, du domicile et de la correspondance, et énonce les conditions dans lesquelles des restrictions à ce droit sont admises[1158]. Le premier paragraphe énumère précisément les droits que l'État doit garantir à toute personne : respect de sa vie privée et familiale, de son domicile et de sa correspondance. Le deuxième paragraphe énonce trois critères qui doivent être satisfaits pour qu'une quelconque ingérence soit conforme à l'article 8, paragraphe 2. Une telle ingérence doit être : prévue par la loi; destinée à atteindre l'un des buts légitimes énumérés à l'article 8, paragraphe 2; et nécessaire dans une société démocratique[1159]. Le contrôle formel tend à vérifier la prévisibilité de ces limites afin d'éviter une adoption arbitraire de telles restrictions en s'assurant que celles-ci présentent certaines caractéristiques intrinsèques répondant à l'impératif de sécurité juridique. C'est-à-dire, tout d'abord, que les restrictions soient « prévues par la loi ». Cette condition n'impose pas seulement l'existence d'une base légale mais elle implique également que cette base légale revête certaines qualités : elle doit être accessible et ses effets prévisibles. De même, la Cour de justice de l'Union européenne vérifie conformément à l'article 52 paragraphe 2 de la Charte que les restrictions au droit à la protection des données personnelles sont justifiées par la poursuite d'un objectif d'intérêt général[1160].

La protection juridictionnelle tant au sein de l'Union qu'au sein de la CEDH a le même objet. Tant dans le droit de l'UE que dans le droit du CEDH, les données à caractère personnel sont définies comme des informations concernant une personne physique identifiée ou

---

1155 A. C. KISS, « Les clauses de limitations et de dérogation dans la CEDH », in D. TURP et G. BEAUDOIN (dir.), *Perspectives canadiennes et européennes des droits de la personne*, Yvone Blais, Cowansville, 1986, p. 123-133.

1156 L. ADAMOVICH, « Marge d'appréciation du législateur et principe de proportionnalité dans l'application des restrictions prévues par la loi au regard de la CEDH », *RTDH*, 1991, N° 7, p. 291-300.

1157 L.E. PETITTI, E. DECAUX, P.H. IMBERT, *La Convention européenne des Droits de l'Homme, Commentaire article par article*, Economica 1999, p. 324.

1158 Voy. L'art. 8: 1)Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2) Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien-être économique du pays, à la défense de l'ordre et à la prévention des infractions pénales, à la protection de la santé ou de la morale, ou à la protection des droits et libertés d'autrui.

1159 Chaque paragraphe 2 des articles 8 à 11 prévoit la limitation par l'autorité publique des droits proclamés.

1160 Voy. art. 52§2 de la Charte : Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui.

identifiable[1161].

Cependant la CourEDH quand elle est appelée à constater une ingérence dans le droit protégé par l'article 8 doit constater au sens de l'article 8§2 si l'ingérence constitue un intérêt légitime, si elle est prévue par la loi, si l'ingérence est nécessaire dans une société démocratique et si l'État assume une obligation positive concernant le respect de l'article 8[1162].

La structure et le libellé de la Charte sont différents de ceux de la CEDH. La Charte ne parle pas d'ingérences dans des droits garantis, selon l'article 52§1 toute limitation à l'exercice des droits et libertés reconnus par la Charte et, par conséquent, à l'exercice du droit à la protection des données à caractère personnel, n'est recevable que si : elle est prévu par la loi, elle respecte le contenu essentiel du droit à la protection des données, elle est nécessaire, sous réserve du principe de proportionnalité et elle répond effectivement à des objectif d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. Ainsi, la Cour de justice se livre tant à un contrôle de type formel que matériel de proportionnalité.

De même, la CourEDH est attentive à ne pas contester les objectifs invoqués par le gouvernement défendeur (le but légitime) pour justifier une restriction, se limitant à émettre» des doutes « en la matière »[1163]. Le but serait donc toujours légitime sous réserve d'un contrôle de proportionnalité des restrictions. En effet, « le pouvoir le plus important des organes de contrôle est celui de sélectionner parmi les divers buts avancés celui qui paraît le plus approprié à l'ingérence en cause ; ce faisant, ils choisissent le terrain sur lequel la discussion de la nécessité de l'ingérence se situera et rendent plus difficile à l'État défendeur la démonstration que la mesure reposait sur des justes motifs »[1164]. Ainsi les critères prévus à l'article 8 (2) de la CEDH et à l'article 52 (1) de la Charte pour une limitation légale du droit au respect de la vie privée sont similaires.

L'article 8 (2) de la CEDH stipule, en outre, que la limitation doit être nécessaire «dans une société démocratique». Même si l'article 52 (1) de la Charte n'utilise pas la même expression, l'élément « société démocratique » est entrelacé dans l'ordre juridique de l'UE, car il découle des valeurs fondamentales de l'UE, y compris le respect de la démocratie (article 2 du TUE). Malgré une formulation différente, les conditions du traitement licite énoncées à l'article 52, (1) de la Charte rappellent celles de l'article 8, (2) de la CEDH, puisque les conditions énumérées à l'article 52, (1) de la Charte doivent être comprises comme conformes à celles visées à l'article 8 (2) de la CEDH. Cela grâce au mécanisme de cohérence de l'article 52§3 de la Charte[1165].Cependant l'article 52§3 précise que « cette disposition ne fait pas obstacle à ce

1161 C'est-à-dire des informations sur une personne dont l'identité est manifestement claire ou peut au moins être établie par l'obtention d'informations complémentaires. Directive 95/46, art. 2, point a ; Convention 108, art. 2, point a.

1162 Voy. art. 8 CEDH, Droit au respect de la vie privée et familiale : 1. Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance. 2. Il ne peut y avoir ingérence d'une autorité publique dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale.

1163 P. MUNZI, *La technique de proportionnalité et le juge de la Convention européenne des droits de l'homme. Essai sur un instrument nécessaire dans une société démocratique*, Aix-en-Provence, PUAM, 2005, 734 p., sp. p. 336.

1164 F. SUDRE, *Droit européen et international des droits de l'homme*, préc. p. 227.

1165 L'art. 53§3 dispose : « dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ».

que le droit de l'Union accorde une protection plus étendue ». Cela signifie que les conditions d'ingérences justifiées selon l'article 8 (2), de la CEDH sont des standards de limitations minimales applicables à des limitations du droit à la protection des données selon la Charte et que le droit de l'UE pourrait toutefois imposer d'autres exigences pour certains cas particuliers[1166]. La CourEDH et la Cour de justice lorsqu'elles sont appelées à constater une ingérence dans le droit protégé par l'article 8 doivent d'abord effectuer un contrôle formel : en premier lieu le juge doit constater si l'ingérence est prévue par la loi, si l'ingérence poursuit un but légitime. Ce contrôle sera plus au moins étendu selon la marge nationale d'appréciation reconnue aux États (§1). À côté du contrôle juridictionnel formel, les deux juridictions sont amenées à effectuer également le contrôle matériel des restrictions. Ainsi tant la CEDH que la Cour de justice sont appelées à effectuer un contrôle sur la proportionnalité de l'ingérence comportant une restriction du droit à la protection des données personnelles[1167](§2).

§1. La légitimité de l'ingérence selon un contrôle formel

146 La prévisibilité de la mesure. Au titre de la CEDH, le droit à la protection des données personnelles joue un rôle fondamental pour l'exercice du droit au respect de la vie privée et familiale consacré par l'article 8 de la CEDH. La législation interne doit donc ménager des garanties appropriées pour empêcher toute utilisation de données à caractère personnel qui ne serait pas conforme aux garanties prévues dans cet article. Depuis l'entrée en vigueur du traité de Lisbonne en décembre 2009, la Convention européenne des droits de l'homme a intégré le droit de l'Union, aux côtés de la Charte des droits fondamentaux de l'Union européenne. Cette dernière, qui lie les institutions de l'Union ainsi que les États membres dans l'exécution du droit de l'Union, comprend comme la CEDH une disposition relative à la protection de la vie privée en général (à son article 7), mais aussi un article qui concerne les données personnelles.
Une ingérence au droit à la vie privée et à la protection des données personnelles peut être validée et acceptée par les deux juridictions, mais à condition qu'elle parvienne à passer le contrôle formel et matériel. Le contrôle de type formel au sein de la CEDH et de l'Union européenne commence par la vérification de l'existence d'une base légale des restrictions. Une mesure restrictive concernant le droit protégé par l'article 8 (de la CEDH et de la Charte) n'est compatible avec ce dernier que si elle est prévue par la loi. Si la mesure contestée ne remplit pas ce critère de légalité, elle est assimilée à une violation sans qu'il soit nécessaire d'examiner

1166 La correspondance du principe du traitement licite dans le droit de l'UE avec les dispositions pertinentes de la CEDH est également corroborée par l'article 6 §3 du TUE qui dispose que « les droits fondamentaux, tels qu'ils sont garantis par la ConventionEDH font partie du droit de l'UE en tant que principes généraux du droit ».

1167 Voy. sur cet aspect J. ZILLER, *Le principe de proportionnalité*, AJDA, 1996, pp. 185 et s., sp. p. 185. Le principe de proportionnalité a été systématisé par la Cour constitutionnelle allemande. Celle-ci a identifié trois principes distincts composant le principe de proportionnalité : le principe d'adéquation, le principe de nécessité et le principe de proportionnalité au sens étroit. Le principe d'adéquation (Geeignetheit) signifie que la mesure restrictive contrôlée doit être appropriée à la réalisation de l'objectif poursuivi. Le principe de nécessité (Erforderlichkeit) implique que la mesure restrictive contrôlée soit indispensable pour atteindre le but recherché. Ainsi, parmi les mesures restrictives adéquates, celle qui limite le moins le droit ou la liberté concernés doit être préférée. Enfin, le principe de proportionnalité au sens strict (Verhältnismässligkeit im engeren Sinne) exige que la mesure restrictive assure un juste équilibre des intérêts en présence.

davantage l'affaire dans le fond. Pour être considérée comme « prévue par la loi », l'ingérence contestée doit avoir une base légale et doit être suffisamment précise et contenir des mesures de protection contre l'arbitraire des autorités publiques (A). Dès lors que les juges établissent que l'ingérence est prévue par la loi, ils continuent leur examen en se demandant si cette limite poursuit un but légitime au sens de l'article 8 §2 CEDH ou 52§1 de la Charte. Le but légitime peut être celui des intérêts publics ou celui des droits et libertés d'autrui (B).

A. L'existence d'une base légale

147 Les conditions de fond et de forme. Le contrôle juridictionnel des restrictions au droit à la protection des données personnelles consiste d'abord en un contrôle formel tendant à vérifier la prévisibilité de celles-ci. Ce contrôle formel a été opéré principalement par la CourEDH à travers l'approfondissement de l'exigence selon laquelle les restrictions doivent être prévues par la loi. Ce contrôle est désormais inscrit dans la clause de limitation de la Charte des droits fondamentaux (art 51§2). Cette condition n'impose pas seulement l'existence d'une base légale mais elle implique également que cette base légale revête certaines qualités : cette base légale doit ainsi être accessible et ses effets prévisibles. L'exigence de prévisibilité joue un rôle très important pour l'ensemble des restrictions au droit à la protection des données personnelles car le risque d'arbitraire est inhérent à toute utilisation de données personnelles.

148 Le contrôle formel par la CourEDH. Le concept de « loi » évoqué par l'article 8 CEDH a été éclairé dans l'affaire *Malone c. Royaume-Uni* de 1984[1168] où le requérant, M. James Malone, inculpé de délits de recel de biens volés, avait été finalement acquitté. Pendant son procès, il était apparu que l'une de ses conversations téléphoniques avait été interceptée pour le compte de la police en vertu d'un mandat délivré par le secrétaire d'État pour le ministre de l'Intérieur. Même si la modalité d'interception de la communication du requérant était légale au regard du droit interne (à l'époque, les écoutes étaient règlementées par une pratique administrative dont les détails n'avaient jamais été publiés et qui ne reposait sur aucune habilitation législative précise), la CourEDH a retenu qu'il n'existait pas de base légale concernant l'étendue et les modalités d'exercice du pouvoir d'appréciation attribué aux autorités publiques dans ce domaine et que l'ingérence résultant de l'exercice de la pratique en question n'était donc pas « prévue par la loi » au sens de l'art. 8 CEDH. Cela en raison du fait que l'écoute secrète des conversations téléphoniques reposait sur une pratique administrative dont les modalités pouvaient être modifiées à tout moment et qu'elle constituait par conséquent une violation de l'article 8. Il n'est pas admissible que les mesures adoptées pour limiter le droit à la protection des données résultent simplement de l'observation d'une pratique administrative ou autres actes juridiques non contraignants[1169]. Selon l'opinion du juge Pettiti, la pratique des

1168 CEDH, Malone c. Royaume-Uni, n. 8691/79, 2 août 1984.

1169 La Cour a pour la première fois fait le lien entre la condition de légalité et le principe de prééminence du droit dans l'affaire Malone c. Royaume-Uni : CEDH, 2 août 1984, Malone c. Royaume-Uni, req. n°8691/79, § 67 : « La Cour rappelle

écoutes a conduit la police à constituer des dossiers contraires à l'efficacité des mécanismes de protection du procès équitable inscrits à l'article 6 CEDH. En effet, l'écoute et l'interception exigent des contre-mesures : le droit d'accès par la personne placée sous écoute et l'effacement des données lorsque la procédure se termine par une décision d'acquittement. Dans cet affaire le test de légalité échoue au premier stade du contrôle. La CourEDH juge l'ingérence, en l'occurrence l'interception des communications du requérant, comme non prévue par la loi car les dispositions auxquelles le gouvernement britannique se référait pour justifier sa pratique de surveillance étaient vagues et sujettes à des interprétations divergentes[1170]. À partir de cette affaire, la jurisprudence de la CourEDH a établi le principe selon lequel l'ingérence est prévue par la loi si elle repose sur le droit national qui présente certaines caractéristiques, on parle alors de qualité de la loi[1171]. Ainsi, la loi doit notamment être « accessible aux personnes concernées et prévisible quant à ses répercussions »[1172]. Une règle est prévisible « si elle est formulée avec une précision suffisante pour permettre à toute personne d'adapter son comportement »[1173].
« Le degré de précision requis de la "loi" à cet égard dépendra du sujet en question »[1174].

149 Le contrôle de type formel par la Cour de justice. La Cour de justice se livre également à un contrôle formel des restrictions mais celui-ci n'apparaît pas aussi poussé que celui exercé par la Cour européenne. La prévision des restrictions par la loi était d'abord appliquée en tant que principe général de droit, ensuite elle a été inscrite à l'art. 52 (1) de la Charte. Dans l'affaire *Volker et Markus*, la Cour de justice a estimé que l'ingérence résultant de la publication sur un site Internet de données personnelles relatives aux bénéficiaires des aides financières versées dans le cadre de la politique agricole commune « doit être regardée comme ayant été "prévue par la loi" au sens de l'article 52, paragraphe 1, de la Charte » dans la mesure où « les articles 1er, paragraphe 1, et 2 du règlement n° 259/2008 prévoient expressément une telle publication »[1175]. Toutefois dans la jurisprudence suivante, la Cour de justice a inauguré la tendance à concevoir cette condition comme une simple vérification de l'existence d'une base légale, comme dans l'affaire *Shwarts* dans laquelle elle constate que la limitation qui résulte du prélèvement et de la conservation d'empreintes digitales dans le cadre de la délivrance de passeports doit être considérée comme étant « prévue par la loi », au sens de l'article 52, paragraphe 1, de la Charte, dès lors que l'article 1er, paragraphe 2, du règlement no 2252/2004

---

qu'à ses yeux le membre de phrase "prévue par la loi" ne se borne pas à renvoyer au droit interne, mais concerne aussi la qualité de la "loi"; il la veut compatible avec la prééminence du droit, mentionnée dans le préambule de la Convention ».

1170 Voy. §79.

1171 CEDH, Malone c. Royaume-Uni, § 66.

1172 CEDH, Amann c. Suisse, 16 février 2000, req. n° 27798/95, §50 ; voy. également CEDH, Kopp c. Suisse, 25 mars 1998, req. n° 23224/94, § 55 et CEDH, Iordachi et autres c. Moldavie, 10 février 2009, req. n° 25198/02, §50.

1173 CEDH, Amann c. Suisse, 16 février 2000, req. n° 27798/95, §56 ; voy. également CEDH, Malone c. Royaume-Uni, 26 avril 1985 req. n° 8691/79, §6 6 ; CEDH, Silver et autres c. Royaume-Uni, 25 mars 1983, req. n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, § 88.

1174 CEDH, The Sunday Times c. Royaume-Uni, 26 avril 1979, req. n° 6538/74, §49 ; voy. également CEHD, Silver et autres c. Royaume-Uni, 25 mars 1983, req. n° 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, § 88.

1175 CJUE, G. Ch., 9 novembre 2010, Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, aff. C-92/09 et C-93/09, § 66.

prévoit ces opérations[1176]. Cette tendance a conduit la Cour de justice dans l'affaire *Digital Rights* à ne pas reprendre dans sa motivation aux conclusions de l'avocat général sur l'existence d'une base légale en ne disant rien sur cet aspect et en passant directement à l'examen de la proportionnalité de la mesure envisagée[1177].

150 La qualité de la loi. La condition de l'existence d'une base légale n'impose pas seulement l'existence d'une loi encadrant la restriction mais elle implique également que cette base légale revête certaines qualités. Ainsi, la base légale doit être accessible et ses effets prévisibles. Concernant la prévisibilité, dans le contexte spécial de l'interception de communications pour les besoins d'enquêtes de police, elle ne saurait signifier qu'il faut permettre à quelqu'un de prévoir si et quand ses communications risquent d'être interceptées par les autorités afin qu'il puisse régler son comportement en conséquence. Or, l'expression « prévu par la loi », au sens du paragraphe 2 de l'art. 8 CEDH, dispose d'abord que l'ingérence ait une base en droit interne qui soit accessible à l'intéressé afin qu'il puisse en prévoir les conséquences, la loi doit fournir une protection adéquate contre l'arbitraire et, en conséquence, définir avec une netteté suffisante l'étendue et les modalités d'exercice du pouvoir conféré aux autorités compétentes. Une ingérence sera conforme au droit si elle a une base juridique et si elle définit clairement les règles régissant son fonctionnement. Ces règles devraient aussi, le cas échéant, indiquer expressément la marge d'appréciation laissée aux services répressifs, donner des orientations pour l'exercice de ce pouvoir d'appréciation et fournir des garanties juridiques adéquates. Dans l'affaire *Laender c. Suède*[1178], les juges de Strasbourg ont estimé que « la loi doit user de termes assez clairs pour leur indiquer de manière adéquate en quelles circonstances et sous quelles conditions elle habilite la puissance publique à se livrer à pareille ingérence secrète, et virtuellement dangereuse, dans leur vie privée et dans leur correspondance ». Dans l'affaire *Rotaru c. Roumanie*[1179], la CourEDH a conclu à une violation de l'article 8 de la CEDH au motif que le droit roumain permettait la collecte, l'enregistrement et l'archivage, dans des dossiers secrets, d'informations affectant la sécurité nationale, sans poser les limites de l'exercice de ces pouvoirs laissées à la discrétion des autorités. Par exemple, le droit national ne définissait pas le type d'informations quipouvaient être traitées, les catégories de personnes à l'égard desquelles des mesures de surveillance pouvaient être prises, les circonstances dans lesquelles de telles mesures pouvaient être prises ou la procédure à suivre. En raison de ces irrégularités, la Cour a conclu que le droit national n'était pas conforme à l'exigence de prévisibilité visée à l'article 8 de la CEDH et que cet article avait été violé. De même, dans l'affaire *Taylor-Sabori c. Royaume-Uni*[1180], le requérant avait fait l'objet d'une surveillance

---

1176 CJUE, 17 octobre 2013, M. Schwarz c. Stadt Bochum, aff. C 291/12, § 35.

1177 Voy. les Concl. de l'Avocat général P. Cruz Villalon, 12 décembre 2013, sous les affaires Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C 293/12 et C 594/12.

1178 CEDH, Leander c. Suède, arrê t du 26 mars 1987.

1179 CEDH, Rotaru c. Roumanie, 4 avril 2000, req. n° 28341/95,§ 57 ; voy. également CEDH, Association pour l'intégration européenne et les droits de l'homme et Ekimdzhiev c. Bulgarie, 28 juin 2007, req. n° 62540/00; CEDH, Shimovolos c. Russie, 21 juin 2011, req.n° 30194/09, ; et CEDH, Vetter c. France, 31 mai 2005, req. n° 59842/00.

1180 CEDH, Taylor-Sabori c. Royaume-Uni, req. n° 47114/99, 22 octobre 2002.

policière. Utilisant un « clone » du téléavertisseur du requérant, la police avait pu intercepter des messages qui lui étaient adressés. Le requérant avait ensuite été arrêté et inculpé pour conspiration en vue de la vente d'une substance réglementée. Une partie des éléments à charge du ministère public était des notes manuscrites récentes sur les messages du téléavertisseur qui avaient été transcrites par la police. Toutefois, au moment du procès du requérant, le droit britannique n'était pas doté de dispositions régissant l'interception de communications transmises par un système de télécommunications privé. L'ingérence dans ses droits n'était donc pas « prévue par la loi ». La CourEDH a conclu à une violation de l'article 8 de la CEDH. On peut conclure que la limitation du droit à la protection des données personnelles est admise s'il existe une loi qui encadre cette limitation, par « "loi" il faut entendre le droit écrit et non écrit »[1181]. L'exigence d'une base légale est substantielle et non formelle, c'est-à-dire qu'une interception téléphonique adoptée en conformité avec la législation interne peut être illégitime lorsque la loi nationale n'est pas accessible à ses destinataires[1182]. Dans le droit de l'Union européenne, la condition de prévisibilité appliquée initialement au titre des principes généraux du droit a été inscrite à l'article 52 paragraphe 1 de la Charte des droits fondamentaux. Celui-ci impose que les limitations apportées à l'exercice de droits consacrés par la Charte soient prévues par la loi. Dans l'affaire *Osterreichischer Rundfunk*[1183] la Cour a imposé le respect de cette condition de légalité et notamment de l'exigence de prévisibilité. Après avoir constaté que la mesure en cause avait bien une base légale, la Cour a examiné attentivement la qualité de celle-ci[1184]. Ce contrôle formel dans l'affaire *Osterreichischer Rundfunk* a été particulièrement remarqué car il ne semble pas repris par la Cour de manière systématique lorsqu'elle vérifie les restrictions aux droits fondamentaux[1185]. Dans des arrêts suivants, la Cour de justice a affirmé une tendance à concevoir cette condition comme une simple vérification de l'existence d'une base légale[1186] au point même de ne pas toujours la reprendre dans sa motivation alors qu'elle avait fait l'objet d'une analyse détaillée par l'Avocat général P. Cruz Villalón dans l'affaire *Digital Rights Ireland*[1187]. Une fois que le juge a vérifié l'existence d'une base légale permettant la restriction, le juge vérifie que l'ingérence poursuit un but légitime.

B. La poursuite d'un but légitime

1181 CEDH, Leander c. Suède, § 51.

1182 CEDH, Khan c. Regno Unito, (Ricorso n. 35394/97), 12 mai 2000.

1183 CJCE, 20 mai 2003, Rechnungshof c. Österreichischer Rundfunk et autres, aff. C-465/00, C-138/01, C-139/01.

1184 Voy. §77 de la décision.

1185 R. TINIERE, *L'office du juge communautaire des droits fondamentaux*, in C. PICHERAL, L. COUTRON (dir.), *Charte des droits fondamentaux de l'Union européenne et Convention européenne des droits de l'homme*, Bruylant, coll. Droit de la Convention européenne des droits de l'homme, Bruxelles, 2012, pp. p. 376-377.

1186 CJUE, 17 octobre 2013, M. Schwarz c. Stadt Bochum, aff. C 291/12, § 35.

1187 Concl. de l'Avocat général P. Cruz Villalon, 12 décembre 2013, dans les affaires Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C 293/12 et C 594/12.

151 Des objectifs justifiant la restriction du droit à la protection des données personnelles. Dès lors que les juges établissent que l'ingérence est prévue par la loi, ils continuent leur examen en se demandant si cette limite poursuit un but légitime au sens de l'article 8 §2 CEDH ou 52§1 de la Charte. Le but légitime peut être celui des intérêts publics ou celui des droits et libertés d'autrui. Le critère de la poursuite d'un but légitime est étroitement lié à l'exigence que l'ingérence soit « nécessaire dans une société démocratique ». Ainsi l'activité doit être menée en vue d'atteindre un des buts énumérés à l'article 8, paragraphe 2 de la CEDH à savoir la défense de l'ordre et la prévention ou la détection des infractions pénales, la protection des droits et libertés d'autrui, etc. En effet, l'État peut invoquer certains objectifs pour justifier la restriction d'un droit fondamental. Ces objectifs doivent être nécessaires à la défense d'une société démocratique. Concernant la signification du mot « nécessaire », les Juges de Strasbourg ont expliqué, dans leur arrê t *Handyside c. Royaume-Uni* [1188], que cet adjectif n'est pas synonyme d'« indispensable », mais n'a pas non plus la souplesse de termes tels qu'« admissible », « normal », « utile », « raisonnable » ou « opportun ». Concernant le terme « démocratique », les Juges de Strasbourg n'ont pas jusqu'à présent décrit dans le détail ce qui constitue à leurs yeux les caractéristiques d'une société démocratique. Cependant, dans l'affaire *Dugeon c. Royaume-Uni*[1189] ils évoquent à ce propos la tolérance et l'esprit d'ouverture. Dans le contexte de l'article 8, ils soulignent l'importance de la prééminence du droit dans une société démocratique et le besoin d'empêcher les ingérences arbitraires dans les droits reconnus par la Convention.

Une analyse de la jurisprudence de la Cour de justice et de la Cour européenne des droits de l'homme indique que la nécessité est un concept fondé sur des faits, plutôt qu'une notion juridique purement abstraite. Tout d'abord les mesures restrictives doivent être décrites[1190], puis il faut indiquer quels droits sont limités par la mesure[1191]. De même dans l'affaire *Leander c.*

1188 CEDH, Handyside c/ Royaume-Uni, 7 décembre 1976.

1189 CEDH, Dudgeon c/ Royaume- Uni, arrê t du 22 octobre 1981, paragraphe 53.

1190 Voy par Exemple the EDPS advice during the public consultation organised by the Commission in 2011 (see Council of the European Union, Doc 6370/13) on the Amendment to common agricultural policy (rules adopted to comply with the Schecke judgment on the policy - now Regulation 1306/2013, in particular Articles 111 - 113 and Recitals 73 - 87): »The EDPS points out that for assessing the compliance with privacy and data protection the envisaged measure intends to serve... Commenting on the control objective, the representative of the EDPS said that the Commission should thereby be clear on whether the aim of the measure also includes to allow a certain form of public control over the spending of EU money by the recipients as such for which the disclosure of the identity of the recipients would be indispensible. However, if the aim only concerns public control over the EU institutions and over how the EU budget is spent, it is less obvious that the identity of the recipients should be provided to the public..."

1191 CJUE, Huber, C-362/14. S'estimant discriminé du fait du traitement dont font l'objet les données le concernant contenues dans l'AZR (registre central des étrangers), en particulier parce qu'une telle base de données n'existe pas pour les ressortissants allemands, M. Huber a demandé la suppression de ces données. La Cour estime que le règlement n° 862/2007 prévoyant la transmission de statistiques relatives aux flux migratoires sur le territoire des États membres présuppose la collecte par ces États des informations permettant l'établissement de ces statistiques (§64). Toutefois, l'exercice de cette compétence ne rend pas pour autant nécessaire, au sens de l'article 7, sous e), de la directive 95/46, la collecte et la conservation de données nominatives auxquelles il est procédé dans le cadre d'un registre tel que l'AZR. En effet, ainsi que l'a indiqué M. l'avocat général au point 23 de ses conclusions, un tel objectif ne nécessite que le traitement d'informations anonymes (§65). Il résulte de l'ensemble des considérations qui précèdent qu'un système de traitement de données à caractère personnel relatives aux citoyens de l'Union non-ressortissants de l'État membre concerné tel que celui mis en place par l'AZRG et ayant pour objectif le soutien des autorités nationales en charge de l'application de la réglementation sur le droit de séjour ne répond pas à l'exigence de nécessité prévue à l'article 7, sous e), de la directive 95/46 (§66) ; Schecke (CJEU, Joined Cases C-92/09 and C-93/09) public funds constitutes a limitation on their private life within the meaning of Article 7 of the Charter (paragraph 58) ; (CJEU, Joined Cases C-293/12 and C-594/12) ; In the case of the Data Retention Directive, the Court found that the obligation

Suède 1192, la CourEDH a retenu que l'observation secrète de personnes postulant à des fonctions importantes pour la sécurité nationale n'est pas, en soi, contraire à l'exigence de démocratie. Les garanties spéciales prévues par la législation nationale dans le but de protéger les intérêts de la personne concernée (par exemple : contrôles exercés par le Parlement et le ministre de la Justice) ont amené la CourEDH à conclure que le système suédois de contrôle du personnel est conforme à l'exigence de l'article 8, paragraphe 2, de la CEDH. Eu égard à la grande marge d'appréciation dont il disposait, l'État défendeur était habilité à considérer que, dans le cas du requérant, les intérêts de la sécurité nationale prévalaient sur les intérêts individuels, des mesures donc « nécessaires ». Quant à la nécessité d'une telle ingérence à assurer la sécurité nationale dans une société démocratique, la Cour reconnaît que la notion de nécessité implique une ingérence fondée sur un besoin social impérieux et que les autorités nationales jouissent d'une marge d'appréciation dont l'ampleur dépend non seulement de la finalité mais encore du caractère propre de l'ingérence : il faut mettre en balance l'intérêt de l'État défendeur à protéger sa sécurité nationale avec la gravité de l'atteinte au droit du requérant au respect de sa vie privée. La Cour a donc estimé que le fait de n'avoir pas porté à la connaissance de M. Leander les renseignements communiqués à l'autorité militaire ne saurait prouver que l'ingérence n'était pas nécessaire à la sûreté nationale dans une société démocratique, et que le système suédois concernant l'adoption des mesures secrètes de surveillance à l'égard de ceux qui accèdent aux emplois publics prévoit des garanties suffisantes et donc, que l'ingérence des autorités publiques dans la vie privée de Leander doit être considérée comme proportionnée au but de protéger la sécurité nationale. Ainsi, la notion de nécessité implique une ingérence fondée sur un « besoin social impérieux et notamment proportionnée au but légitime recherché »[1193]. Selon la doctrine, l'intérêt général constitue une notion floue[1194] puisque liée à des valeurs changeantes et contingentes au sein d'une société donnée, elle évolue en fonction des besoins sociaux à satisfaire et des nouveaux enjeux auxquels

imposed on providers of publicly available electronic communications services or of public communications networks to retain, for 6 months to two years, communications data, such as the calling and called telephone line, the email addresses, the IP addresses used for accessing the Internet, »constitutes in itself an interference with the rights guaranteed by Article 7 of the Charter" (paragraph 34). »The access of the competent national authorities to the data constitutes a further interference with that fundamental right" (paragraph 35). The Court also found also that » Directive 2006/24 constitutes a limitation on the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter because it provides for the processing of personal data" (paragraph 36).

1192 CEDH, Leander c. Suède, req, n° 9248/81, 11 juillet 1985, § 59 et 67. Dans l'affaire Laender c. Suède, le requérant prétend que la procédure de contrôle du personnel appliquée à son sujet a méconnu l'article 8 de la Convention. Selon lui ses antécédents ne fournissaient aucune raison qui commandât, dans une société démocratique, de l'inscrire dans un registre de la Sûreté et en conséquence de l'exclure de l'emploi public dont il s'agit. En outre, l'ordonnance de contrôle du personnel ne saurait passer par une loi aux fins du paragraphe 2 de l'article 8. La Cour a estimé que la mémorisation des données relatives à M. Leander et le refus de lui accorder la faculté de les réfuter, portaient atteinte à son droit au respect de sa vie privée garanti par l'art. 8-1 de la Convention. La Cour a ensuite évalué si l'ingérence du système suédois de contrôle du personnel poursuit un but légitime (sécurité nationale) et à savoir si l'ingérence était prévue par la loi et nécessaire dans une société démocratique.

1193 CEDH, Leander c. Suède, 11 juillet 1985, req. n° 9248/81, § 58. Dans cette affaire le requérant a tenté de se suicider dans la rue en se taillant les poignets, sans savoir qu'une caméra de surveillance avait filmé toute la scène. Après avoir sauvé le requérant, la police a diffusé la séquence dans les médias, et ceux-ci l'ont publiée sans masquer le visage du requérant. La CouEDH a constaté l'absence de motifs pertinents ou suffisants pour justifier la divulgation directe de la séquence par les autorités au public sans obtenir préalablement le consentement du requérant ou sans masquer son identité. La CourEDH a conclu à une violation de l'article 8 de la CEDH.

1194 J. BOULOIS, (Préface), in D. TRUCHET, « Les fonctions de l'intérêt général en droit administratif français », *in Revue Internationale de Droit comparé*, 1978 sp. p. 15 : la recherche de l'essence de l'intérêt général « finit, en effet, par paraître douteuse, et, au plus mauvais sens du mot, dès lors que cette essence devient tributaire d'a priori philosophico-politiques ».

est confrontée la société [1195] . Parmi les situations d'intérêt général qui sont régulièrement invoquées pour limiter le droit à la protection des données personnelles on trouve la sécurité nationale (1), les enjeux économiques (2) et sanitaires (3).

1) La sécurité nationale comme intérêt général

Au titre de l'art. 52§1 de la Charte des droits fondamentaux, toute limitation à l'exercice des droits et libertés reconnus par la Charte, n'est recevable que si : elle est prévue par la loi, elle respecte le contenu essentiel du droit à la protection des données, elle est nécessaire, sous réserve du principe de proportionnalité et elle répond effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui. Telle prévision a été codifié dans le droit secondaire de l'Union européenne et en particulier à l'art. 22 du RGPD, qui de manière explicite prévoit la sécurité nationale, la sécurité publique, la prévention et la détection pénales parmi les motifs d'intérêt légitime.[1196] Les États invoquent souvent le motif d'intérêt général d'ordre sécuritaire pour limiter le droit à la protection des données personnelles. L'article 8 paragraphe 2 de la Convention énumère plusieurs motifs d'intérêt général d'ordre sécuritaire : la sécurité nationale, la sureté publique, la défense de l'ordre et la prévention des infractions pénales constituent ainsi des buts légitimes au nom desquels le droit à la protection des données personnelles peut être restreint.

152 Les limitations justifiées par l'intérêt général selon la CourEDH. La sécurité nationale, qui vise à défendre l'ordre constitutionnel démocratique face aux menaces intérieures et extérieures, est souvent invoquée pour limiter le droit à la protection des données personnelles comme l'ont montré plusieurs affaires de surveillance secrète dans le cadre de la lutte contre le terrorisme[1197]. L'autre limite évoquée est la défense de l'ordre et la prévention du crime, on peut ici citer les affaires concernant le fichage judiciaire[1198], les interceptions téléphoniques par

1195 S. GREER, « Les exceptions aux articles 8-11 de la Convention européenne des droits de l'homme », Editions du Conseil de l'Europe, Dossiers Droits de l'Homme n° 15, 1997, 67 p., spéc., p. 19.

1196 Voy. art. 22 RGPD : l'ensemble des droits accordés à la personne peuvent faire l'objet d'une limitation lorsqu'une telle limitation respecte le contenu essentiel des libertés et droits fondamentaux et constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir : la sécurité nationale, la défense nationale, la sécurité publique, la prévention et la détection d'infractions pénales

1197 CEDH, 6 septembre 1978, Klass c/ Allemagne, req. n°5502971, A28 ; CEDH, 26 mars 1987, Leander c/ Suède, req. n°9248/81, A116 ; CEDH, 6 juin 2006, Segerstedt-Wiberg et autres. c/ Suède, req. n°62332/00, Rec. 2006-VII ; CEDH, 2 septembre 2010, Uzun c/ Allemagne, req. n° 35623/05, Rec. 2010.

1198 Sur la conservation des données relatives aux empreintes digitales et génétiques pour des personnes poursuivies mais non condamnées v. CEDH, GC, 4 décembre 2008, S. et Marper c/ Royaume-Uni, req. n°30562/04 et n°30566/04, Rec. 2008 ; Sur l'inscription au fichier judiciaire national automatisé des auteurs d'infractions sexuelles (FIJAIS) v. CEDH, 17 décembre 2009, Gardel c/ France, req. n°16428/05, Rec. 2009 ; CEDH, 17 décembre 2009, M.B. c/ France, req. n°22115/06 ; CEDH, 17 décembre 2009, B.B. c/ France, req. n°5335/06 ; Sur la classification comme « prostituée » dans un fichier de police v. CEDH, 18 octobre 2011, Khelili c/ Suisse, req. n° 16188/07, § 60.

la police ou par l'autorité judiciaire[1199], la surveillance de personnes soupçonnées d'infractions pénales par GPS[1200], l'interception et le contrôle du courrier des détenus[1201], la divulgation dans un procès pénal de données médicales[1202]ou la divulgation dans les médias d'un extrait d'un enregistrement de vidéosurveillance[1203]. L'affaire *Leander contre Suède*, concernait un ancien militant communiste et syndicaliste se plaignant de ne pas avoir été recruté par la marine militaire suite à une procédure de contrôle pour laquelle un fichier secret de police avait été mis à profit. La CEDH a alors estimé que cette interférence était prévue par la loi, que son objectif, la sécurité nationale, était légitime et que la loi nationale garantissait l'équilibre entre droit à la vie privée et cet objectif légitime, puisqu'elle offrait des voies de recours, notamment auprès d'un médiateur indépendant donc les avis sont généralement respectés et suivis[1204].

153 Les limitations justifiées par l'intérêt général selon la Cour de justice. Au sein de l'Union européenne les motifs d'intérêt général sont peu fréquents. Ainsi dans l'affaire *PNR* relative au transfert des données des passagers aériens, la Cour de justice aurait pu reconnaître une telle limite, ainsi que le proposait l'Avocat général P. Léger, si elle n'avait pas constaté d'abord un défaut de base légale des actes contestés en s'arrêtant dans son raisonnement[1205]. Toutefois dans l'affaire *Shwartz*, la Cour de justice a admis que l'instauration des passeports biométriques tend à prévenir leur falsification et à empêcher leur utilisation frauduleuse par d'autres personnes que leur titulaire légitime. Ce faisant, les passeports biométriques visent «à empêcher, notamment, l'entrée illégale de personnes sur le territoire de l'Union » et poursuivent également un objectif d'intérêt général reconnu par l'Union [1206] . Récemment cette limite relevant de l'intérêt général a été reconnue dans l'affaire *Digital Rights*, relative à l'obligation de conservation des données de connexion imposée aux fournisseurs d'accès à Internet par la directive 24/2006 qui avait selon la Cour de justice pour objectif la lutte contre la criminalité grave. Ainsi la Cour de justice a affirmé que « la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des

---

1199 v. par ex. CEDH, 2 août 1984, Malone c/ Royaume-Uni, req. n°8691/79, A82 ; par l'autorité judiciaire v. par ex. CEDH, 24 avril 1990, Kruslin c/ France, req. n°11801/85, A176-A, § 27.

1200 CEDH, 2 septembre 2010, Uzun c/ Allemagne, req. n° 35623/05, Rec. 2010, § 77.

1201 CEDH, 25 mars 1983, Silver c/ Royaume-Uni, req. n°5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 7136/75, A61, § 96 ; CEDH, 25 mars 1992, Campbell c/ Royaume-Uni, req. n°13590/88, A233, § 41.

1202 CEDH, 25 février 1997, Z. c/ Finlande, req. n°22009/93, Rec. 1997-I, § 76.

1203 CEDH, 28 janvier 2003, Peck c/ Royaume-Uni, req. n°44647/98, Rec. 2003-I, § 67.

1204 CEDH 26 mars 1987. Leander contre Su.de. Req. 9248/81, pt. 81 et pt. 82

1205 Voy. Conclusions de l'avocat général P. Léger, présentées le 22 novembre 2005, Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes, aff. C-317/04 et C-318/04.

1206 CJUE, 17 octobre 2013, M. Schwarz c. Stadt Bochum, aff. C- 291/12, §§ 36-38.

techniques modernes d'enquête »[1207]. Pour ce faire, elle rattache l'obligation de conservation aux fournisseurs d'accès à Internet à l'intérêt général de la lutte contre la criminalité grave afin de garantir la sécurité publique. Cette dernière est proclamée et garantie par l'article 6 de la Charte reconnaissant à toute personne un droit à la sûreté[1208]. Au-delà des motifs d'intérêt sécuritaire, d'autres motifs d'intérêt général sont aussi souvent invoqués pour limiter le droit à la protection des données personnelles. Si la plupart des limitations sont justifiées par l'intérêt général, notamment par le but de sécurité publique, on peut douter qu'il en soit ainsi concernant le domaine économique et financier comme prévu par l'art. 23 §1, e) du RGPD. En effet de telles matières ne devraient pas prévaloir sur la protection des individus.

2) Le développement économique comme restriction relevant de l'intérêt général

154 Une limite rarement invoquée. Le bien-être économique d'un État permettrait de justifier des restrictions qui n'auraient pas d'autre fondement possible. C'est une limite propre à l'article 8 paragraphe 2 de la CEDH et qui est repris par l'art. 23, §1, e) du RGPD[1209]. Il s'agit d'un motif qui est rarement invoqué pour justifier les restrictions au droit à la protection des données personnelles. Toutefois, quelques exemples illustrent l'intérêt de cette limitation. Selon la Cour EDH, participent au bien-être économique de l'État la transmission d'un dossier médical à un organisme de sécurité sociale en ce qu'elle est potentiellement décisive pour l'allocation de fonds publics à des demandeurs remplissant les critères[1210] ou encore la saisie de documents par les douaniers dans le cadre d'une enquête sur des irrégularités présumées en matière de relations financières avec l'étranger[1211]. Malgré la faiblesse quantitative de tels motifs, ces exemples attestent bien de leur réalité et pertinence. La Cour de justice a également reconnu que des motifs d'intérêt général d'ordre économique peuvent limiter le droit à la protection des données personnelles. Dans la première affaire qu'elle a eu à examiner relative à l'interprétation de la directive n° 95/46 CE, la Cour de justice a considéré que la divulgation du nom et du montant des revenus annuels des personnes employées par des entités soumises au contrôle de la Cour des comptes autrichienne, lorsque ces revenus excèdent un certain plafond, vise à garantir une utilisation des fonds publics en maintenant les salaires dans une limite raisonnable. Ce faisant,

---

1207 CJUE, G. Ch., 8 avril 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C-293/12 et C-594/12, §§ 41-42.

1208 Voy. sur ce point CJUE, G. Ch., 8 avril 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C-293/12 et C-594/12, §§ 41-42.

1209 Le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement ou le sous-traitant est soumis peuvent, par la voie de mesures législatives, limiter la portée des obligations et des droits prévus aux articles 12 à 22 et à l'article 34, ainsi qu'à l'article 5 dans la mesure où les dispositions du droit en question correspondent aux droits et obligations prévus aux articles 12 à 22, lorsqu'une telle limitation respecte l'essence des libertés et droits fondamentaux et qu'elle constitue une mesure nécessaire et proportionnée dans une société démocratique pour garantir: e) d'autres objectifs importants d'intérêt public général de l'Union ou d'un État membre, notamment un intérêt économique ou financier important de l'Union ou d'un État membre, y compris dans les domaines monétaire, budgétaire et fiscal, de la santé publique et de la sécurité sociale.

1210 CEDH, M.S. c Suède, 27 août 1997, req. n° 20837/92, Rec. 1997-IV.

1211 CEDH, 25 février 1993, Funke c/ France, req. n°10828/84, A256-A, § 52 ; CEDH, 25 février 1993, Crémieux c/ France, req. n°11471/85, A256-B, § 35 ; CEDH, 25 février 1993, Miailhe c/ France (n°1), req. n°12661/87, A256-C § 33.

elle tend au bien-être économique du pays, but légitime reconnu à l'article 8 paragraphe 2 de la Convention européenne des droits de l'homme[1212].
Aux limites liées à l'intérêt général économique s'ajoute le motif d'intérêt général relatif à la santé publique.

3) Des motifs d'ordre sanitaire invoqués comme motifs d'intérêt général

Une justification relevant de l'intérêt général invoquée par les États portant une limitation au droit à la protection des données personnelles est constituée par la santé publique. La protection de la santé est expressément prévue au §2 de l'art 8 CEDH. Dans une affaire, la CourEDH a été confrontée à la question des registres de personnes internées d'office dans les établissements d'aliénés et celle des dossiers médicaux des malades admis dans les établissements hospitaliers. A cette occasion, la Commission a reconnu que ces restrictions à la protection des données personnelles répondent au but légitime de protection de la santé entendu tant de manière collective qu'individuelle. En effet, « la consignation des informations concernant les malades mentaux répond au but légitime que représente le bon fonctionnement du service public hospitalier, mais aussi à celui de protéger les droits des malades eux-mêmes, spécialement en cas d'internement d'office »[1213]. Sans rentrer trop dans le débat, le droit à la protection des données personnelles peut aussi être restreint au nom de la moralité publique et de la transparence. La moralité publique varie, selon la CourEDH, dans le temps et dans l'espace. C'est pourquoi le juge laisse aux États le soin de définir ces questions d'ordre moral mais aussi, d'ordre éthique qui sont susceptibles de limiter les droits fondamentaux dont le droit à la protection des données personnelles. Parmi les justifications invoquées, on trouve également l'intérêt général à la transparence, lequel tend à constituer une limite au droit à la protection des données personnelles tant au sein de la jurisprudence de la Cour européenne[1214] que de la Cour de justice[1215]. Mais cette limite apparaît parfois sous un angle davantage individuel que collectif à travers la reconnaissance d'un droit à l'information. Les restrictions au droit à la protection des données personnelles prises par les autorités nationales au nom d'un intérêt général peuvent

---

1212 CJCE, 20 mai 2003, Rechnungshof c. EDH, 7 septembre 1976, Handyside c. Royaume-Uni, req. n°5493/72, A24, § 48. C-465/00, C-138/01, C-139/01, Rec. I-4989, § 81.

1213 Comm. EDH (déc..), 9 juillet 1991, Chave née Jullien c/ France, req. n° 14461/88.

1214 Certes l'article 8 paragraphe 2 de la Convention ne comprend pas un tel motif parmi la liste des buts légitimes. Mais un tel motif pourrait être retenu à travers la protection des droits d'autrui qui constitue bien un but légitime. En effet la Cour européenne reconnaît sur le fondement de l'article 10 de la Convention relatif à la liberté de communiquer mais aussi de recevoir des informations une forme de droit d'accès à l'information.

1215 CJUE, G. Ch., 29 juin 2010, Commission européenne c. The Bavarian Lager Co. Ltd., aff. C-28/08, § 54 ; v. F. Kauff-Gazin, « Transparence », Europe, 2010, n° 10, pp. 12 et s. Dans l'affaire Bavarian Lager, confrontée à la question de la communication des procès-verbaux de réunions susceptibles de contenir des données personnelles, la Cour a reconnu que le principe de transparence censé « assurer une meilleure participation des citoyens au processus décisionnel ainsi que [...] garantir une plus grande légitimité, efficacité et responsabilité de l'administration à l'égard des citoyens dans un système démocratique »,1930 constitue un objectif d'intérêt général permettant de limiter un tel droit.

faire l'objet d'un contrôle restreint, plus ou moins poussé, par la Cour européenne et par la Cour de justice, eu égard à la marge nationale d'appréciation reconnue aux États.

155 La marge d'appréciation. Les juges européens reconnaissent aux États une marge d'appréciation pour restreindre le droit à la protection des données personnelles. En vertu de la marge d'appréciation, comme en vertu du principe plus large de subsidiarité, la CourEDH reconnaît que, tant du point de vue des principes que du point de vue pratique, les autorités nationales sont mieux placées pour se livrer à une appréciation de la nécessité et de la proportionnalité des mesures restreignant les droits et libertés garantis par la Convention. La Cour s'oblige en conséquence à une certaine retenue qui traduit le pouvoir discrétionnaire ou la marge d'appréciation dont bénéficient les autorités nationales. La doctrine de la marge d'appréciation permet de reconnaître qu'en appliquant certaines garanties consacrées par la ConventionEDH, il peut y avoir un éventail de solutions différentes mais légitimes selon le contexte, particulièrement en ce qui concerne l'appréciation de la proportionnalité d'une restriction autorisée à un droit ou à une liberté, ou le fait de ménager un équilibre entre différents droits en concurrence. La Cour européenne des droits de l'homme et la Cour de justice de l'Union européenne exercent un contrôle sur le motif d'intérêt général au nom duquel le droit à la protection des données personnelles peut être restreint. Tel contrôle apparaît particulièrement limité puisque les juges ne veulent pas se substituer aux autorités publiques des États dans la détermination discrétionnaire des restrictions au droit à la protection des données personnelles, notamment lorsque les restrictions au droit à la protection des données personnelles visent à assurer la sécurité nationale [1216] . L'expression marge d'appréciation indique les différentes sortes de pouvoir discrétionnaire dont disposent les États pour la mise en œuvre de leurs obligations au titre de la Convention européenne des droits de l'homme[1217]. Elle se caractérise par sa nature casuistique. La formulation des articles 8 à 11 implique dans le §2 un critère objectif de limitation de la marge d'appréciation. D'abord, il faut démontrer que l'ingérence est nécessaire dans une société démocratique, deuxièmement, la restriction doit être prévue par la loi et, enfin, correspondre à un besoin social impérieux. Toutefois, le principe de proportionnalité autorise des marges d'appréciation variables. Tout d'abord, la marge d'appréciation peut être plus au moins étendue par rapport à l'importance du droit en cause, aux circonstances particulières de l'espèce, et surtout à l'existence d'une norme européenne uniforme en la matière, c'est-à-dire qu'une pratique européenne commune peut fortement plaider en faveur d'une limitation du pouvoir discrétionnaire de l'État dans un cas déterminé. La CourEDH a reconnu une large marge d'appréciation lorsqu'il s'agit de mesures visant à

1216 Toutefois le contrôle restreint du but légitime devient un contrôle approfondi lors d'un contrôle de proportionnalité des restrictions.

1217 L'expression marge d'appréciation ne se trouve toutefois ni dans le texte de la Convention elle-mê me ni dans les travaux préparatoires, mais apparaît pour la première fois en 1958 dans le rapport de la Commission dans l'affaire Grèce c. Royaume-Uni, ayant son origine dans la requê te de la Grèce alléguant de violations commises par le Royaume-Uni à Chypre. Depuis, elle a été reprise dans plusieurs autres décisions de la Commission et dans plusieurs arrê ts de la Cour. Voy. sur ce point : H.C. YOUROW, *The Margin of Appreciation Doctrine in the Dynamics of European Human Rights Jurisprudence*, La Haye, Boston, Londres : Kluwer, 1996, p. 14.

assurer la sécurité nationale[1218]. Ainsi dans l'affaire *Leander c. Suède*, la Cour reconnaît que l'État défendeur « était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant [1219]. Dans l'affaire *Z c. Finlande*, la Cour admet une large marge nationale d'appréciation puisqu'il n'appartient pas à la Cour de substituer son point de vue à celui des autorités nationales quant à la pertinence des éléments de preuve utilisés lors de la procédure judiciaire », qu'« il incombe en premier lieu aux autorités nationales de juger de l'opportunité d'obtenir des témoignages et il n'appartient pas à la Cour de substituer son point de vue au leur en la matière » et qu'« il incombe en premier lieu aux autorités nationales de juger de l'opportunité pour elles de fournir et retenir des preuves pendant la procédure interne et qu'il n'entre pas normalement dans ses attributions de substituer son point de vue au leur en la matière »[1220]. Une large marge d'appréciation a également été admise s'agissant de la « protection de la santé ou de la morale » au motif que ces notions varient selon les États membres. Des marges d'appréciation variables ont été également reconnues s'agissant de l'exception tirée de la « défense de l'ordre et la prévention du crime ». Une large marge d'appréciation a été accordée par la CourEDH aux autorités nationales pour restreindre le droit à la protection des données personnelles [1221] dans l'affaire *Klass c. République fédérale d'Allemagne*. La Cour constate en effet que le système de surveillance mis en place établi un juste équilibre entre les intérêts opposés [1222] . Ainsi dans l'affaire *Leander c. Suède*, l'État défendeur « était en droit de considérer que les intérêts de la sécurité nationale prévalaient en l'occurrence sur les intérêts individuels du requérant et que pour préserver la sécurité nationale, les États contractants ont indéniablement besoin de lois qui habilitent les autorités internes compétentes à recueillir et à mémoriser dans des fichiers secrets des renseignements sur des personnes, puis à les utiliser quand il s'agit d'évaluer l'aptitude de candidats à des postes importants du point de vue de ladite sécurité »[1223].

La Cour de justice de l'Union européenne reconnaît également aux États une marge d'appréciation pour restreindre le droit à la protection des données personnelles. Lorsqu'elle a eu à interpréter pour la première fois la directive n° 95/46 CE dans l'affaire *Rechnungshof*, la Cour de justice, sollicitée sur une question préjudicielle par le juge national pour apprécier la conformité d'une loi constitutionnelle autrichienne à cette directive, a reconnu une certaine

---

1218 Cela n'a pas empêché les organes de Strasbourg de se livrer à un examen approfondi de procédures de surveillance secrète lorsqu'ils l'ont estimé approprié, voy. par exemple, affaire Klass c. République fédérale d'Allemagne, arrêt du 6 septembre 1978, série A no 28 ; affaire Leander c/ Suède, arrêt du 26 mars 1987, série A no 116.

1219 CEDH, 26 mars 1987, Leander c/ Suède, req. n°9248/81, A116, § 59, « Pour préserver la sécurité nationale, les États contractants ont indéniablement besoin de lois qui habilitent les autorités internes compétentes à recueillir et à mémoriser dans des fichiers secrets des renseignements sur des personnes, puis à les utiliser quand il s'agit d'évaluer l'aptitude de candidats à des postes importants du point de vue de ladite sécurité ».

1220 CEDH, 25 février 1997, Z. c/ Finlande, req. n°22009/93, Rec. 1997-I, §§ 98, 103 et 109

1221 C. OVEY, « The Margin of Appreciation and Article 8 of the Convention », *Human Rights Law Journal* 1998, no 19, pp. 10-12.

1222 CEDH, 6 septembre 1978, Klass c/ Allemagne, req. n°5502971, A28, § 59.

1223 CEDH, 26 mars 1987, Leander c/ Suède, req. n°9248/81, A116, § 59.

marge d'appréciation aux États. Elle a vérifié comme son homologue (CEDH) [1224] que l'obligation faite aux organismes publics soumis au contrôle de la Cour des comptes autrichienne de communiquer le montant des pensions de retraite excédant un certain seuil était bien nécessaire dans une société démocratique pour atteindre le but légitime poursuivi de bonne utilisation des fonds publics. La Cour de justice a été elle aussi confrontée au conflit des données personnelles avec un autre droit fondamental. Dans ces hypothèses, la Cour de justice a également reconnu qu'il appartenait aux États de concilier ces droits antagonistes. Dans l'affaire *Promusicae*, opposant le droit à la protection des données personnelles aux droits de propriété intellectuelle et de recours juridictionnel effectif, la Cour a directement renvoyé aux États membres le soin de trouver cet équilibre entre ces différents droits sans fournir d'indication sur la manière de déterminer cet équilibre[1225]. Toutefois la Cour de justice a donné des indications sur la manière d'interpréter les droits en conflit lorsqu'elle juge qu'un droit a un poids majeur. Dans l'affaire *Stamedia*, opposant le droit à la protection des données et la liberté d'expression, le juge semble en effet privilégier la liberté d'expression : « afin de tenir compte de l'importance que détient la liberté d'expression dans toute société démocratique, il convient, d'une part, d'interpréter les notions y afférentes, dont celle de journalisme, de manière large. D'autre part, et pour obtenir une pondération équilibrée entre les deux droits fondamentaux, la protection du droit fondamental à la vie privée exige que les dérogations et limitations de la protection des données […] doivent s'opérer dans les limites du strict nécessaire »[1226]. La Cour a été amenée à interpréter l'article 9 de la directive qui impose aux États membres de prévoir des exemptions et dérogations à la protection des données personnelles lorsqu'elles sont utilisées « aux seules fins de journalisme ou d'expression artistique ou littéraire ». Puisque cet article « contient explicitement une obligation faite aux États de garantir un équilibre entre les deux libertés opposées », la Cour en déduit en toute logique que la tâche d'établir la conciliation entre ces deux droits fondamentaux incombe aux États membres[1227]. Cette tendance à fournir des indications sur la manière d'interpréter les droits en conflit a été utilisée dans l'affaire *Google Spain*[1228], mais la CourEDH et la Cour de justice ne fournissent aucune indication précise sur la manière de parvenir à ce juste équilibre

---

1224 J. RIDEAU, Les limites de la protection juridictionnelle des droits de l'homme, in F. SUDRE, H. LABAYEe (dir), Réalités et perspectives du droit communautaire des droits fondamentaux, pp. 399 et s., spéc. p. 419.

1225 CJUE, G. Ch., 29 janvier 2008, Productores de Música de España (Promusicae) c. Telefónica de España SAU, aff. C-275/06, Rec. I-00271, § 70 : « Il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme aux dites directives, mais également de veiller à ne pas se fonder sur une interprétati on de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité ». Voy. en ce sens, F. COUDERT, E. WERKERS, « La protection des droits d'auteur face aux réseaux peer-to-peer : la levée du secret des communications est-elle justifiée ? », *RTDI*, 2008, n° 30, pp. 76 et s., sp. p. 83.

1226 CJCE, G. Ch., 16 décembre 2008, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, aff. C-73/07, Rec. I-09831, § 56.

1227 CJCE, G. Ch., 16 décembre 2008, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, aff. C-73/07, Rec. I-09831, § 54.

1228 Voy. § 98 de la décision. Dans cette affaire relative à l'activité des moteurs de recherche, la Cour considère « dans la mesure où il ne semble pas exister, […], de raisons particulières justifiant un intérêt prépondérant du public à avoir, dans le cadre d'une telle recherche, accès à ces informations, ce qu'il appartient toutefois à la juridiction de renvoi de vérifier, la personne concernée peut, en vertu […] de la directive 95/46, exiger la suppression desdits liens de cette liste de résultats.

lorsqu'elles accordent la même importance aux droits en conflit. Toutefois si elles attribuent une importance particulière à l'un d'entre eux, elles peuvent alors imposer un certain nombre de critères que les États devront prendre en compte dans leur appréciation. La Cour de justice de l'Union européenne reprenant le raisonnement effectué par la CourEDH, reconnaît également aux États une marge d'appréciation pour restreindre le droit à la protection des données personnelles au nom de l'intérêt général qui peut être plus au moins étendu. Toutefois les obligations positives auxquelles sont tenus les États dans la mise en œuvre de la convention constituent un renforcement à leur marge d'appréciation.

156 Les obligations positives. La plupart des obligations découlant de l'adhésion à la Convention sont négatives. Il s'agit d'une obligation de renoncer à tout acte qui emporte violation des droits de la Convention. Toutefois, le juge européen a considéré que tous les droits substantiels énoncés par la Convention renferment une obligation implicite de mettre en place et de rendre effectives des procédures permettant à la personne concernée de revendiquer au niveau national le droit en cause et de contester les mesures y portant atteinte [1229]. La CourEDH a ainsi interprété certaines des dispositions comme impliquant une action positive de l'État pour protéger les droits, il s'agit d'une interprétation téléologique. La CourEDH a établi progressivement une obligation positive découlant de l'art. 8 se concrétisant dans l'adoption de mesures visant au respect de la vie privée. En effet, l'objet essentiel de l'article 8 est de « prémunir l'individu contre des ingérences arbitraires des pouvoirs publics », une obligation donc négative ; néanmoins, la Cour estime que cette disposition peut engendrer, de surcroit, des obligations positives inhérentes à un respect effectif des valeurs qu'elle protège[1230]. Ainsi, l'État doit respecter l'obligation négative de s'abstenir d'interférer arbitrairement dans la vie privée et familiale, le domicile et la correspondance d'une personne, mais il doit également être amené à agir concrètement pour assurer le respect de toute une série d'intérêts personnels énoncés par cette disposition. La CourEDH a considéré que « tous les droits substantiels énoncés par la Convention renferment une obligation implicite de rendre effectives des procédures permettant à la personne concernée de revendiquer au niveau national le droit en cause et de contester les mesures y portant atteinte »[1231]. Celle-ci n'est pas seulement le résultat du développement de la technique des obligations positives, elle résulte également de l'interprétation de l'exigence selon laquelle les restrictions aux droits fondamentaux doivent être prévues par la loi. Ainsi la Cour rappelle que le recours aux obligations positives n'est pas différent du recours aux obligations négatives[1232]. Cependant, dans la mise en œuvre d'une obligation positive, l'État

---

1229 F. SUDRE, *Droit européen et international des droits de l'homme*, PUF, Droit fondamental, 13e édition Parution 10/2016, spéc. p. 262.

1230 Voy. CEDH, *Kroon c/ Pays-Bas, arrê t du 27 octobre 1994, paragraphe 31.*

1231 F. SUDRE, *Droit européen et international des droits de l'homme*, préc., spéc. p. 262.

1232 La frontière entre les obligations positives et négatives de l'État au regard de l'article 8 ne se prête pas à une définition précise ; les principes applicables sont néanmoins comparables. En particulier, dans les deux cas, il faut prendre en compte le juste équilibre à ménager entre l'intérêt général et les intérêts de l'individu, l'État jouissant en toute hypothèse d'une marge d'appréciation ». Voy. en ce sens CEDH, 24 juin 2004, Von Hannover c/ Allemagne, req. n°59320/00, Rec. 2004-VI, § 57 ; CEDH, 25 novembre 1994, Stjerna c/ Finlande, req. n°18131/91, A299-B, § 39 ; CEDH, 7 février 2002, Mikulic c. Croatie, req. n°53176/99, Rec. 2002-I, § 58 ; Cour EDH, Odievre c. France [GC], 13 février 2003, req. n° 42326/98, §40.

dispose d'un certain pouvoir discrétionnaire. Dans l'affaire *X. & Y. c/ Pays-Bas*[1233], la CEDH a affirmé que « L'article 8 ne se contente pas de commander à l'État de s'abstenir de pareilles ingérences : à cet engagement plutôt négatif peuvent s'ajouter des obligations positives inhérentes à un respect effectif de la vie privée ou familiale. Elles peuvent impliquer l'adoption de mesures visant au respect de la vie privée jusque dans les relations des individus entre eux ». Il est difficile d'identifier les circonstances dans lesquelles le respect de l'article 8 CEDH impose une action positive. La Cour estime qu'étant donné les contours imprécis de la notion de « respect » et la diversité des conditions et circonstances prévalant dans les États contractants, les mesures requises pour assurer le respect de la vie familiale peuvent considérablement varier d'un cas à l'autre. Le contrôle formel opéré par l'ordre juridique de l'Union européenne et consistant dans l'examen de la base légale et de la poursuite d'un but légitime ne semble pas aussi développé que dans l'ordre juridique du Conseil de l'Europe. Cela peut s'expliquer par le développement approfondi du contrôle matériel de proportionnalité effectué par la Cour de justice.

§2. La légitimité de l'ingérence selon un contrôle matériel

157 La pondération des restrictions. Les restrictions au droit à la protection des données personnelles doivent être justifiées tant d'un point de vue formel que d'un point de vue matériel. Cela implique que non seulement les restrictions doivent être prévues et connues par leurs destinataires mais aussi qu'elles soient conformes aux principes de nécessité et de proportionnalité. Tant la CourEDH que la Cour de justice sont appelées à effectuer le contrôle matériel de l'ingérence à travers le test de proportionnalité [1234] . Même si le principe de proportionnalité n'est pas expressément cité dans l' art. 8§2 de la CEDH, cette dernière effectue une pondération des intérêts en jeu afin de vérifier la nécessité des restrictions[1235]. Les critères pour une limitation matérielle du droit à la protection des données personnelles prévus à l'article 8 (2) CEDH et à l'article 52 (1) de la Charte sont similaires. Toutefois, à la différence de la Charte, l'article 8 (2) CEDH ajoute, que la limitation doit être « nécessaire dans une société démocratique ». Même si l'article 52 (1) de la Charte n'utilise pas la même expression, l'élément « société démocratique » est étroitement lié à l'ordre juridique de l'Union européenne

---

1233 CEDH, X. & Y. c/ Pays-Bas, arrê t du 26 mars 1985, § 23.

1234 Voy. sur cet aspect J. ZILLER, *Le principe de proportionnalité*, AJDA, 1996, pp. 185 et s., sp. p. 185. Le principe de proportionnalité a été systématisé par la Cour constitutionnelle allemande. Celle-ci a identifié trois principes distincts composant le principe de proportionnalité : le principe d'adéquation, le principe de nécessité et le principe de proportionnalité au sens étroit. Le principe d'adéquation (Geeignetheit) signifie que la mesure restrictive doit être appropriée à la réalisation de l'objectif poursuivi. Le principe de nécessité (Erforderlichkeit) implique que la mesure restrictive soit indispensable pour atteindre le but recherché. Ainsi, parmi les mesures restrictives adéquates, celle qui limite le moins le droit ou la liberté concernés doit être préférée. Enfin, le principe de proportionnalité au sens strict (Verhältnismässligkeit im engeren Sinne) exige que la mesure restrictive assure un juste équilibre des intérêts en présence.

1235 S. VAN DROOGHNBROECK, *La proportionnalité dans le droit de la Convention européenne des droits de l'homme. Prendre l'idée simple au sérieux,* Facultés Universitaires Saint-Louis Bruxelles - F.U.S.L., Parution 04/2002, p. 46 et ss; P. MUNZY, *La technique de la proportionnalité et le juge de la Convention européenne des droits de l'homme*, Presses Universitaires d'Aix-Marseille - P.U.A.M., Parution 10/2005, p. 27 et s.

comme une valeur fondamentale de l'Union (article 2 du TUE) [1236] . La proportionnalité constitue l'un des moyens pour parvenir à cet équilibre et son usage est désormais courant dans l'application de la Convention par les Juges de Strasbourg. Ceux-ci ont notamment rappelé à plusieurs reprises que « le souci d'assurer un juste équilibre entre les exigences de l'intérêt général de la communauté et les impératifs de la sauvegarde des droits fondamentaux de l'individu est inhérent à l'ensemble de la Convention »[1237]. Afin d'apprécier laproportionnalité d'une mesure restrictive, la CourEDH examine à la fois l'impact sur ce droit, les motifs, les effets dans le chef du requérant ainsi que le contexte[1238]. Les motifs doivent être « pertinents et suffisants », la nécessité d'une restriction doit être « établie de façon convaincante », les exceptions doivent être interprétées strictement[1239] et l'ingérence doit répondre à « un besoin social impérieux »[1240]. Ces exigences tendent à limiter la portée du pouvoir discrétionnaire de l'État, toutefois, les circonstances particulières du cas d'espèce et la situation interne de l'État à l'époque des faits peuvent, à l'inverse, l'élargir en pratique[1241]. Cependant il n'appartient pas à la CourEDH de statuer sur le fond des décisions rendues par les tribunaux nationaux. Son rôle consiste plutôt à examiner l'ensemble de l'affaire afin de déterminer si les autorités avaient des raisons « pertinentes » et des motifs « suffisants » pour prendre les mesures litigieuses. La Cour de justice recourt à un contrôle approfondi, et à un triple test de proportionnalité repris par la jurisprudence constitutionnelle allemande [1242] . Ainsi le principe revêt une exigence d'adéquation, de nécessité et de proportionnalité *stricto sensu* [1243] . C'est à travers la jurisprudence de la Cour de justice qu'on peut apprécier l'application des trois éléments composant le principe de proportionnalité[1244]. La Cour de justice examine premièrement, si la mesure envisagée répond bien à un objectif d'intérêt général de l'Union, deuxièmement, si la mesure ne dépasse pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs, pour finir avec le test de proportionnalité *stricto sensu* en vérifiant si les inconvénients

1236 Pour une analyse détaillée de la jurisprudence de la CEDH sur l'application des prescriptions de l'article 8 (2) de la Convention, voy. Avis 01/2014 de l'article 29, Groupe de travail sur l'application des concepts de nécessité et de proportionnalité et la protection des données.

1237 CEDH, Soering c/ Royaume-Uni, arrêt du 7 juillet 1989.

1238 Mc BRIDE, *Proportionality and the European Convention on Human Right*, in E. ELLIS (éditeurs), *The Principle of Proportionality in the Laws of Europe*, Oxford, Hart Publishing, 1999, pp. 23-35.

1239 Voy. arrêt Klass, op. cit., par. 42 ; arrêt Sunday Times (1979), op. cit., par. 65.

1240 Voy. par ex., CEDH, Observer et Guardian, par. 71.

1241 Voy. CEDH, Sunday Times, 1991, par. 50.

1242 J. ZILLER, *Le principe de proportionnalité*, préc., sp. p. 168.

1243 D. SIMON, *Le contrôle de proportionnalité exercé par le Cour de justice des communautés européennes*, *LPA*, 2007, n°46, p. 7 et s.

1244 M. FROMONT, « Le principe de proportionnalité », in R. BOUSTA (dir.), *La « spécificité » du contrôle constitutionnel français de proportionnalité*, RIDC 2007, spéc. p. 161.

auxquels aboutit la mesure ne dépassent pas ses avantages[1245]. Une analyse de la jurisprudence en matière de protection des données personnelles révèle que le test de proportionnalité de la CourEDH (A) s'avère moins approfondi que celui de la Cour de justice (B).

A. L'appréciation sur la proportionnalité de la mesure par la CourEDH

158 Une mise en balance nuancée. La CourEDH a aussi souligné que la nécessité d'une mesure « implique l'existence d'un "besoin social impérieux" »[1246] cela en raison du fait que la notion de « nécessité » ne devrait pas être interprétée d'une façon trop large, qui faciliterait le contournement de droits fondamentaux. Elle ne devrait pas non plus être interprétée trop littéralement, car ce serait placer la barre trop haut et il deviendrait alors excessivement difficile de justifier des activités qui peuvent légitimement interférer avec des droits fondamentaux. Dans la même affaire, la Cour s'est penchée sur le droit à la liberté d'expression, en tant que condition de l'existence et de l'épanouissement continu d'une « société démocratique ». Elle a déclaré que, dans cet esprit, « toute formalité, condition, restriction "ou sanction" imposée […] doit être proportionnée au but légitime poursuivi »[1247]. Enfin, la CEDH a expliqué que sonrôle était dès lors de décider « […]si les motifs donnés par les autorités nationales pour justifier les mesures concrètes d' "ingérence" qu'elles adoptent sont pertinents et suffisants» [1248] . Concernant le critère de proportionnalité dans l'affaire *S et Marper*, les requérants se plaignaient de ce que la conservation de leur profil ADN et de leurs empreintes digitales par les autorités constituait une ingérence injustifiée dans l'exercice de leurs droits garantis par l'article 8. Dans l'affaire *Z c. Finlande*1249 le problème était que des informations personnelles sur la requérante (et notamment sur son état de santé) avaient été rendues publiques. Dans les deux affaires, la CEDH a convenu que les activités en question poursuivaient un but légitime de prévention ou de détection d'infractions pénales et de défense de l'ordre. La CEDH s'est ensuite demandée si ces activités étaient « nécessaires dans une société démocratique ». À cet égard, la CEDH a considéré que les motifs n'étaient pas pertinents ou suffisants pour primer sur l'intérêt des requérants à la confidentialité des données. Ainsi dans l'affaire *Marper c. Royaume-Uni*[1250], elle a jugé disproportionné le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, qu'il ne traduisait pas un juste équilibre entre les intérêts publics et privés concurrents en jeu, et que l'État défendeur avait outrepassé

1245 Voy. sur le contrôle de proportionnalité *stricto sensu* l'affaire Sky Österreich afin de trancher la question de la conciliation entre la liberté d'expression et la liberté d'entreprise.C-293/12, op. cit., pt. 46 ; voy. CJUE (grande chambre), 22 janvier 2013, Sky Österreich, C-283/11.

1246 Voy. §48 de la décision.

1247 CEDH, Handyside c./Royaume-Uni, req. n° 5493/72,7 décembre 1976, point 49.

1248 CEDH, Handyside c./Royaume-Uni, req. n° 5493/72, 7 décembre 1976), point 50.

1249 CEDH, Z. c./Finlande, requête n° 22009/93, 25 février 1997.

1250 CEDH Gr. Ch. S et Marper c./Royaume-Uni, requêtes n° 30562/04 et n° 30566/04, 4 décembre 2008.

toute marge d'appréciation acceptable en la matière. Il s'agit selon elle d'une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique [1251] . Ainsi elle a souligné l'absence de prise en considération de « la nature et la gravité des infractions dont la personne était à l'origine soupçonnée » ou « de son âge » et a observé que la conservation n'était pas limitée dans le temps, quelles que soient la nature ou la gravité de l'infraction. L'insuffisance des garanties a aussi été soulignée, notamment le fait qu'il n'existe « que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données »[1252] et le manque de contrôle indépendant de la justification de la conservation des échantillons. Dans l'affaire *Laender c. Suède*, la Cour a explicité que l'exigence de nécessité dans une société démocratique implique que les restrictions à la protection des données personnelles correspondent à un besoin social impérieux mais aussi qu'elles soient proportionnées au but légitime poursuivi[1253]. De même dans l'arrêt *Z. c. Finlande* relative à la divulgation de données personnelles de santé dans le cadre d'un procès pénal, elle estime que la législation interne doit prévoir « des garanties appropriées pour empêcher toute communication ou divulgation de données à caractère personnel relatives à la santé qui ne serait pas conforme aux garanties prévues à l'article 8 de la Convention »[1254]. La CourEDH a précisé également dans son arrêt *Handyside/Royaume-Uni*[1255], que si l'adjectif « nécessaire » n'était « […] pas synonyme d' "indispensable" […], il n'a pas non plus la souplesse de termes tels qu' "admissible", "normal", "utile", "raisonnable" ou "opportun"». On compte à présent bon nombre d'affaires portées devant la CEDH qui se rapportent toutes à un ou plusieurs des critères adoptés par la CEDH pour déterminer si une mesure est « nécessaire dans une société démocratique » à travers la notion de besoin social impérieux (1), et de motifs pertinents et suffisants (2).

1) Un besoin social impérieux

Ainsi l'expression « besoin social impérieux » suppose un niveau plus élevé de gravité, d'urgence ou d'immédiateté associé au besoin que la mesure vise à satisfaire. Par conséquent, la définition d'un besoin social impérieux impliquera la prise en considération de plusieurs facteurs, qui peuvent inclure la préoccupation de l'opinion publique, la nature du problème à régler, etc. Ces facteurs influenceront certainement le choix des données à caractère personnel

---

1251 CEDH, Gr Ch. 4 décembre 2008, S. et Marper c/ Royaume-Uni, req. n°30562/04 et n°30566/04, Rec. 2008, § 125. D. De Beer, P. De Hert, G. Gonzalez Fuster, S. Gutwirth, « Nouveaux éclairages de la notion de "donnée personnelle" et application audacieuse du critère de proportionnalité », *Revue trimesterielle des droits de l'homme*, 2010, sp. pp. 144-154.

1252 CEDH, S et Marper/Royaume-Uni, requêtes n° 30562/04 et n° 30566/04, 4 décembre 2008, point 119.

1253 CEDH, 26 mars 1987, Leander c/ Suède, req. n°9248/81, A116, § 58

1254 CEDH, 25 février 1997, Z. c/ Finlande, req. n°22009/93, Rec. 1997-I, § 95

1255 CEDH, Handyside/Royaume-Uni, requête n° 5493/72,7 décembre 1976.

qui pourront éventuellement être traitées pour répondre à ce problème/besoin social impérieux. L'affaire Dudgeon/Royaume-Uni[1256] constitue un cas particulier examiné par la CEDH. Le requérant soutenait que la législation en vigueur en Irlande du Nord, érigeant en infractions pénales les actes homosexuels indépendamment du lieu où ils étaient pratiqués, de l'âge des personnes concernées, de leur consentement éventuel ou de leur capacité à donner leur consentement, violait les droits qui lui étaient garantis par l'article 8 de la Convention.

2) Des motifs pertinents et suffisants

Le deuxième critère retenu par la CEDH précise qu'une ingérence pour être nécessaire dans une société démocratique doit être justifiée par des motifs pertinents et suffisants liés aux exigences des deux critères précédents. Il est possible de conclure à l'existence de motifs pertinents et suffisants qui justifient une ingérence, si le critère de l'existence d'un besoin social impérieux et si la mesure proposée/adoptée est la mieux proportionnée ont été remplis. Cependant, en plus ou au lieu de s'en remettre à leur propre analyse, les autorités de l'ELSJ ou le législateur peuvent s'appuyer sur des études, des enquêtes ou d'autres informations pour étayer leur raisonnement. Dans l'affaire *K et T/Finlande* [1257] les requérants contestaient la décision prise par les autorités locales finlandaises de leur retirer la garde de deux enfants, qui avaient été placés dans un foyer d'accueil, avec des restrictions concernant les visites aux enfants. Bien que la mesure s'appliquât à deux enfants de la même famille, la CEDH a estimé que les autorités avaient fourni des motifs pertinents et suffisants pour justifier leur décision dans le cas d'un enfant, mais non de l'autre.

B. L'appréciation sur la proportionnalité de la mesure par la Cour de justice

159 Le rapport entre proportionnalité et nécessité. La proportionnalité est un principe général du droit de l'Union européenne prévoyant que « le contenu et la forme de l'action de l'Union ne doivent pas dépasser ce qui est nécessaire pour atteindre les objectifs des traités » [1258]. Ce principe est inscrit dans l'art. 5§4 du TUE, il exige que les actes des institutions de l'Union européenne soient appropriés pour atteindre les objectifs légitimes poursuivis par la législation en cause et ne dépassent pas les limites de ce qui est « approprié et nécessaire pour atteindre ces objectifs » [1259] . Ce principe « restreint l'exercice des pouvoirs des autorités

1256 CEDH, Dudgeon/Royaume-Uni, requête n° 7525/76, 22 octobre 1981.

1257 K et T/Finlande, requête n° 25702/94 (CEDH, 12 juillet 2001).

1258 Voy. art. 5§4 TUE.

1259 Voy. l'affaire CJUE C-62/14, Gauweiler, paragraph 67.

nationales en exigeant un équilibre entre les moyens utilisés et le but visé » [1260]. En vertu de l'article 52 (1) de la Charte, « sous réserve du principe de proportionnalité, les limitations à l'exercice des droits fondamentaux ne peuvent être appliquées que si elles sont nécessaires »[1261]. La proportionnalité au sens large englobe à la fois la nécessité et la pertinence d'une mesure, c'est-à-dire qu'il existe un lien logique entre la mesure et le but poursuivi. En outre, les avantages résultant de la mesure ne devraient pas être contrebalancés par les inconvénients que la mesure entraîne à l'égard de l'exercice des droits fondamentaux[1262]. Ce dernier élément décrit la proportionnalité dans un sens et constitue le test de proportionnalité *stricto sensu*. Ainsi la nécessité d'une mesure restrictive, telle qu'interprétée par la Cour de justice, implique également que les mesures adoptées doivent être les moins intrusives. Si une limitation est jugée strictement nécessaire, il est également nécessaire de déterminer si elle est proportionnée. Ainsi la proportionnalité d'une mesure restrictive signifie que les avantages résultant de la limitation devraient l'emporter sur les inconvénients que cette dernière entraîne pour l'exercice des droits fondamentaux en jeu [1263] . Au-delà de la proportionnalité des restrictions, une condition ultérieure est invoquée comme « limite aux limites »[1264] . Cette condition est celle relative à l'interdiction d'atteinte au contenu essentiel du droit fondamental. Si une restriction porte atteinte au contenu essentiel du droit fondamental, la mesure est contraire au droit de l'Union européenne. Si l'essence du droit est compromise, la limitation doit être considérée comme illégale, sans qu'il soit nécessaire de déterminer si elle sert un

---

1260 K. LENAERTS, P. VAN NUFFEL, *European Union Law*, Sweet and Maxwell, 3rd edition, London, 2011, p. 141.

1261 Comme le relève l'avocat général dans l'affaire Digital Ireland, « il faut conserver à l'esprit que les contrôles effectués au titre de ces deux dispositions sont de nature différente. La proportionnalité au sens de l'article 5, paragraphe 4, TUE est, en conjonction avec le principe de subsidiarité, un principe général régissant l'action de l'Union et conditionnant l'adoption de tous les actes des institutions. Elle a plus particulièrement vocation à canaliser l'intervention de l'Union dans le respect des compétences des États membres. La proportionnalité au sens de l'article 52, paragraphe 1, de la Charte est une condition de légitimité de toute limitation de l'exercice des droits fondamentaux. Si les contrôles opérés au titre des deux dispositions peuvent suivre le même parcours, ils ne s'exercent pas, en revanche, avec les mêmes rigueurs. Cela précisé, il importe de rappeler que, dans un domaine de compétence partagée, tel que celui du marché intérieur (72), il incombe au législateur de l'Union de déterminer les mesures qu'il estime nécessaires pour atteindre les objectifs visés, tout en respectant les principes de subsidiarité et de proportionnalité consacrés à l'article 5 TUE ». Voy. en ce sens les conclusions de l'avocat général points 89-90.

1262 Voy. l'affaire C-83/14, para. 123. La Cour déclare : « Par ailleurs, et à supposer qu'aucune autre mesure aussi efficace ne puisse être identifiée, la juridiction de renvoi devra encore vérifier si les inconvénients causés par la pratique litigieuse ne sont pas démesurés par rapport aux objectifs poursuivis et si cette pratique ne porte pas une atteinte excessive aux intérêts légitimes des personnes habitant les quartiers concernés ». Voy. également l'avis AG dans les affaires jointes C-203/15 et C-698/15, Tele2 Sverige AB, paragraphes 132,172, 247, 248 déclarant que la CJUE dans l'affaire Digital Rights Ireland « le régime établi par la directive 2006/24 dépassait les limites de ce qui était strictement nécessaire » Il a ensuite déclaré que « l'exigence de proportionnalité dans un sens étroit (*stricto sensu*) au sein d'une société démocratique couvre à la fois de l'article 15 (1) de la directive 2002/58 et de l'article 52 (1) de la Charte. Ainsi, comme constamment interprétée par la jurisprudence, une mesure qui interfère dans les droits fondamentaux ne peut être considérée comme proportionnelle que si les inconvénients causés ne sont pas disproportionnés par rapport aux objectifs poursuivis ». La cour a également souligné que l'exigence de proportionnalité dans le cas particulier de la conservation d'une telle quantité de données « ouvre un débat sur les valeurs qui doivent prévaloir dans une société démocratique et, en fin de compte, sur quel genre de société nous souhaitons vivre ».

1263 Voy. EDPS, Necessity Toolkit, 2017, p. 5.

1264 Cette interdiction implique l'existence d'un noyau dur intouchable au sein de chaque droit fondamental qui ne saurait jamais être atteint, quel que soit le but légitime poursuivi. Elle est apparue dans la loi fondamentale allemande, ainsi l'article 19 alinéa 2 de la Loi fondamentale allemande interdit de porter « atteinte à la substance d'un droit fondamental ».

objectif d'intérêt général et satisfait aux critères de nécessité et de proportionnalité[1265]. Au contraire, une restriction qui respecte le contenu essentiel du droit à la protection des données personnelles doit être en mesure de passer le test de proportionnalité. Cette condition est parfois invoquée comme « limite aux limites »[1266]. Si la mesure envisagée respecte le contenu du droit (1), le juge peut examiner la restriction sous l'angle de la proportionnalité (2).

1) Le respect du contenu essentiel du droit fondamental à la protection des données personnelles « limite aux limites »

160 Le noyau dur du droit fondamental à la protection des données personnelles. D'après l'article 52 de la Charte, toute limitation des droits fondamentaux doit être prévue par la loi, respecter le contenu essentiel de ces droits ainsi que le principe de proportionnalité, faute de quoi la législation de l'Union est considérée comme nulle[1267]. Une mesure restrictive méconnaît le contenu essentiel du droit lorsqu'elle vide le droit de son essence, de son contenu et que l'individu se trouve dans l'impossibilité d'exercer son droit. Si le juge, après avoir évalué l'existence d'une base légale, estime que le contenu des droits a été méconnu, il ne procède pas

1265 Pour un commentaire sur le rapport entre contenu essentiel et proportionnalité Voy. R. SHUTZE, *Three bills of rights for the european Union* , 30 yearbook of european law, 2011, p. 131-140.

1266 Cela implique l'existence d'un noyau dur intouchable au sein de chaque droit fondamental qui ne saurait jamais être atteint, quel que soit le but légitime poursuivi. L'interdiction de porter atteinte à la substance des droits fondamentaux a été dégagée par la Cour européenne dès l'affaire linguistique belge où elle a pour la première fois exercé un contrôle de proportionnalité des restrictions étatiques aux droits fondamentaux v. CEDH, 23 juillet 1968, Affaire « relative à certains aspects du régime linguistique de l'enseignement en Belgique » c/ Belgique, req. n°1474/62 ; 1677/62 ; 1691/62 ; 1769/63 ; 1994/63 ; 2126/64, A6, § 5. Cette exigence a été appliquée par la Cour à de nombreuses reprises v. P. MUNZY, La technique de la proportionnalité et le juge de la CEDH, préc., notes 145 et 146, sp. pp. 295-296. L'interdiction d'atteinte au contenu essentiel des droits fondamentaux a également été dégagée par la Cour de justice de l'Union européenne avant d'être consacrée par la Charte des droits fondamentaux. Dans la mesure où cette interdiction est inscrite dans plusieurs constitutions nationales et a été dégagée par la Cour européenne des droits de l'homme, le juge communautaire avait là une source d'inspiration bien établie v. R. TINIERE, *L'office du juge communautaire des droits fondamentaux*, Bruxelles, Bruylant, coll. Droit de l'Union européenne, 2007, 708 p.

1267 Voy. COM(2010) 573 final. Dans ce document, la Commission a adopté une « stratégie pour la mise en œuvre effective de la Charte » qui vise à promouvoir une « culture des droits fondamentaux » à toutes les étapes de la procédure législative, du projet initial de proposition jusqu'à la vérification de la légalité du texte définitif, en passant par l'analyse d'impact de la Commission. Comparé à la pratique « d'auto-certification » qui avait cours précédemment, en vertu de laquelle le législateur se contentait de déclarer le texte législatif « conforme » à la Charte (comme c'est le cas, par exemple, pour la décision cadre sur le mandat d'arrêt européen), les nouveaux textes de l'Union mentionnent clairement les droits fondamentaux concernés, en particulier lorsqu'il est nécessaire de trouver un équilibre entre plusieurs droits différents. Depuis 2010, les personnels de la Commission doivent s'appuyer sur la « check-list » suivante qui reflète le contenu de l'article 52, paragraphe 2, de la Charte: 1. Quels sont les droits fondamentaux concernés? 2. S'agit-il de droits absolus (qui ne peuvent être soumis à aucune limitation – par exemple, la dignité humaine et l'interdiction de la torture) ? 3.Quel sont les impacts des différentes options politiques envisagées sur les droits fondamentaux? S'agit-il d'impacts positifs (promotion des droits fondamentaux) ou négatifs (limitations des droits fondamentaux)? 4. Les options ont-elles à la fois des impacts positifs et négatifs en fonction des droits fondamentaux concernés (par exemple, impact négatif sur la liberté d'expression et positif sur la propriété intellectuelle) ? 5. Les limitations éventuelles des droits fondamentaux seraient-elles formulées d'une manière précise et prévisible ? 6. Est-ce que, le cas échéant, des limitations apportées aux droits fondamentaux seraient nécessaires pour réaliser un objectif d'intérêt général ou pour protéger les droits et libertés d'autrui (lesquels) ? Seraient proportionnées à l'objectif poursuivi et respecteraient le contenu essentiel des droits fondamentaux concernés ? Voy. égalmeent les conclusions du Conseil sur le rapport 2013 de la Commission sur l'application de la Charte des droits fondamentaux de l'UE et sur la cohérence entre les aspects internes et externes de la protection et de la promotion des droits de l'homme dans l'Union européenne, 5 et 6 juin 2014.

au test de nécessité et de proportionnalité, déclarant l'illégitimité de la mesure [1268] . Cette interdiction repose sur l'idée qu'il existerait au sein de chaque droit fondamental un noyau dur [1269] lorsqu'il s'agit d'identifier sa portée et de le distinguer du principe de proportionnalité[1270]. Si l'essence du droit est affectée, la mesure est illégale et il n'est pas nécessaire de continuer avec l'évaluation de sa compatibilité avec les règles énoncées à l'article 52 de la Charte. C'est peu fréquent que les juges de la Cour de Luxembourg, dans l'évaluation de la conformité de la législation secondaire par rapport aux droits fondamentaux protégés par la Charte, se fondent sur une analyse séparée des deux profils prévus à l'art. 52, par. 1, à savoir la violation du contenu essentiel et la proportionnalité des restrictions. Cette approche a été inaugurée par l'arrêt *Digital Rights et Schrems*. Dans l'affaire *Digital Ireland*, la Cour de justice s'est livrée à un contrôle de proportionnalité, étant donné que le contenu des communications n'avait pas été exploité et que, donc, une violation du contenu essentiel des droits énoncés aux articles. 7, 8 et 52.1 de la Charte ne pouvait pas avoir lieu (a). Toutefois, lorsque le contrôle concerne la dimension externe à l'Union, notamment dans l'affaire qui a invalidé l'accord *Safe Harbor* avec les États-Unis, la Cour de justice a conclu que ce système constituait une violation du contenu essentiel des droits fondamentaux contenus dans les articles 7, 8 et 47 de la Charte (b).

a) La non violation du contenu essentiel

161 L'appréciation du respect du contenu essentiel du droit à la protection des données dans l'affaire *Digital Right*. La Cour de justice a développé le principe du respect du contenu

1268 European Data Protection Supervisor, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit, 11 avril 2017, www.edps.europa.eu, p. 4 ; pour un exemple voy. CJUE (grande chambre), 6 octobre 2015, Schrems, C-362/14, op. cit., pt. 95 : « De même, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte ».

1269 While the case-law is not abundant regarding the conditions under which the essence of a right is affected, one can state that this would be the case if the limitation goes so far that it empties the right of its core elements and thus prevents the exercise of the right. In Schrems, the CJEU found that the essence of the right to an effective remedy was affected. »Legislation not providing for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain enshrined in Article 47 of the Charter" (paragraph 95). It then did not go on with the examination whether such a limitation was necessary but invalidated -also on other grounds- the Commission's Decision on the adequacy of the Safe Harbour Principles. In Digital Rights Ireland, the CJEU found that the essence of the right to respect for private life was not affected since the Data Retention directive did not allow the acquisition of knowledge of the content of electronic communications. The CJEU similarly found that the essence of the right to the protection of personal data is not affected because the Data Retention directive provided for the basic rule that appropriate organisational and technical measures should be adopted against accidental or unlawful destruction, loss or alteration of the retained data (paragraphs 39, 40). Only then did the Court proceed to examine the necessity of the measure. The deprivation of review, by an independent authority, of compliance with the level of protection guarnteed by EU law could also affect the essence of the right to the protection of personal data as this is expressly required in Article 8(3) of the Charter and »If that were not so, persons whose personal data was retained would be deprived of the right, guararnteed in Article 8(1) and (3) of the Charter, to lodge with the national supervisory authorities a claim seeking the protection of their data", see Tele2 Sverige AB, paragraph 123.

1270 M. HOTTELIER, « Le noyau intangible des libertés », in Meyer-Bisch Patrice, Marie Jean-Bernard (Ed.). *Noyau intangible des droits de l'homme: VIIe Colloque interdisciplinaire sur les droits de l'homme*, Fribourg, Ed. universitaires, 1991, p. 67-74.

essentiel du droit à la protection des données personnelles à travers sa jurisprudence[1271]. Dans l'arrêt *Digital Right Ireland*[1272] la Cour a annulé la directive sur la conservation des données[1273] en raison d'une violation du principe de proportionnalité, mais pour ce faire elle s'est livrée au contrôle du respect du contenu essentiel du droit à la protection des données personnelles. Il est possible de souligner que concernant l'application de l'article 52.1 de la Charte, la Cour de justice n'avait jamais séparé le profil qui concerne l'application du principe de proportionnalité et celui qui concerne la violation du contenu essentiel des droits. Dans cette affaire, la Cour de justice relève, que même si la conservation des données imposée par la directive 2006/24 constitue une ingérence particulièrement grave dans ces droits, elle n'est pas de nature à porter atteinte audit contenu étant donné que, ainsi qu'il découle de son article 1er, paragraphe 2, cette directive ne permet pas de prendre connaissance du contenu des communications électroniques en tant que tel. Selon le raisonnement de la Cour, cette conservation des données n'est pas de nature à porter atteinte au contenu essentiel du droit fondamental à la protection des données à caractère personnel consacré à l'article 8 de la Charte. Cela en raison du fait que la directive 2006/24 prévoit, à son article 7, une règle relative à la protection et à la sécurité des données selon laquelle, certains principes doivent être respectés par les fournisseurs de services de communications électroniques et c'est aux États membres de veiller à l'adoption de mesures techniques et organisationnelles appropriées contre la destruction accidentelle ou illicite, la perte ou l'altération accidentelle des données. De plus, le contenu des communications n'est pas enregistré.[1274]Au final, le noyau dur du droit à la protection des données personnelles est respecté puisque l'art. 7 de la directive 2006/24/CE impose le respect des certains principes de sécurité et protection des données (même si énoncé d'une façon générique)[1275] et même si la conservation des données constitue une ingérence dans la vie privée cela ne permet pas de capter le contenu des conversations. Toutefois, même si la conservation constitue une ingérence particulièrement grave dans le droit au respect de la vie privée, elle n'est pas susceptible de nuire à l'essence de ces droits étant donné que la directive ne permet pas d'acquérir une connaissance du contenu des communications électroniques. Cela n'affecte pas non plus l'essence même du droit à la protection des données personnelles, car certains principes de protection des données et de sécurité des données doivent être respectés par les fournisseurs de services de communications électroniques accessibles au public ou de réseaux de communications publiques - afin d'assurer que des mesures techniques et organisationnelles appropriées soient adoptées contre la destruction accidentelle ou illégale, la perte accidentelle

---

1271 A. VON BOGDANDY, A. VON KOTTMANN, M. ANTPOHLRT, C. DICKSCHEN, J. HENTEI, R. SOLANGE, « Protecting the essence of fundamental rights against EU Member States », *Common Market Law Review* 49.2, 2012, p. 489-519.

1272 CJUE, Grande Chambre, 8 avril 2014, Digital Rights Ireland Ltd & Michael Seitlinger e.a., affaires jointes C-293/12 & C-594/12.

1273 Directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54).

1274 CJUE, Digital Rights Ireland, Aff. C-293/12 et C-594/12, 8 avril 2014, § 39-40.

1275 CJUE, G. Ch., 8 avril 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C-293/12 et C-594/12, §§ 38-40.

ou l'altération des données[1276]. La Cour de Luxembourg passe alors au test de proportionnalité strict[1277]. Il s'agit d'un arrêt majeur pour la protection du droit des données personnelles, bien que la conservation des données requise par la directive pouvait être jugée adaptée pour atteindre l'objectif recherché[1278], l'atteinte particulièrement étendue et grave de la directive aux droits fondamentaux n'était pas limitée au strict nécessaire[1279]. Autrement dit, la lutte contre la criminalité organisée et contre le terrorisme, au nom de la préoccupation de sécurité intérieure, ne saurait autoriser des atteintes inutiles et inadéquates, inappropriées et injustifiées aux droits fondamentaux des citoyens européens. De plus, la conservation des données en vue de leur transmission éventuelle aux autorités nationales compétentes répond effectivement à un objectif d'intérêt général, à savoir la lutte contre la criminalité grave ainsi que, en définitive, la sécurité publique. Toutefois, la Cour estime qu'en adoptant la directive sur la conservation des données, le législateur de l'Union a excédé les limites qu'impose le respect du principe de proportionnalité. Premièrement, la directive était disproportionnée car elle couvrait, d'une manière générale, toutes les personnes, tous les moyens de communications électroniques sans différenciation ou limitation[1280]. Deuxièmement, elle ne fournissait aucun critère objectif pour permettre aux autorités nationales compétentes d'accéder aux données concernant les « crimes graves » mais renvoyait à la définition de « crime grave » par chaque État membre. Elle ne définissait pas non plus les conditions de fond et de procédure pour l'accès et l'utilisation des données par les autorités nationales compétentes[1281]. Le législateur communautaire aurait dû prévoir l'exigence que l'accès aux données puisse avoir lieu seulement après un examen préalable par un tribunal ou un organisme administratif indépendant.

Troisièmement, la directive ne prévoyait pas de critères objectifs permettant de déterminer la période de conservation afin de faire en sorte qu'elle se limite au strict nécessaire, mais elle imposait une période de conservation d'au moins six mois, sans établir une distinction entre les catégories de données en fonction des personnes concernées[1282]. C'est pourquoi la Cour de

---

1276 Voy. § 38-40.

1277 Voy. §48 : « Compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict ».

1278 L'objectif général poursuivi semble relever pour la Cour de l'évidence (point 44) : il s'agit de « garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves », donc « de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique » (point 41), ce qui est présenté comme un « objectif d'intérêt général de l'Union » (point 42 ; voy. CJUE, grande chambre, 23 novembre 2010, Tsakouridis, affaire C 145/09, points 46 et 47). Certes, il estime que « la lutte contre la criminalité grave, notamment contre la criminalité organisée et le terrorisme, est d'une importance primordiale pour garantir la sécurité publique et son efficacité peut dépendre dans une large mesure de l'utilisation des techniques modernes d'enquête » ; néanmoins, il ajoute immédiatement que « un tel objectif d'intérêt général, pour fondamental qu'il soit, ne saurait à lui seul justifier qu'une mesure de conservation telle que celle instaurée par la directive 2006/24 soit considérée comme nécessaire aux fins de ladite lutte » (point 51).

1279 T. KONSTADINIDES, « Destroying Democracy on the Ground of Defending It ? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem », *European Law Review*, 2017, p.722.

1280 Voy. l'arrêt § 56.

1281 Voy. l'arrêt § 60-61.

1282 Voy. l'arrêt § 63.

justice a estimé que le législateur de l'Union n'avait pas respecté le principe de proportionnalité et que les dispositions de la directive représentaient une atteinte particulièrement grave portant atteinte au contenu essentiel des droits garantis (art. 7 et 8)[1283]. Contrairement aux conclusions de l'Avocat général qui s'était penché sur la question de savoir si la base légale de la directive avait été respectée, la Cour de justice se penche directement sur le respect du principe de proportionnalité et le respect du contenu essentiel[1284]. Avant 2014, la Cour de justice n'avait jamais constaté elle-même sur le fondement du droit à la protection des données personnelles, l'existence d'une disproportion entre les objectifs visés et l'atteinte contestée. Le plus souvent elle avait préféré renvoyer la question à l'appréciation des autorités nationales. Il est donc possible de constater une évolution de la jurisprudence de la Cour de justice.

162 L'appréciation du respect du contenu essentiel du droit à la protection des données dans l'affaire PNR. La Cour de justice s'est à nouveau penchée sur le respect du contenu essentiel du droit à la protection des données dans son avis concernant la conclusion de l'accord avec le Canada visant à garantir la sécurité publique au moyen d'un transfert des données *PNR* et de l'utilisation de celles-ci dans le cadre de la lutte contre des infractions terroristes et la criminalité transnationale grave, elle a statué sur l'objectif d'intérêt général et le respect du contenu essentiel des droits fondamentaux en cause[1285]. Cet objectif constitue, comme il ressort de la jurisprudence de la Cour, un objectif d'intérêt général de l'Union susceptible de justifier des ingérences, même graves, dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte. Au demeurant, la protection de la sécurité publique contribue également à la protection des droits et des libertés d'autrui. À cet égard, l'article 6 de la Charte énonce le droit de toute personne non seulement à la liberté, mais également à la sûreté[1286]. En ce qui concerne le contenu essentiel du droit fondamental au respect de la vie privée, consacré à l'article 7 de la Charte, même si les données PNR peuvent, le cas échéant, révéler des informations très précises sur la vie privée d'une personne, la nature de ces informations est limitée à certains aspects de cette vie privée, relatifs en particulier aux voyages aériens entre le Canada et l'Union. Quant au contenu essentiel du droit à la protection des données à caractère personnel, consacré à l'article 8 de la Charte, l'accord envisagé circonscrit, à son article 3, les finalités du traitement des données PNR et prévoit, à son article 9, des règles destinées à assurer, notamment, la sécurité, la confidentialité et l'intégrité de ces données, ainsi qu'à les protéger contre les accès et les traitements illégaux. Dans ces conditions, les ingérences que comporte l'accord envisagé sont susceptibles d'être justifiées par un objectif d'intérêt général de l'Union et ne sont pas de nature à porter atteinte au contenu essentiel des droits fondamentaux consacrés aux articles 7 et 8 de

---

1283 M.-L BASILIEN-GAINCHE, « Une prohibition européenne claire de la surveillance électronique de masse », in *La Revue des droits de l'homme*, Actualités Droits-Libertés, mis en ligne le 14 mai 2014, consulté le 6 avril 2017, disponible à l'adresse: http://revdh.revues.org/746

1284 L'avocat général estimait que la directive 2006/24 était incompatible avec l'article 52, paragraphe 1, de la Charte, puisque ses dispositions sur la conservation obligatoire des données personnelles ne sont pas accompagnées des garanties nécessaires pour encadrer l'accès et leur utilisation. Le critère de prévision de la loi doit être vu comme un critère substantiel et non formel. La limitation du droit doit être accompagnée des garanties, Voy. point § 131 et § 111 des conclusions.

1285 Voy. l'Avis 1/15 de la CJUE du 26 juillet 2017 point 148-153.

1286 Voy., en ce sens, arrêts du 8 avril 2014, Digital Rights Ireland e.a., C 293/12 et C 594/12, EU:C:2014:238, points 42 et 44, ainsi que du 15 février 2016, N., C-601/15 PPU, EU:C:2016:84, point 53.

la Charte. Toutefois La CJUE estime que si le transfert, la conservation et l'utilisation systématiques de l'ensemble des données de dossiers passagers que prévoit l'accord sont pour l'essentiel admissibles, plusieurs dispositions du projet ne répondent pas aux exigences découlant des droits fondamentaux de l'Union.

b) La violation du contenu essentiel du droit à la protection des données personnelles

163 **L'appréciation de la violation du contenu essentiel du droit à la protection des données personnelles dans l'affaire *Schrems.*** Dans l'affaire *Schrems*, le requérant, ressortissant autrichien, était un utilisateur de Facebook Ireland, une filiale de Facebook Inc. située aux États-Unis. Les données personnelles des utilisateurs qui résident dans l'UE sont transférées aux serveurs de Facebook Inc. aux États-Unis et traitées ultérieurement. Le requérant a demandé d'interdire à Facebook Ireland de transférer ses données personnelles aux États-Unis, sur la base de la considération que les États-Unis ne garantiraient pas une protection adéquate contre les activités de surveillance qui y sont engagées par les autorités publiques, en particulier la NSA[1287]. Cela fait suite au contexte marqué par les révélations d'E. Snowden sur le programme Prism et l'espionnage de l'Europe par les États-Unis. Le défendeur a rejeté la plainte en raison de l'absence de preuve que ses données avaient été collectées par la NSA et sur la base de la décision 2000/520 de la Commission qui avait constaté que les États-Unis garantissent un niveau de protection adéquat dans le programme *Safe Harbor*. La Cour estime, face au refus de l'autorité de contrôle de statuer sur la conformité de la décision de la Commission 2000/520 à la situation du requérant, que selon la législation des États-Unis, les autorités des États-Unis ne sont pas tenues de se conformer aux principes de la sphère de sécurité prévus par l'accord *Safe Harbor* conclu sur la base de la Décision 2000/520. Ainsi, la Décision 2000/520 ne contenait pas suffisamment de garanties concernant les mesures des États-Unis qui assurent l'adéquation de la protection des données en raison du droit interne ou aux engagements internationaux. Au contraire, elle permet plutôt l'ingérence dans le droit fondamental au respect de la vie privée des personnes dont les données personnelles sont transférées de l'UE aux États-Unis[1288]. Cependant, lorsque de telles restrictions sont prises par les institutions et organes de l'Union européenne, la Cour de justice ne semble pas reconnaître une marge d'appréciation équivalente aux États[1289]. Ainsi dans l'affaire *Parlement c.*

1287 S. PEYROU, « La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel », *RTDE*, 2015, n°1, p. 117.

1288 Voy. §82-87.

1289 C'est à travers les recours en annulation et les recours préjudiciels en appréciation de validité d'actes des institutions et des organes de l'Union européenne qu'une telle marge d'appréciation pourrait être évaluée. Mais cette possibilité fait l'objet de débats en doctrine. Voy. sur les problèmes théoriques liés à la reconnaissance d'une telle marge et son rejet v. R. TINIERE, *L'office du juge communautaire des droits fondamentaux*, préc., spéc. p. 598.

Conseil[1290], la Cour n'a pas eu besoin de contrôler le respect du principe du proportionnalité puisqu'elle a annulé pour défaut de base légale la décision du Conseil concernant la conclusion d'un accord entre la Communauté européenne et les États- Unis sur le traitement et le transfert de telles données et la décision de la Commission reconnaissant un niveau de protection adéquat garanti par les États-Unis au sens de la directive n° 95/46 CE. Cependant l'avocat général, dans ses conclusions [1291] , avait proposé de valider les deux décisions en ce qu'elles étaient proportionnées au but légitime poursuivi de lutte contre le terrorisme, eu égard notamment à la marge d'appréciation dont bénéficieraient les institutions et organes de l'Union en la matière, et s'était livré à un contrôle de proportionnalité. La Cour de justice estime que les mesures objets du litige portaient atteinte au contenu essentiel du droit. Ainsi, une réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par les articles 7 et 8 de la Charte[1292]. De même, une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant, ou d'obtenir la rectification ou la suppression de telles données, ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte [1293] . Or, la Cour rappelle que l'institution d'autorités indépendantes dans les États membres résulte, selon une jurisprudence constante, d'une double exigence issue de l'article 8, paragraphe 3, de la CDFUE et de l'article 16, paragraphe 2, TFUE et constitue à ce titre un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel. Le délicat exercice de conciliation entre le respect du droit fondamental à la vie privée et les intérêts économiques liés à la libre circulation des données à caractère personnel que doivent opérer ces instances implique que celles-ci puissent disposer d'un large éventail de pouvoirs dont, notamment, des pouvoirs d'investigation et des pouvoirs effectifs de sanction et d'intervention tels que celui d'interdire temporairement ou définitivement un traitement de données ou celui d'ester en justice[1294]. La portée de cet arrêt conduit à considérer tout système de surveillance de masse comme une violation en soi du contenu essentiel de la vie privée. Après vérification que la condition relative à l'interdiction d'atteinte au contenu essentiel du droit fondamental invoquée comme « limite aux limites »[1295] est respectée, le juge peut examiner la restriction sous l'angle de la proportionnalité.

1290 Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes, aff. C-317/04 et C-318/04.

1291 Voy. les Conclusion de l'Avocat général P. Léger, présentées le 22 novembre 2005, Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes, aff. C-317/04 et C-318/04.

1292 Sur la violation du contenu essentiel du droit, voy. en ce sens, arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, point 39.

1293 Voy. point 88-95 de la décision.

1294 Voy. § 42 et 43 de la décision.

1295 Cela implique l'existence d'un noyau dur intouchable au sein de chaque droit fondamental qui ne saurait jamais être atteint, quel que soit le but légitime poursuivi. L'interdiction de porter atteinte à la substance des droits fondamentaux a été dégagée par la Cour européenne dès l'affaire linguistique belge où elle a pour la première fois exercé un contrôle de

2) L'intensité du test de proportionnalité

164 La distinction entre nécessité et proportionnalité de la mesure. La prémisse est qu'il est possible de procéder au test de proportionnalité seulement après l'évaluation de la nécessité d'une mesure. La proportionnalité devrait clairement être distinguée de la nécessité[1296]. Ainsi dans des affaires récentes, lorsque les mesures restrictives du droit à la protection des données personnelles n'ont pas passé le test de nécessité, la Cour de justice n'a pas procédé à l'évaluation de la proportionnalité[1297]. Cependant, la nécessité de la mesure envisagée a un lien avec la proportionnalité. En effet, la proportionnalité dans un sens large englobe à la fois la nécessité et la pertinence de la mesure. Une mesure restrictive est considérée comme nécessaire s'il y a un lien logique entre la mesure et l'objectif (légitime) poursuivi. De plus, dans le cas d'une mesure qui respecte le principe de proportionnalité consacré à l'article 52 (1) de la Charte, les inconvénients résultant de la mesure ne doivent pas dépasser les avantages. Ce dernier élément décrit la proportionnalité dans un sens étroit. Dans son arrêt *Schwarz*[1298], la Cour de justice a examiné de plus près la question de la proportionnalité et de la nécessité. La Cour de justice a estimé qu'« il convient de vérifier si les limitations apportées auxdits droits sont proportionnées au regard des buts et des objectif poursuivis. Il y a lieu ainsi d'examiner si les moyens mis en œuvre par ce règlement sont aptes à réaliser ces buts et ne vont pas au-delà de ce qui est nécessaire pour les atteindre »[1299] . « En ce qui concerne, ensuite, l'examen du caractère nécessaire d'un tel traitement, le législateur est notamment tenu de vérifier si des mesures moins attentatoires aux droits reconnus par les articles 7 et 8 de la Charte sont concevables tout en contribuant de manière efficace aux buts de la réglementation de l'Union

proportionnalité des restrictions étatiques aux droits fondamentaux v. CEDH, 23 juillet 1968, Affaire « relative à certains aspects du régime linguistique de l'enseignement en Belgique » c/ Belgique, req. n°1474/62 ; 1677/62 ; 1691/62 ; 1769/63 ; 1994/63 ; 2126/64, A6, § 5. Cette exigence a été appliquée par la Cour à de nombreuses reprises v. P. MUNZY, *La technique de la proportionnalité et le juge de la CEDH* préc. pp. 295-296. L'interdiction d'atteinte au contenu essentiel des droits fondamentaux a également été dégagée par la Cour de justice de l'Union européenne avant d'être consacrée par la Charte des droits fondamentaux. Dans la mesure où cette interdiction est inscrite dans plusieurs constitutions nationales et a été dégagée par la Cour européenne des droits de l'homme, le juge communautaire avait là une source d'inspiration bien établie v. R. TINIERE, *L'office du juge communautaire des droits fondamentaux*, Préc.p708.

1296 Voy. EDPS (2017), *Necessity Toolkit*, Brussels, 11 April 2017. Disponible à l'adresse : https://edps.europa.eu/data-protection/our-work/publications/papers/necessity-toolkit_fr

1297 Dans l'affaire Digital Righs (aff. Jointes C-293/12, et C-594/12) la Cour a décidé que la proportionnalité était composée de la pertinence et de la nécessité de la mesure (paragraphe 46). Elle a ensuite établi que la limitation des droits protégés par les articles 7 et 8 ne sont pas nécessaires (voy. paragraphe 65) et elle a donc conclu que les limitations ne sont pas proportionnelles (paragraphe 69). De même, dans l'affaire C-362/14, Schrems (paragraphes 92, 93) où la CJUE a analysé la nécessité et a trouvé la décision *Safe Harbor* invalide, sans faire référence à la proportionnalité (paragraphe 98).

1298 Voy. L'affaire C-291/12, Schwarz/Stadt Bochum (CJUE, 17 octobre 2013) M. Schwarz contestait le refus des autorités de la ville allemande de Bochum de lui délivrer un passeport (UE) sans que soient relevées deux de ses empreintes digitales devant être stockées sur ce passeport. Cette obligation découle du règlement (CE) n° 2252/2004 du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage.

1299 Voy. § 40 de l'arrêt.

en cause »[1300]. Plus récemment encore, l'avocat général Pedro Cruz Villalón a précisé, dans ses conclusions sur les actions engagées en Irlande et en Autriche contre la directive 2006/24/CE[1301] sur la conservation des données, que si la directive poursuivait bien une fin légitime, elle n'était cependant pas nécessaire du fait de son «[incompatibilité] avec le principe de proportionnalité en ce qu'elle impose aux États membres de garantir [que les données] soient conservées pendant une durée dont la limite supérieure est fixée à deux ans»[1302]. Il s'ensuit que, faute de motifs pertinents et suffisants justifiant la période de conservation de deux ans, la directive n'est pas nécessaire. Cela a conduit à une intrusion disproportionnée dans les vies privées de clients dont les données sont conservées, en l'absence de tout soupçon, pendant une durée maximale de deux ans.

165 Le contrôle de stricte nécessité par la jurisprudence. Dans les cas récents, la CJUE a évalué si les objectifs légitimes poursuivis par la législation de l'Union ne dépassaient pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs[1303].La prémisse est que seule une mesure qui s'est avérée nécessaire au sens de l'art. 52 (1) de la Charte peut être soumise au test de proportionnalité. Ainsi, dans l'affaire *Schrems*, la Cour de justice a invalidé la décision *Safe Harbor* puisqu'elle n'avait pas passé le test de stricte nécessité, sans besoin de passer par le test de proportionnalité[1304] . Ainsi dans cette décision, la Cour estime que la protection du droit fondamental au respect de la vie privée au niveau de l'Union exige que les dérogations à la protection des données à caractère personnel et les limitations de celle-ci s'opèrent dans les limites du strict nécessaire[1305]. Il résulte que, une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi et sans que soit prévu un critère objectif permettant de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure à des fins précises, strictement restreintes et susceptibles de justifier l'ingérence que comportent tant l'accès que l'utilisation de ces données, n'est pas limitée au strict nécessaire[1306]. L'exigence de stricte nécessité a une conséquence sur le contrôle judiciaire. En d'autres termes, le pouvoir discrétionnaire du législateur dans le choix

---

1300 Voy. §46 de l'arrêt.

1301 Voy. Les affaires jointes C-293/12 et C-594/12

1302 Communiqué de presse sur les conclusions de l'avocat général, Disponible à l'adresse : http://europa.eu/rapid/press-release_CJE-13- 157_fr.htm.

1303 Voy. affaire CJUE, C-293/12, § 50.

1304 Voy. §98 de l'arrêt.

1305 La Cour de justice rappelle ici la jurisprudence Data Retention, voy. arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, point 52.

1306 La Cour de justice rappelle ici sa jurisprudence Data Retention, voy. en ce sens, en ce qui concerne la directive 2006/24/CE du Parlement européen et du Conseil, du 15 mars 2006, sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE (JO L 105, p. 54), arrêt Digital Rights Ireland e.a., C 293/12 et C 594/12, points 57 à 61.

de la mesure est limité[1307]. Ainsi une mesure restrictive doit prévoir quel droit est limité[1308], doit se justifier par l'objectif poursuivi, conformément à l'article 52 (1) de la Charte, il doit s'agir d'une mesure nécessaire afin d'atteindre l'intérêt général reconnu par l'Union ou afin de protéger les droits et libertés d'autrui. Les objectifs d'intérêt général de l'Union comprennent, par exemple, les objectifs généraux mentionnés à l'article 3 ou 4 (2) du TUE et d'autres intérêts protégés par des dispositions spécifiques du traité [1309] , ainsi que l'interprétation de la jurisprudence de la Cour de justice. Les droits d'autrui comprennent la protection des droits de propriété intellectuelle et les droits à un recours effectif à la liberté d'expression [1310]. Le juge doit vérifier que l'ingérence de la mesure envisagée soit la moins intrusive pour les droits en jeu[1311]. Le CEDP a souligné dans son avis sur le projet d'accord PNR UE-Canada, qu'en raison du traitement systématique et particulièrement intrusif des données personnelles, le contrôle judiciaire doit être strict[1312]. La nécessité implique une combinaison, l'évaluation fondée sur

---

1307 Ainsi une mesure législative doit contenir une description détaillée de la nécessité de la mesure envisagée. Voy. en ce sens : EDPS advice during the public consultation organised by the Commission in 2011 (see Council of the European Union, Doc 6370/13) on the Amendment to the commission proposal COM (2011) 628 final/2 for Regulation of the European Parliement and of the council of the financing, management, and monitoring of the common agricultural policy (rules adopted to comply with the Schecke judgment on the publication of personal data of beneficiaries in the context of the common agricolture policy-now regulation 1306/2013,, in particular Articles 111 - 113 and Recitals 73 – 87 : « *The EDPS points out that for assessing the compliance with privacy and data protection requirements, it is of crucial importance to have a clear and well-defined purpose wich the envisaged measure intends to serve. Commenting on the control objective, the representative of the EDPS said that the Commission should thereby be clear on whether the aim of the measure also includes to allow a certain form of public control over the spending of EU money by the recipients as such for which the disclosure of the identity of the recipients would be indispensible. However, if the aim only concerns public control over the EU institutions and over how the EU budget is spent, it is less obvious that the identity of the recipients should be provided to the public...*».

1308 Ainsi, dans l'affaire Digital Rights concernant la validité de la directive 24/2006 sur la conservation des données, la Cour a jugé que l'obligation aux fournisseurs de services de communications électroniques accessibles au public ou de publics réseaux de communication de conserver, pendant 6 mois à deux ans, les communications de données, comme la ligne d'appel téléphonique, les adresses e-mail, les adresses IP utilisées pour accéder à Internet, « constitue en soi une ingérence dans les droits garantis par l'article 7 de la Charte « (paragraphe 34). « L'accès aux données par les autorités nationales compétentes constitue une ingérence dans ce droit fondamental » (Paragraphe 35). La Cour a également constaté que « la directive 2006/24 constitue une limitation sur le droit fondamental à la protection des données personnelles garanti par l'article 8 de la Charte parce qu'il prévoit le traitement des données à caractère personnel « (paragraphe 36).

1309 Comme par exemple les articles 36 et 346 du TFUE, la transparence et le contrôle public sont également prévus par les articles 1 et 15 (1) TUE) permettant au citoyen de participer plus étroitement à la prise de décision. Voy. sur les objectifs d'intérêt général les notes explicatives concernant l'article 52 la Charte.

1310 Concernant le droit d'autrui : Voy. l'affaire Promusicae CJCE, C-275/06. La CJCE a jugé que la protection du droit à la propriété intellectuelle est un but légitime pour le traitement des données de communication (adresses IP) en faisant référence à l'article 13 de la directive 95/46 qui vise des limitations au traitement des données à caractère personnel (paragraphes 26). Concernant l'objectif d'intérêt général voy. : Paragraphe 9 de l'Avis du CEDP 3/2016 sur l'échange d'informations sur les pays tiers dans l'European Criminal Records Informations System (ECRIS). Le CEPD estime que la proposition de la Commisison ECRIS pour faciliter l'accès à des renseignements sur les convictions religieuses des ressortissants des pays tiers constitue un but dans la lutte contre le terrorisme afin d'assurer la sécurité publique reconnue comme un objectif d'intérêt général dans le droit communautaire.

1311 Ainsi dans l'affaire Schecke (CJEU,aff.jointes C-92/09 et C-93/09), la Cour a conclu que « les limitations à la protection des données à caractère personnel ne doivent s'appliquer que dans la mesure strictement nécessaire (Satakunnan Markkinapörssi et Satamedia, point 56) et qu'il est possible que d'autres mesures prévoient une incidence sur le droit fondamental des personnes physiques à la protection des données moins négative et qui contribuent encore efficacement aux objectifs de l'Union européenne en question... ». (Paragraphes, 81, 82, 83, 86).

1312 Voy. l'Avis du CEPD dans le cas de l'accord de projet PNR UE-Canada, disponible à l'adresse suivante: https: //secure.edps.europa.eu / EDPSWEB / webdav / site / monsite / shared / Documents / Consultation / Cour / 2016 / 16-04-05_Pleading_Canada_PNR2_EN.pdf; Avis 1/15 (demande d'avis présentée par le Parlement européen) sur le projet d'accord entre le Canada et l'UE sur le transfert et le traitement des données PNR, déclare que l'examen rigoureux du pouvoir

l'efficacité *en concreto* de la mesure envisagée pour atteindre l'objectif poursuivi et l'évaluation du caractère intrusif de cette mesure par rapport à d'autres options afin d'atteindre les mêmes objectifs. La nécessité est également un principe de qualité des données et une condition récurrente dans les exigences sur la légalité du traitement des données personnelles provenant de la législation de l'Union. La jurisprudence de la Cour de justice applique le test de la stricte nécessité pour toutes les restrictions à l'exercice du droit à la protection des données personnelles et le respect de la vie privée, ainsi les dérogations et limitations ne doivent s'appliquer que dans une mesure strictement nécessaire. Au contraire, la CourEDH applique le test de stricte nécessité seulement en fonction du contexte et des enjeux, comme en ce qui concerne la surveillance secrète[1313]. Ainsi, la CourEDH s'est penchée sur la surveillance secrète dans l'affaire *Roman Zakharov c. Russie*[1314]. La Cour avait conclu que le système d'interception secrète des communications de téléphonie mobile en Russie violait l'article 8 de la Convention. Cependant, le cas d'espèce restait limité à la possibilité pour les services secrets russes d'intercepter une communication téléphonique à n'importe quel moment. Les juges de Strasbourg ne se sont pas penchés sur la question de l'interception de toutes les communications à tout moment comme l'a fait la Cour de justice dans l'affaire *Schrems*. Ainsi, le champ d'application de l'affaire *Zakharov* a été étendu dans l'affaire *Szabó et Vissy c. Hongrie*[1315]. Dans cette décision, la CourEDH semble condamner la surveillance massive et arbitraire de la législation hongroise car elle « peut potentiellement affecter tout le monde et, qu'à ce titre, elle peut être interprétée comme ouvrant la voie à la surveillance illimitée d'un grand nombre de citoyens ». De plus, la Cour donne des critères et considère que des mesures de surveillance secrète ne peuvent être utilisées que si strictement nécessaires [1316] à la sauvegarde des institutions démocratiques[1317] et à l'obtention de renseignements vitaux dans une opération individuelle et que dans le cas d'espèce, la législation hongroise ne prévoit aucun moyen afin de « vérifier s'il existe, dans chaque cas, des raisons suffisantes à l'interception des communications d'un individu spécifique ». Toutefois, l'interdiction de la surveillance sécrète ne semble pas totale, la CourEDH « admet que les formes prises par le terrorisme ont pour

discrétionnaire du législateur est basé sur l'importance que le traitement des données personnelles a dans la société et la gravité de la limitation que la mesure en cause peut provoquer (Paragraphe 201). Voy. Egalement CJUE, affaires jointes C 293/12 et C 594/12, Digital Rights Irlande, point 47.

1313 CEDH, Szabo and Vissy c. Hongrie 12 Janvier 2016, § 73.

1314 CEDH, Roman Zakharov c. Russie,4 décembre 2015, req. n° 47143/06.

1315 Voy. CEDH, Szabo et Vissy c. Hongrie Req. n° 37138/14. Voy. Sarah ST.VINCENT, « Did the European Court of Human Rights Just Outlaw "Massive Monitoring of Communications" in Europe ? », 13 janvier 2016 accessible sur le site : https://cdt.org/blog/did-the-european-court-of-human-rights-just-outlaw-massive-monitoring-of-communications-in-europe/.

1316 Sur ce point la CEDH rappelle la jurisprudence de la CJ Digital Rights Ireland (C-293/12 et C-594/12). Sont cités notamment les §§ 52 et 62 de l'arrêt de la CJUE, qui exigent la « stricte nécessité » des mesures de rétention des données de communication électroniques organisée par la directive 2006/24/CE, examinée à « la lumière des objectifs poursuivis ». La Cour de Strasbourg fait donc un parallèle entre la rétention des données organisée par la directive à des fins de lutte contre le terrorisme et les mesures de surveillance secrète – notamment des communications – mises en place par la législation hongroise aux mêmes fins. La CourEDH souligne l'ampleur des conséquences que peut entraîner la mise en œuvre des techniques de surveillance de masse qui portent atteinte au droit au respect de la vie privée des personnes. C'est la raison pour laquelle de telles mesures de surveillance doivent être nécessairement accompagnées de garanties assurant le respect des droits des citoyens, et doivent de surcroît justifier d'une « stricte nécessité » au regard de la défense des institutions démocratiques.

1317 La CourEDH cite ici l'affaire Klass, voy. décision Klass §42.

conséquence naturelle un recours par les gouvernements à des technologies de pointe, notamment à des techniques de surveillance massive des communications, afin d'éviter des incidents imminents »[1318]. La décision semble ambigüe puisqu'elle admet qu'en cas de « soupçon individuel »[1319] et non de « soupçon raisonnable », comme elle le faisait avant, les autorités peuvent, dans la lutte contre le terrorisme recueillir « une masse d'informations utilisant des méthodes hautement efficaces et traitant des données en masse, potentiellement sur chaque personne liée, d'une manière ou d'une autre, à des sujets ou objets suspects d'êtres en lien avec une attaque terroriste ». La CourEDH souligne que la priorité est désormais d'instaurer un contrôle effectif sur les législations permettant la surveillance de masse. Ainsi la durée de la surveillance doit être clairement définie ; la supervision des mesures de surveillance par un membre du gouvernement n'est pas suffisante puisque un contrôle judiciaire externe « offre les meilleures garanties d'indépendance, d'impartialité et de bon déroulement[1320] » ; les services de renseignement doivent démontrer la nécessité des mesures de surveillance lors de leur mise œuvre et la relation réelle ou présumée des personnes surveillées avec une quelconque menace terroriste ; il faut assurer un droit de recours aux citoyens et donc, au préalable, un droit d'être informé: « dès lors que la notification peut être effectuée après la fin de la mesure de surveillance sans mettre en danger le but de la restriction, les informations doivent être fournies à la personne concernée »[1321]. Ce contrôle effectif de la législation est joué par le juge mais également au sein de la société civile par les autorités de contrôle indépendantes. Ainsi, la CourEDH a conclu que la surveillance secrète sans contrôle ou sans possibilité effective de recours judiciaire constitue une violation des droits des requérants en vertu de l'article 6 ainsi que de l'article 13 lus conjointement avec l'article 8 de la Convention. Cependant, il s'agit d'un arrêt ambigu comme le démontre l'avis contraire[1322] du juge Pinto de Albuquerque et le fait qu'il a été rendu par la quatrième chambre de la CEDH. Ce sera à la Grande Chambre de le trancher à l'avenir. Ainsi dans l'interdiction de la surveillance de masse, la CourEDH semble plus prudente que la Cour de justice. Au contraire, il découle de la jurisprudence de la Cour de

---

1318 Voy. Considérant 69.

1319 Voy. §73 de l'arrêt, La Cour considère que l'exigence « nécessaire dans une société démocratique » doit être interprétée dans ce contexte comme exigeant « une nécessité stricte » dans deux aspects. Une mesure de la surveillance secrète ne peut être considérée comme conforme à la Convention que si cela est strictement nécessaire, en tant que considération générale, pour la sauvegarde des institutions démocratiques et, d'autre part, s'il est strictement nécessaire, en tant que considération particulière, pour l'obtention d'un renseignement essentiel dans une opération individuelle

1320 La CourEDH cite ici l'arrêt Roman Zakharov, § 258.

1321 Voy. § 86 de la décision.

1322 Conformément à l'article 45 § 2 de la Convention et à l'article 74 § 2 du Règlement de la Cour, l'avis contraire du Juge Pinto de Albuquerque a été annexé à la décision. Il affirme que la raison pour laquelle la Cour a fait disparaître le terme de « soupçon raisonnable » en faveur du terme « soupçon individuel » est qu'elle considère que la lutte contre le terrorisme nécessite « une masse d'informations accessible aux autorités utilisant des méthodes hautement efficaces et traitant des données en masse, potentiellement sur chaque personne liée, d'une manière ou d'une autre, à des sujets ou objets suspects d'êtres en lien avec une attaque terroriste ». Il considère que la Cour a voulu laisser la voie ouverte aux traitements en masse des données si seulement entourés de garanties. Cette approche semble trouver une base dans l'affirmation de la Cour qui justifie et admet que les formes prises par le terrorisme de nos jours ont pour conséquence naturelle un recours par les gouvernements à des technologies de pointe, notamment à des techniques de surveillance massive des communications, afin d'éviter des incidents imminents ».

justice que la condition de la stricte nécessité est horizontale, quel que soit le domaine du droit européen en cause[1323].

166 Le triple test de proportionnalité. Le contrôle opéré par la Cour de justice comporte plusieurs degrés[1324]. C'est la Cour constitutionnelle allemande qui a identifié trois principes distincts composant le principe de proportionnalité : le principe d'adéquation, le principe de nécessité et le principe de proportionnalité au sens étroit [1325] . Le principe d'adéquation (*Geeignetheit*) signifie que la mesure restrictive contrôlée doit être appropriée à la réalisation de l'objectif poursuivi. Le principe de nécessité (*Erforderlichkeit*) implique que la mesure restrictive contrôlée soit indispensable pour atteindre le but recherché. Ainsi, parmi les mesures restrictives adéquates, celle qui limite le moins le droit ou la liberté concernés doit être préférée. Enfin, le principe de proportionnalité au sens strict (*Verhältnismässligkeit im engeren Sinne*) exige que la mesure restrictive assure un juste équilibre des intérêts en présence[1326]. Toutefois, la Cour de justice ne recourt pas systématiquement aux trois degrés du contrôle. Le contrôle plus au moins étendu dépend de la nature des données concernées par la mesure restrictive et par l'intensité de la restriction. Le contrôle opéré par la Cour de justice comporte plusieurs degrés. Dans la plupart des cas, le contrôle de proportionnalité est exercé de manière réduite (a). Toutefois, lorsque certaines circonstances accordent une importance particulière au droit à la protection des données personnelles le contrôle de proportionnalité est exercé de manière approfondie (b).

a) Le contrôle réduit de proportionnalité.

167 Un contrôle réduit en raison de la marge de manœuvre des États. Le test de proportionnalité au sein de l'UE se compose de trois phases. Ainsi, dans l'affaire *Digital Rights*, la Cour a d'abord déclaré que la mesure de rétention des données répondait bien à un objectif général de l'Union[1327], elle a été amenée ensuite à se prononcer sur la proportionnalité de

1323 Voy. Directive 2016/680 du Parlement européen et du Conseil du 27 Avril 2016 portant sur la protection des personnes physiques à égard du traitement des données à caractère personnel par les autorités compétentes aux fins de la prévention, la recherche, la détection ou la poursuite d'infractions pénales ou l'exécution des sanctions pénales et à la libre circulation de ces données, et abrogeant Décision-cadre du Conseil 2008/977 / JAI du Conseil, JO L119, 04.05.2016.

1324 D. SIMON, *Le contrôle de proportionnalité exercé par la Cour de justice des Communautés européennes*, préc.p. 14

1325 M. FROMONT, « État de droit et principe de proportionnalité. Commentaire de la décision du 15 décembre 1970 de la Cour constitutionnelle fédérale allemande », in P. BON, D. MAUS (dir.), *Les grandes décisions des cours constitutionnelles européennes*, Dalloz, Paris, 2008, pp. 5-8.

1326 J. ZILLER, *Le principe de proportionnalité*, AJDA, 1996, pp. 185 et s., spéc p. 185.

1327 L'objectif matériel de cette directive vise, ainsi qu'il découle de son article 1er, paragraphe 1, à garantir la disponibilité de ces données à des fins de recherche, de détection et de poursuite d'infractions graves telles qu'elles sont définies par chaque État membre dans son droit interne. L'objectif matériel de cette directive est, dès lors, de contribuer à la lutte contre la criminalité grave et ainsi, en fin de compte, à la sécurité publique.

l'ingérence tenant à la pertinence et la nécessité de la mesure [1328] . Elle a estimé que les limitations des droits protégés aux articles 7 et 8 n'étaient pas nécessaires[1329] et donc que les limitations n'étaient pas proportionnées[1330]. Elle ne s'est pas penchée sur le troisième degré de proportionnalité, c'est-à-dire vérifier si les inconvénients auxquels aboutit l'action ne dépassent pas ses avantages. Elle s'est arrêtée au deuxième niveau du test de proportionnalité visant la nécessité. Ainsi, la Cour de justice a estimé que le principe de proportionnalité exige que les actes des institutions de l'UE soient appropriés pour atteindre les objectifs légitimes poursuivis par la législation et ne dépassent pas les limites de ce qui est approprié et nécessaire pour atteindre ces objectifs. Ici, compte tenu du rôle important joué par la protection des données à la lumière du droit fondamentalà la vie privée et de l'étendue et de la gravité de l'ingérence, le pouvoir discrétionnaire du législateur de l'UE est réduit, de sorte que l'examen de ce pouvoir discrétionnaire devrait être strict. La rétention des données est un outil approprié pour l'objectif poursuivi[1331]. Le contrôle de proportionnalité est restreint lorsque la CourEDH reconnaît une marge nationale d'appréciation aux États afin d'établir un juste équilibre entre les intérêts publics et privés en conflit. Dans sa jurisprudence la CourEDH semble souvent laisser aux États une très grande marge d'appréciation dans la détermination de l'équilibre à respecter entre le droit au respect de la vie privée et l'objectif poursuivi. Pour déterminer si les mesures qu'il prend sont compatibles avec l'article 8, l'État dispose d'une certaine marge d'appréciation, en vertu d'un principe établi pour la première fois dans l'affaire *Handyside* à propos de l'art 10 mais valable aussi pour l'article 8 : selon la Cour, les autorités de l'État se trouvent en principe mieux placées que le juge international pour se prononcer sur le contenu précis de ces exigences comme sur la « nécessité » d'une « restriction » ou « sanction » destinée à y répondre [...] Il n'en appartient pas moins aux autorités nationales de juger, au premier chef, de la réalité du besoin social impérieux qu'implique en l'occurrence le concept de « nécessité »[1332]. Ainsidans l'affaire *Khelili c. Suisse* [1333], la police a découvert lors d'un contrôle que la requérante transportait des cartes de visite indiquant : « Femme belle et charmante, la trentaine, cherche à rencontrer un homme pour boire un verre ou sortir de temps en temps. Tél. : (...) ». Selon la requérante, suite à cette découverte, les policiers l'ont enregistrée dans leurs dossiers comme prostituée, une profession qu'elle a toujours niée. La requérante a demandé que le terme « prostituée » soit supprimé des dossiers informatiques de la police. La CourEDH a reconnu que la conservation des données à caractère personnel de certains individus, au motif que

---

1328 Voy. §46-50. « Les actes des institutions de l'Union soient aptes à réaliser les objectifs légitimes poursuivis par la réglementation en cause et ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs. »

1329 Voy. point §65. Voy. également les conclusions de l'Avocat général Cruz Villalon, la rétention de données prévue par la directive 2006/24 constitue une ingérence dans les droits fondamentaux consacrés aux articles 7 (vie privée) et 8 (protection des données personnelles) de la Charte qui s'avère « d'une vaste ampleur » et « particulièrement grave », en outre « susceptible de générer dans l'esprit des personnes concernées (…) le sentiment que leur vie privée fait l'objet d'une surveillance constante ».

1330 Voy. §69 de la décision.

1331 Voy. Décision Data Retention point 46-49.

1332 Handyside c/ Royaume- Uni, arrê t du 7 décembre 1976, paragraphes 48 et 49.

1333 CEDH, Khelili c. Suisse, 18 octobre 2011, req. n° 16188/07.

l'individu pourrait commettre une autre infraction, peut en principe être proportionnée dans certaines circonstances. Toutefois, dans le cas de la requérante, l'allégation de prostitution illégale semblait trop vague et générale, n'était étayée par aucun élément concret, celle-ci n'ayant jamais été condamnée pour prostitution illicite, et ne pouvait donc pas être considérée comme fondée sur un « besoin social impérieux » au sens de l'article 8 de la CEDH. Elle a estimé que l'allégation de « prostitution clandestine » dans un fichier de police alors que la requérante n'avait fait l'objet d'aucune poursuite pénale était vague et générale, et qu'elle constituait une ingérence disproportionnée lorsque les autorités ne pouvaient pas apporter la preuve de l'exactitude de cette information[1334]. Considérant qu'il appartenait aux autorités de démontrer l'exactitude des données enregistrées sur la requérante, et compte tenu de la gravité de l'ingérence dans les droits de la requérante, la CourEDH a conclu que la conservation du terme « prostituée » dans les dossiers de la police pendant des années n'était pas nécessaire dans une société démocratique. La CourEDH a conclu à une violation de l'article 8 de la CEDH. La Cour avait déjà reconnu une certaine discrétionnalité à l'État dans l'affaire *Klass et autres c. Allemagne*[1335] en déclarant qu' « un refus d'accès intégral à un fichier de police secret au niveau national est nécessaire lorsque l'État peut légitimement craindre que la communication de telles informations risque de compromettre l'efficacité du système de surveillance secrète destiné à protéger la sécurité nationale et à lutter contre le terrorisme ». Dans l'affaire plus récente *Segerstedt-Wiberg et autres c. Suède*[1336] la Cour a repris cette analyse. Le contrôle restreint qui se manifeste avec la marge d'appréciation laissée aux États s'exerce au-delà de la sécurité nationale lorsque les restrictions ont comme objet le bien-être économique de l'État. Ainsi dans l'affaire *M.S. c. Suède*[1337], la Cour européenne a admis, eu égard à la marge nationale d'appréciation, la communication des données personnelles de santé par un service de gynécologie, sans le consentement de la personne et sans qu'elle puisse contester cette communication devant un tribunal[1338]. L'ingérence était prévue par la loi et constituait un but légitime puisque la communication des renseignements était potentiellement décisive pour l'allocation de fonds publics à des demandeurs remplissant les critères. Elle peut donc passer pour avoir tendu à protéger le bien-être économique du pays. Concernant la nécessité de la mesure, le service de gynécologie avait des raisons pertinentes et satisfaisantes de communiquer à la Caisse le dossier médical de l'intéressée et la mesure n'était pas disproportionnée au but légitime poursuivi. Il n'y a donc pas eu violation de l'article 8 de la Convention[1339]. Concernant la Cour de justice, la première fois qu'elle a été amenée à interpréter la directive 95/46 dans

1334 CEDH, Khelili c. Suisse, n° 16188/07, 18 octobre 2011.

1335 CEDH, 6 septembre 1978, Klass et autres c/ Allemagne, req. n° 5029/71, §58.

1336 CEDH, 6 juin, 2006, Segerstedt-Wiberg et autres c/Suède, req. n° 62332/00, §102.

1337 Cour eur. DH, arrê t M.S. c. Suède du 27 aoû t 1997.

1338 CEDH, M.S. c. Suède, 27 août 1997, req. n° 20837/92.

1339 Voy. § 41-44 des motifs et point 1 du dispositif.

l'affaire *Rechnungshof* c. Österreichischer Rundfunk [1340], elle a vérifié que l'obligation faite aux organismes publics soumis au contrôle de la Cour des comptes autrichienne de communiquer le montant des pensions de retraite excédant un certain seuil était bien nécessaire dans une société démocratique pour atteindre le but légitime poursuivi de bonne utilisation des fonds publics. Ainsi elle a reconnu une large marge de manœuvre à l'État[1341]. Dans cette affaire, elle a emprunté le raisonnement sur la marge d'appréciation à la Cour européenne des droits de l'homme. De plus, dans l'affaire *Volker et Markus*, elle a indiqué que le contrôle de proportionnalité des restrictions au droit à la protection des données personnelles était le même que celui exercé dans le cadre de l'article 8 de Convention européenne des droits de l'homme [1342] . Avant la consécration par la Charte du droit à la protection des données personnelles, la CJ a utilisé comme grille d'analyse la CEDH et les principes généraux du droit. Ainsi, dans l'affaire *Bodil Lindqvist*, elle affirme explicitement qu'il incombe aux autorités et juridictions nationales d'interpréter la directive 95/46 de manière conforme aux droits fondamentaux protégés par l'ordre juridique de l'Union européenne et aux principes généraux du droit, tels que le principe de proportionnalité[1343]. Dans l'affaire *Shwartz*[1344], la CJ estime que le stockage des empreintes digitales sur un support de base des données hautement sécurisé réduit le risque de falsification de passeports et facilite le travail des autorités chargées de vérifier l'authenticité des passeports aux frontières de l'UE. Ainsi, cette mesure est appropriée au but poursuivi puisqu'elle consiste à prendre les empreintes de deux doigts, ce qui ne provoque aucun inconfort physique ou mental, ainsi qu'une image du visage[1345]. La seule alternative possible aux empreintes digitales est l'analyse par iris, dont la technologie n'est pas encore aussi avancée que la reconnaissance d'empreintes digitales. Ainsi, il n'y a pas d'alternative apparente suffisamment efficace et moins menaçante pour les droits protégés[1346]. La préoccupation selon laquelle les données peuvent être centralisées et utilisées à d'autres fins (par exemple, enquêtes criminelles ou surveillance indirecte de la personne) n'affecte pas la validité du règlement [1347] qui prévoit uniquement la prévention d'une entrée illégale dans

---

1340 CJCE, 20 mai 2003, Rechnungshof c. Österreichischer Rundfunk et autres, aff. C-465/00, C-138/01, C-139/01, Rec. I-4989, § 83, « L'adjectif »nécessaire", […], implique qu' »un besoin social impérieux" soit en cause et que la mesure prise soit »proportionnée au but légitime recherché" […]. En outre, les autorités nationales jouissent d'une marge d'appréciation »dont l'ampleur dépend non seulement de la finalité, mais encore du caractère propre de l'ingérence" ».

1341 C. MAUBERNARD, *Chronique de droit communautaire des droits fondamentaux*, RTDH, 2004, pp. 724 et s., sp. p. 724.

1342 Voy. CJUE, G. Ch., 9 novembre 2010, Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, aff. C-92/09 et C-93/09, §72, elle avait été saisie d'un renvoi préjudiciel en appréciation de validité de la règlementation de l'Union relative à la publication d'informations sur les bénéficiaires des aides versées dans le cadre de la politique agricole commune.

1343 CJCE, 6 novembre 2003, Bodil Lindqvist, aff. C-101/01, Rec. I-12971, § 87.

1344 CJUE, C-291/12, Schwartz c. Bochum, 17 octobre 2014.

1345 Voy. point 41-45 de la décision.

1346 Voy. points 48-53 de la décision.

1347 Voy. Règlement 2252/2004.

l'UE[1348]. Dans l'affaire *Huber*[1349], un ressortissant Autrichien résident en Allemagne, a demandé la suppression des données personnelles le concernant (nom, date et lieu de naissance, nationalité, état matrimonial, sexe, entrées et sorties de l'Allemagne, statut de résidence, précisions sur les passeports, déclarations concernant le domicile, numéros de référence) dans le registre central allemand des ressortissants étrangers (AZR). L'AZR est utilisé à des fins statistiques et par les services de sécurité ou de police et les autorités judiciaires pour la poursuite et l'enquête sur les activités criminelles. L'Allemagne a rejeté la demande de Huber. La Cour estime que compte tenu du fait que la directive 95/46 vise à assurer un niveau équivalent de protection des données dans tous les États membres afin d'assurer un niveau élevé de protection dans l'UE, le concept de nécessité inscrit à l'article 7 e) ne peut pas avoir une signification qui varie selon les États membres. Ainsi, c'est un concept qui a son propre sens indépendant dans le droit de l'UE et doit être interprété d'une manière qui reflète pleinement l'objectif de la directive 95/46[1350]. En vertu de la législation de l'UE, le droit de libre circulation d'un État membre national n'est pas inconditionnel, mais peut être soumis aux limitations et aux conditions imposées par le Traité et ses règles d'application. La législation prévoit qu'un État membre peut exiger que certains documents soient fournis pour déterminer les conditions du droit de séjour. Ainsi, il est nécessaire qu'un État membre dispose des informations et des documents pertinents afin de vérifier s'il existe un droit de séjour sur son territoire. L'utilisation d'un registre pour soutenir les autorités responsables de l'application de la législation sur le droit de séjour est, en principe, légitime. Toutefois, le registre ne doit contenir aucune information autre que ce qui est nécessaire à cette fin et doit être tenu à jour. Seules les informations anonymes sont nécessaires à des fins statistiques. L'accès doit être limité aux autorités responsables. Le registre central pourrait être nécessaire s'il contribue à une application plus efficace de cette législation. La juridiction nationale devrait décider si ces conditions sont remplies[1351]. Comme on le sait, les données peuvent être traitées lorsque « il est nécessaire pour l'accomplissement d'une tâche dans l'intérêt public ou dans l'exercice de l'autorité publique » [1352]. Dans cette affaire c'est le principe de non-discrimination, art. 18 TUE, qui était mis en cause compte tenu qu'il n'existait pas une tel registre pour les ressortissants allemands. À cet égard, l'avocat général Maduro Polaires a identifié trois aspects de l'inégalité de traitement. Tout d'abord, les données personnelles des citoyens étrangers ont été conservées non seulement dans les registres municipaux (comme ceux de leurs citoyens), mais aussi dans le registre central des étrangers; d'autre part, le registre central contient un plus grand nombre d'informations par rapport aux registres municipaux; en troisième lieu, la possibilité d'une consultation rapide et sans contraintes des données relatives aux étrangers, alors que cela était impossible pour les citoyens allemands. Selon la Cour, les aspects en question devaient s'examiner à la lumière de l'interdiction de la discrimination et sur la base de la directive

1348 Voy. § 61-62.

1349 CJCE, C-524/06, Huber c. Allemagne 16.12.2008

1350 Voy. § 50-51.

1351 Voy. § 54-62.

1352 Art. 7, lett. e) della direttiva 95/46/CE sulla protezione dei dati personali.

2004/387CE[1353] sur le droit de séjour. Ainsi, la Cour a estimé que le traitement du bureau de l'immigration allemande n'était pas justifié à moins de démontrer l'absence d'autres moyens plus efficaces de mise en œuvre des règles en matière d'immigration et de séjour. Concernant l'application de la directive 95/46/CE, l'avocat général a examiné si le traitement centralisé des données des étrangers pouvait être considéré comme « nécessaire » en vertu de l'article 7 de la directive. Il a reconstruit le concept de « nécessité » qui « a une longue histoire dans le droit communautaire et qui a un lien étroit avec le critère de proportionnalité. Cela signifie que l'autorité avant d'adopter une mesure interférant avec un droit fondamental doit démontrer qu'il s'agit de la mesure la moins restrictive pour atteindre l'objectif »[1354]. La Cour a enfin vérifié la légitimité du traitement des données à caractère personnel aux fins de lutte contre la criminalité. Étant donné que ce domaine ne rentre pas dans le champ d'application de la directive 95/46 / CE, la base juridique est plutôt l'article 18 TFUE. Bien que l'objectif poursuivi, la lutte contre la criminalité, soit légitime, la Cour a estimé qu'il n'était pas suffisant pour justifier le traitement systématique des données des étrangers et que cette pratique était discriminatoire. L'avocat général a souligné le parallélisme entre le niveau de protection de la CEDH et celui de la directive européenne, rappelant que la Cour, dans l'affaire *Österreichischer Rundfunk*, avait déjà estimé que « si une mesure nationale est incompatible avec l'article 8 CEDH, elle ne peut pas être compatible avec l'art. 7, lett. e) de la directive 95/46[1355]. La Cour de justice a choisi d'appliquer le même niveau de protection que le Conseil de l'Europe pour la protection de la vie privée. Ainsi dans la recherche de l'équilibre avec les autres exigences de l'État (à savoir l'application effective de la législation sur l'immigration et la lutte contre la criminalité) la Cour a montré une grande coopération avec la juridiction nationale, à qui elle a renvoyé le devoir de déterminer concrètement la nécessité d'une telle législation. Alors qu'en présence d'une large marge d'appréciation de l'État, le contrôle de proportionnalité est souvent réduit, dans certaines circonstances et en raison de la nature des données le contrôle de proportionnalité peut être renforcé.

b) Un contrôle renforcé

168 Un contrôle étroit en raison de la nature des données personnelles. Le contrôle de proportionnalité est plus strict lorsque sont en jeu certaines données personnelles. Ainsi lorsque les restrictions concernent des données sensibles, la Cour va restreindre la marge d'appréciation de l'État [1356]. Appartiennent à cette catégorie celles qui font apparaître directement ou

1353 Direttiva 2004/38/CE del Parlamento europeo e del Consiglio, del 29 aprile 2004, relativa al diritto dei cittadini dell'Unione e dei loro familiari di circolare e di soggiornare liberamente nel territorio degli Stati membri, in GU L 158 del 30 aprile 2004.

1354 CJCE, Huber c. Bundesrepublik Deutschland, cit.,§ 52.

1355 CJCE, Huber c. Bundesrepublik Deutschland, cit.,§ 52.

1356 EDH, 25 février 1997, Z. c/ Finlande, req. n°22009/93, Rec. 1997-I, § 99 ; pour un développement de ces critères v. CEDH [GC], 4 décembre 2008, S. et Marper c/ Royaume-Uni, req. n°30562/04 et n°30566/04, Rec. 2008, § 102 : « L'étendue

indirectement les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé[1357] ou à la vie sexuelle de celles-ci. D'autres catégories de données personnelles ont été assimilées qui, bien qu'elles n'aient pas été énumérées dans cette liste exhaustive, sont soumises à une même protection renforcée. Tel est par exemple le cas des données relatives aux infractions, condamnations et aux mesures de sûreté, mais aussi des données biométriques et des données génétiques. Par leur nature, de telles données sont susceptibles de porter une atteinte particulièrement grave à la vie privée de la personne concernée et, contrairement aux autres données personnelles, les données sensibles ne peuvent en principe pas être utilisées. Concernant la surveillance de masse dans l'affaire *Digital Rights,* c'est en raison du traitement des données généralisées, et par l'atteinte particulièrement grave au droit à la protection des données personnelles que la Cour de justice a annulé la directive 2006/24 imposant aux États de prévoir une obligation de conservation des données de connexion pour les fournisseurs d'accès à Internet. Cette obligation n'était pas proportionnée au but poursuivi car elle se caractérisait par sa généralité et sa globalité et par l'atteinte particulièrement grave au droit à la protection des données personnelles[1358]. Ainsi dans l'affaire *Schrems,* la CJ a invalidé la décision 2000/520/CE qui validait les principes dits de la « sphère de sécurité » ou « *Safe Harbor* », qui constituaient auparavant le fondement des transferts de données de l'Union Européenne vers les États-Unis parce qu'il ne respectait pas le principe de proportionnalité. Au fil de sa jurisprudence, la Cour a non seulement soumis les autorités nationales chargées de l'application du droit de l'Union européenne au respect du principe de proportionnalité pour les restrictions qui seraient portées à la protection des données personnelles, mais elle les a guidées en leur expliquant comment contrôler de telles restrictions. C'est pourquoi « lors de la mise en œuvre des mesures de transposition des directives, il incombe aux autorités et aux juridictions des États membres non seulement d'interpréter leur droit national d'une manière conforme à ces mêmes directives, mais également de ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité »[1359]. Ainsi, la CJ a rappelé dans l'affaire *Data Retention* que l'« étendue du pouvoir d'appréciation du législateur de l'Union

---

de cette marge est variable et dépend d'un certain nombre de facteurs, dont la nature du droit en cause garanti par la Convention, son importance pour la personne concernée, la nature de l'ingérence et la finalité de celle-ci. Cette marge est d'autant plus restreinte que le droit en cause est important pour garantir à l'individu la jouissance effective des droits fondamentaux ou d'ordre « intime » qui lui sont reconnus […]. Lorsqu'un aspect particulièrement important de l'existence ou de l'identité d'un individu se trouve en jeu, la marge laissée à l'État est restreinte [...]. En revanche, lorsqu'il n'y a pas de consensus au sein des États membres du Conseil de l'Europe, que ce soit sur l'importance relative de l'intérêt en jeu ou sur les meilleurs moyens de le protéger, la marge d'appréciation est plus large [...] ».

1357 La CJ dans l'affaire Lindquist a spécifié que la référence au fait qu'une personne s'est blessée le pied et est en congé médical constitue des données personnelles concernant la santé au sens de l'article 8 (1), car cette disposition doit être interprétée de manière à inclure tous les aspects, physiques et mentaux, de la santé d'un individu. Voy. point 50-51.

1358 CJUE, G. Ch., 8 avril 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C-293/12 et C-594/12, § 58 : Ainsi que la Cour le note cette obligation « concerne de manière globale l'ensemble des personnes faisant usage de services de communications électroniques, sans toutefois que les personnes dont les données sont conservées se trouvent, même indirectement, dans une situation susceptible de donner lieu à des poursuites pénales ». Voy. sur ce point du contrôle strict, C. CASTETS -RENARD, « L'invalidation de la directive n° 2006/24/CE par la CJUE : une onde de choc en faveur de la protection des données personnelles », D., 2014, pp. 1355 et s.

1359 CJCE, C-275/06, Productores de música de España (Promusicae) c/ Telefónica de España Sau.

peut s'avérer limitée en fonction d'un certain nombre d'éléments, parmi lesquels, le domaine concerné, la nature du droit en cause, la nature et la gravité de l'ingérence ainsi que la finalité de celle-ci ». Dans cette affaire, la Cour a estimé, qu'« en l'espèce, compte tenu, d'une part, du rôle important que joue la protection des données à caractère personnel au regard du droit fondamental au respect de la vie privée et, d'autre part, de l'ampleur et de la gravité de l'ingérence dans ce droit que comporte la directive 2006/24, le pouvoir d'appréciation du législateur de l'Union s'avère réduit de sorte qu'il convient de procéder à un contrôle strict »[1360]. Ainsi, il a été observé que les intérêts constitutionnels nationaux sont dûment pris en compte afin de limiter l'autonomie politique de l'Union européenne[1361] . Dans l'affaire *Digital Rights,* la Cour de justice arrive au point central de son *reasoning* concernant l'examen de la nécessité de la mesure par rapport aux objectifs poursuivis. Selon la CJ, la lutte contre la criminalité et le terrorisme, comme un objectif d'intérêt général, ne justifie pas la conservation massive et généralisée des données personnelles[1362]. Telle mesure ne peut pas être considérée comme nécessaire dans une société démocratique seulement parce qu'elle poursuit un but d'intérêt général, mais doit être équilibrée avec des intérêts opposés dignes de protection. Plus précisément, la garantie du droit fondamental au respect de la vie privée n'admet des exceptions ou limitations à la protection des données personnelles que dans la mesure où celles-ci sont strictement nécessaires pour être considérées comme proportionnées. La législation de l'Union doit prévoir des règles claires et précises relatives à la portée et à l'application de la mesure en question et imposer des exigences minimales pour que les personnes dont les données ont été ont conservées aient des garanties suffisantes qui permettent de protéger efficacement leurs données contre les risques d'abus, ainsi que contre tout accès illicite et l'utilisation de ces données [1363]. La nécessité de fournir de telles garanties est encore plus grande lorsque les données personnelles font l'objet d'un traitement automatisé et massif. Dans le cas d'espèce, la collecte d'informations de trafic est généralisée et totalement indépendante de la présence ou l'absence d'une menace réelle pour la sécurité publique, elle ne se limite pas à une zone géographique ou un groupe de personnes liées aux milieux criminels. Il s'agit d'une « rétention de masse soupçon moins de données au cas où ils peuvent être utiles à l'avenir »[1364]. La Cour souligne que le manque de définition d'un critère objectif de « criminalité grave » permettant la collecte, l'accès aux données recueillies et leur l'utilisation entraîne des différences d'application de la directive. En bref, il ne suffit pas d'une référence générale à la criminalité grave contenue dans l'art. 1 de la directive. Il manque les conditions de fond et de procédure à la lumière desquelles les autorités nationales compétentes peuvent avoir accès aux informations stockées. Ainsi, leur utilisation ne se limite pas explicitement aux fins de la prévention, ni

---

1360 Voy. Décision C-293/12, § 47-48.

1361 E. DUBOUT, « Droits fondamentaux et pluralisme constitutionnel », in TR. TINIÈRE et C. VIAL (dir.), *La protection des droits fondamentaux dans l'Union européenne. Entre évolution et permanence*, Bruylant, 2015, pp. 107-159. pp. p155.

1362 Voy. §51 de la décision.

1363 Voy. §54 de la décision.

1364 P. SCHAAR, *Data Retention: a landmark Court of Justice's ruling. From now on, no more just in case retention of data* , 10 Avril 2014, disponible à l'adresse : http://free-group.eu/.

n'établit une liste de personnes autorisées, ni ne prévoit une décision d'un tribunal ou d'une autorité administrative indépendante[1365]. De plus, en ce qui concerne la période de stockage des informations recueillies, la directive établit une limite minimale (6 mois) et maximale (24 mois), mais elle n'indique pas les critères objectifs pour leur détermination, ni n'introduit une distinction entre les catégories de données enregistrées ou des personnes concernées[1366]. La lutte contre la criminalité grave et le terrorisme est de la plus haute importance pour assurer la sécurité publique et son efficacité peut dépendre de l'utilisation de techniques d'investigation modernes. Mais cela ne justifie pas, en soi, la nécessité de la mesure de conservation. Les dérogations et les limitations relatives à la protection des données ne doivent s'appliquer que dans la mesure strictement nécessaire. Ici, la législation doit fixer des règles claires et précises régissant la portée et l'application des mesures en question et imposant des garanties minimales afin que les personnes dont les données ont été retenues aient des garanties suffisantes pour protéger efficacement leurs données personnelles contre les risques d'abus, d'accès illégal et d'utilisation des données. La nécessité de sauvegarde est d'autant plus grande que les données personnelles sont soumises à un traitement automatique et qu'il existe un risque important d'accès illégal à ces données. En outre, la directive exige la conservation de toutes les données de trafic concernant la téléphonie fixe, la téléphonie mobile, l'accès à Internet ou les emails, dont l'utilisation est très répandue et d'une importance croissante dans la vie quotidienne des gens. Cela couvre tous les abonnés et les utilisateurs enregistrés, et implique donc une ingérence dans les droits fondamentaux de pratiquement toute la population européenne, sans avoir besoin d'un lien avec le crime[1367]. En conséquence, le législateur de l'Union a dépassé les limites imposées par le respect du principe de proportionnalité à la lumière des articles 7, 8 et 52 (1)[1368]. Au regard des considérations qui précèdent, la Cour de justice a déclaré invalide la directive 2006/24 / CE, car le législateur a dépassé les limites imposées par le respect du principe de proportionnalité, en référence à l'art. 7, 8 et 52.1 de la Charte. Dans un contexte d'interaction entre le droit de la Convention européenne des droits de l'homme et le droit de l'Union européenne, il est intéressant de noter que la Cour de Strasbourg s'est également penchée sur la question de la surveillance de masse[1369] et qu'elle en a opéré une condamnation stricte dans son arrêt *Zakharov* de décembre 2015 et son arrêt *Szabo* de janvier 2016. Elle a rappelé ses jurisprudences *Rotaru*[1370], S. et *Marper*[1371], dans lesquelles elle avait établi les exigences de qualité et de nécessité que doit remplir une législation pour passer le test du contrôle opéré par

1365 Voy. §61et 62 de la décision.

1366 Voy. §63 et 64 de la décision.

1367 Voy. point 51-58 de la décision.

1368 Voy. point 69.

1369 J. F. FOEGLE, « Chronique du droit « Post-Snowden » : La CJUE et la CEDH sonnent le glas de la surveillance de masse », *La Revue des droits de l'homme, Actualités Droits-Libertés*, mars 2016, disponible à l'adresse :. https://journals.openedition.org/revdh/2074

1370 CEDH, Gr. Ch., 4 mai 2000, Rotaru c. Roumanie, req. n°28341/95.

1371 CEDH, Gr.Ch., 4 décembre 2008, S. et Marper c. Royaume Uni, Req. n° 30562/04 et 30566/04. V., sur cet arrêt : Sylvie Peyrou-Pistouley, « L'affaire Marper c/ Royaume-Uni : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », RFDA 2009, p.94 ; Rocco Bellanova et Paul De Hert, « Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen », Cultures & Conflits [En ligne], 76 | hiver 2009, mis en ligne le 03 mai 2011.

la Cour. Premièrement, la loi doit être accessible à la personne concernée et prévisible quant à ses effets[1372] et, si cette exigence de prévisibilité et d'accessibilité n'a pas la même portée en matière de surveillance secrète, celle-ci doit en revanche être rédigée avec suffisamment de clarté pour permettre aux individus de savoir « en quelles circonstances et sous quelles conditions elle habilite la puissance publique à prendre pareilles mesures secrètes » [1373] . Deuxièmement, la loi doit « définir l'étendue et les modalités d'exercice d'un tel pouvoir de surveillance secrète » et préciser la nature des infractions susceptibles d'être couvertes, mais également « la définition des catégories de personnes susceptibles d'être mises sur écoute, la fixation d'une limite à la durée d'exécution de la mesure, la procédure à suivre pour l'examen, l'utilisation et la conservation des données recueillies, les précautions à prendre pour la communication des données à d'autres parties, et les circonstances dans lesquelles peut ou doit s'opérer l'effacement ou la destruction des enregistrements »[1374]. Sur le plan matériel la loi doit également être « nécessaire dans une société démocratique » à la réalisation d'un but légitime. Ainsi, la Cour a reconnu que les États membres disposent « d'une certaine marge d'appréciation dans le choix des moyens propres à atteindre le but légitime que constitue la protection de la sécurité nationale », les juges devant s'assurer de l'existence de « garanties adéquates et effectives contre les abus »[1375]. Dans l'affaire *Zakharov* concernant la surveillance secrète, la Cour a conclu que les dispositions du droit russe régissant l'interception de communications ne « comportent pas de garanties adéquates et effectives contre l'arbitraire et le risque d'abus inhérent à tout système de surveillance secrète »[1376]. Elle estime que la législation russe ne donne aucune indication sur « les circonstances dans lesquelles les communications d'une personne peuvent être interceptées en raison de faits ou d'activités qui mettent en péril la sécurité nationale, militaire, économique ou écologique », ce qui confère aux autorités une « latitude quasi illimitée »[1377] . Elle relève que la délivrance d'autorisations d'effectuer des écoutes téléphoniques par un service non judiciaire peut être compatible avec la Convention, toutefois, il importe à cet égard que l'organisme de contrôle soit suffisamment indépendant à l'égard de l'exécutif [1378] et dispose de tous les pouvoirs nécessaires pour s'assurer que l'interception des données présente un caractère de nécessité et de proportionnalité au regard des buts poursuivis « en vérifiant par exemple s'il est possible d'atteindre les buts recherchés

---

1372 CEDH, 26 mars 1987, Leander c. Suède ; Cour EDH, 2 août 1984, Malone c. Royaume-Uni.

1373 CEDH, 24 avril 1990, Huvig contre France, Req. n°11105/84, § 34, Cour EDH, 16 février.

1374 CEDH, 16 février 2000, Amann c. Suisse, Req. no 27798/95, §§ 56-58.

1375 CEDH, 16 février 2000, Amann c. Suisse, Req. no 27798/95, §§ 56-58 ; Weber et Saravia c. Allemagne,§ 95.

1376 Voy. l'arrêt Zakharov, §302. Voy. en ce sens Lorna Woods, "Zakharov v Russia: Mass Surveillance and the European Court of Human Rights", EU Law analysis, 16 décembre 2015.

1377 L.WOODS, « Zakharov c. Russia: Mass Surveillance and the European Court of Human Rights », *EU Law analysis*, 16 décembre 2015.

1378 CEDH, Kennedy c. Royaume-Uni, préc, §159 et § 31.

par des moyens moins restrictifs »[1379]. La Cour a confirmé cette jurisprudence dans son plus récent arrêt *Szabo*, faisant grief à la législation hongroise de ne soumettre le contrôle a posteriori des mesures de surveillance qu'à une instance politique, le ministère de la Justice. Si l'arrêt *Zakharov* ne concerne que des mesures de surveillance ciblées et ne porte pas sur le cas spécifique de l'interception de toutes les données à tout moment, l'affaire *Szabo* condamne a fortiori ce type de surveillance[1380]. Dans cette récente affaire, la Cour relève que la législation hongroise « peut potentiellement affecter tout le monde et, qu'à ce titre, elle peut ouvrir la voie à la surveillance illimitée d'un grand nombre de citoyens »[1381], et elle énonce que ces mesures ne peuvent être mises en œuvre qu'en cas de stricte nécessité liée à la sauvegarde des institutions démocratiques et à l'obtention de renseignements par le biais d'une opération individuelle[1382]. Ainsi dans l'affaire *Z. c. Finlande*[1383], la Cour européenne des droits de l'homme s'est livrée à un examen approfondi compte tenu du caractère extrêmement intime et sensible des informations divulguées lors d'un procès pénal concernant des données personnelles de santé relatives à la séropositivité de la requérante. La Cour a reconnu la violation de l'art. 8 CEDH puisque la publication, par la presse, des motifs de la décision, dans la mesure où cela a conduit à la révélation de l'identité ainsi que le statut séropositif de la femme du condamné, bien que prévu par la loi et poursuivant un but légitime, ne pouvait pas être considérée comme nécessaire dans une société démocratique. Aux yeux de la Cour, la protection des données médicales est essentielle non seulement pour protéger la vie privée des malades, mais aussi pour préserver leur confiance dans les services médicaux et de santé en général. À défaut de telles garanties, les personnes pourraient être dissuadées de demander des soins médicaux ou de fournir les renseignements personnels et intimes nécessaires au traitement approprié et même de consulter un médecin, ce qui pourrait mettre en danger leur santé, et dans le cas des maladies contagieuses, celle de la collectivité[1384]. La Cour a conclu que la divulgation de l'identité et de la séropositivité de la requérante dans le texte de l'arrêt de la cour d'appel communiqué à la presse ne se justifiait pas par un motif impérieux. Dès lors, la Cour a jugé à l'unanimité que la publication de ces informations a porté une atteinte disproportionnée, dans le chef de la requérante, au droit au respect de la vie privée et familiale garanti par l'article 8[1385]. Aux fins de

---

1379 Klass et autres contre Allemagne, préc., §51. La Cour avait énoncé que les individus peuvent, sous certaines conditions, bénéficier du statut de « victime » au sens de l'article suscité en raison de l'existence même de programmes de surveillance secrète, et sans avoir à prouver qu'ils ont effectivement fait l'objet d'une telle surveillance. En effet, lorsqu'un État « instaure une surveillance secrète dont les personnes contrôlées ignorent l'existence et [...] demeure dès lors inattaquable », les droits consacrés par la convention pourraient se trouver réduits à néant. Voy. aussi l'arrêt Zakharov, en ce sens la CourEDH juge que les modalités de nomination des procureurs russes conduit à « susciter des doutes quant à leur indépendance à l'égard de l'exécutif » §279. Enfin, l'effectivité des recours est compromise par l'absence de notification des interceptions à un stade quelconque, ou d'un accès approprié aux documents relatifs aux interceptions, §302.

1380 CEDH, Szabo c. Hongrie.

1381 CEDH, Szabo c. Hongrie, §67.

1382 S. St.VINCENT, « Did the European Court of Human Rights Just Outlaw »Massive Monitoring of Communications », in *Europe*, CDT Blog 13 janvier 2016.

1383 CEDH, *Z. c. Finlandia*, § 96.

1384 Voy. Considérant n. 165 Recommandation n°R (89) 14 adoptée par le Comité des ministres du Conseil de l'Europe le 24 octobre 1989 et exposé des motifs « Les incidences éthiques de l'infection VIH dans le cadre sanitaire et social ».

déterminer si les mesures incriminées étaient « nécessaires dans une société démocratique », la Cour a tenu compte du rôle fondamental que joue la protection des données à caractère personnel contenues dans les informations médicales pour l'exercice du droit au respect de la vie privée et familiale garanti par l'article 8. Le respect du caractère confidentiel des informations sur la santé constitue un principe essentiel du système juridique de toutes les parties contractantes à la Convention. Il est capital non seulement pour protéger la vie privée des malades mais également pour préserver leur confiance dans le corps médical et les services de santé en général[1386]. L'intérêt qu'il y a à protéger la confidentialité de telles informations pèsera donc lourdement dans la balance lorsqu'il s'agira de déterminer si l'ingérence était proportionnée au but légitime poursuivi, sachant qu'une telle ingérence ne peut se concilier avec l'article 8 de la Convention que si elle vise à défendre un aspect primordial de l'intérêt public. La jurisprudence de la Cour européenne a exercé un contrôle juridictionnel approfondi également lorsque les mesures restrictives avaient comme objet l'utilisation de données personnelles relatives à l'origine raciale ou ethnique[1387]. Dans le cas d'un tel contrôle, il y a une réduction de la marge nationale d'appréciation des États. Ainsi, dans l'affaire *S. et Marper c. Royaume-Uni*[1388], la Cour a rappelé la crainte, relative à la conservation dans les fichiers de police des profils ADN, échantillons cellulaires et empreintes digitales de personnes soupçonnées mais non condamnées, que de telles mesures puissent conduire à déterminer l'identité ethnique des personnes à partir des échantillons biologiques et renforcer les théories racistes quant à la propension à commettre des infractions. Les requérants se plaignaient de la conservation par les autorités de leurs empreintes digitales, échantillons cellulaires et profils ADN après la conclusion, respectivement par un acquittement et par une décision de classement sans suite, des poursuites pénales menées contre eux. Ils évoquaient les articles 8 (droit au respect de la vie privée et familiale) et 14 (discrimination fondée sur la religion dans l'exercice du droit au respect de la vie familiale). La Cour admet que la conservation des données relatives aux empreintes digitales et génétiques vise un but légitime : la détection et, par voie de conséquence, la prévention des infractions pénales. Cependant, compte tenu du caractère intrinsèquement privé de ces informations, la Cour se doit de procéder à un examen rigoureux de toute mesure prise par un État pour autoriser leur conservation et leur utilisation par les autorités sans le consentement de la personne concernée. Dans cette affaire, la Cour doit se pencher sur le point de savoir si la conservation des empreintes digitales et données ADN des requérants, qui avaient été soupçonnés d'avoir commis certaines infractions pénales mais n'avaient pas été condamnés, était nécessaire dans une société démocratique. La conservation des données doit être proportionnée au but pour lequel elles ont été recueillies et être limitée

1385 Voy. Point 113 des motifs.

1386 La Cour relève que ces considérations valent particulièrement lorsqu'il s'agit de protéger la confidentialité des informations relatives à la séropositivité, dont la divulgation peut avoir des conséquences dévastatrices sur la vie privée et familiale de la personne concernée et sur sa situation sociale et professionnelle, l'exposant à l'opprobre et à un risque d'exclusion. Certaines personnes peuvent de la sorte se laisser dissuader de se soumettre à un diagnostic ou à un traitement, sapant ainsi les efforts prophylactiques déployés par la collectivité pour contenir la pandémie.

1387 Voy. CEDH Gr.Ch, *Natchova et autres c/ Bulgarie*, req. n°43577/98 et 43579/98, 6 juillet 2005, § 145. La discrimination raciale ou ethnique prohibée par l'article 14 de la Convention, la Cour exige une « vigilance spéciale et une réaction vigoureuse de la part des autorités ».

1388 Voy. CEDH, *S. et Marper c. Royaume-Uni* du 4 décembre 2008, req. n 30562/04 et 30566/04.

dans le temps. Les États contractants appliquent systématiquement ces principes dans le secteur de la police, conformément à la Convention du Conseil de l'Europe de 1981 sur la protection des données et aux recommandations ultérieures du Comité des ministres du Conseil de l'Europe. Pour ce qui concerne plus particulièrement les échantillons cellulaires, la plupart des États contractants n'en autorisent le prélèvement dans le cadre de procédures pénales que sur les individus soupçonnés d'avoir commis des infractions présentant un certain seuil de gravité. Dans la grande majorité des États contractants disposant de bases de données ADN en service, les échantillons et les profils génétiques qui en sont tirés doivent être respectivement détruits ou effacés soit immédiatement soit dans un certain délai après un acquittement ou un non-lieu. Certains États contractants autorisent un nombre restreint d'exceptions à ce principe. La Cour relève que l'Angleterre, le pays de Galles et l'Irlande du Nord sont les seuls ordres juridiques au sein de Conseil de l'Europe à autoriser la conservation illimitée des empreintes digitales, échantillons biologiques et profils ADN de toute personne, quel que soit son âge, soupçonnée d'avoir commis une infraction emportant inscription dans les fichiers de la police. En particulier, les données en cause peuvent être conservées quelles que soient la nature et la gravité des infractions dont la personne était à l'origine soupçonnée et indépendamment de son âge ; la conservation n'est pas limitée dans le temps ; et il n'existe que peu de possibilités pour un individu acquitté d'obtenir l'effacement des données de la base nationale ou la destruction des échantillons. La Cour estime en outre que la conservation de données relatives à des personnes non condamnées peut être particulièrement préjudiciable dans le cas de mineurs, tel le premier requérant, en raison de leur situation spéciale et de l'importance que revêt leur développement et leur intégration dans la société. En conclusion, la Cour estime que le caractère général et indifférencié du pouvoir de conservation des empreintes digitales, échantillons biologiques et profils ADN des personnes soupçonnées d'avoir commis des infractions mais non condamnées, tel qu'il a été appliqué aux requérants en l'espèce, ne traduit pas un juste équilibre entre les intérêts publics et privés en jeu, et que l'État défendeur a outrepassé toute marge d'appréciation acceptable en la matière. Ainsi, la conservation en cause s'analyse en une atteinte disproportionnée au droit des requérants au respect de leur vie privée et ne peut passer pour nécessaire dans une société démocratique. La Cour conclut à l'unanimité qu'il y a eu en l'espèce violation de l'article 8. Il semble que seules les données personnelles ayant un lien très intime avec l'individu semblent impliquer un tel degré de contrôle de proportionnalité.

169 La proportionnalité *stricto sensu*. L'article 52 paragraphe 1 de la Charte énonce que « dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ». Sur ce fondement, la Cour a explicitement dégagé les trois éléments du principe de proportionnalité lorsqu'elle contrôle les restrictions au droit à la protection des données personnelles (la mesure restrictive contrôlée doit être appropriée à la réalisation de l'objectif poursuivi, la mesure restrictive contrôlée est indispensable pour atteindre le but recherché, la mesure de restriction choisie doit être celle qui limite le moins le droit ou la liberté concernée). L'affaire *Volker und Markus Schecke*[1389] offre l'opportunité de suivre le raisonnement de la Cour de justice dans le triple test

1389 CJUE aff. Jointes C-92/09 ET C-93/09 Volker und Markus Schecke c. Land Hessen, 9 novembre 2010, § 86 et 89.

de proportionnalité. La Cour de justice a conclu que le Conseil et la Commission, en imposant la publication de données à caractère personnel relatives aux bénéficiaires d'une aide (provenant d'un fond agricole), sans opérer de distinction, telles que les périodes pendant lesquelles ils avaient perçu de telles aides, la fréquence ou encore le type de celles-ci, excédaient les limites qu'impose le respect du principe de proportionnalité. Par conséquent, la Cour de justice a jugé nécessaire d'annuler certaines dispositions du règlement n° 1290/2005 du Conseil et d'annuler le règlement n°295/20081390. Si en l'espèce la publication a été jugée apte à poursuivre l'objectif affiché, elle n'a pas été jugée nécessaire au regard de cet objectif. Elle ne constituait pas une entrave minimale au droit à la protection des données personnelles car les institutions communautaires auraient pu moduler la publication en fonction des périodes concernées, du montant ou du type d'aides perçues. De telles données, par leur nature, sont susceptibles de porter une atteinte particulièrement grave. La Cour de justice a effectué un contrôle approfondi dans l'affaire *X c. Commission* relative au dépistage du Sida dans le cadre d'examens médicaux préalables à l'engagement dans la fonction publique communautaire. La Cour a considéré que le requérant avait expressément refusé de se soumettre à un test de dépistage du sida et que par conséquent, en l'absence de consentement, les examens médicaux préalables au recrutement ne sauraient aboutir à soupçonner ou à constater l'existence de cette maladie[1391]. Selon la Cour de justice la création d'une base centralisée des empreintes digitales est ainsi vue comme l'indice d'une atteinte de nature à affecter gravement le droit à la protection des données personnelles qu'il appartient aux juridictions nationales de prendre en compte[1392]. Ainsi dans l'affaire *Shwarts*, imposant la mise en place de passeports biométriques, la Cour estime que ledit système ne saurait constituer « une base juridique à une éventuelle centralisation des données collectées sur son fondement ou à l'utilisation de ces dernières à d'autres fins que celle visant à empêcher l'entrée illégale de personnes sur le territoire de l'Union ». Le stockage des empreintes digitales sur un support de stockage hautement sécurisé risque de réduire le risque de falsification de passeports et de faciliter le travail des autorités chargées de vérifier l'authenticité des passeports aux frontières de l'Union. Ainsi, l'action consistant à prendre les empreintes de deux doigts, qui ne provoque aucun inconfort physique ou mental, ainsi qu'une image du visage, est appropriée. Aussi, il n'existe aucune alternative apparente suffisamment efficace et moins menaçante pour les droits protégés car l'analyse par iris constitue une technologie peu avancée par rapport à la reconnaissance d'empreintes digitales[1393]. La préoccupation selon laquelle les données peuvent être stockées centralement et utilisées à d'autres fins (par exemple, une enquête criminelle ou pour surveiller indirectement la personne) n'affecte pas la validité du règlement, qui prévoit uniquement la prévention de l'entrée illégale dans l'UE.

1390 Règlement n° 1290/2005 du Conseil du 21 juin 2005 relatif au financement de la politique agricole commune ; le Règlement n°295/2008 de la Commission du 18 mars 2008 portant modalités d'application du Règlement n° 1290/2005 du Conseil en ce qui concerne la publication des informations relatives aux bénéficiaires de fonds en provenance du Fonds européen agricole de garantie et du Fonds européen agricole pour le développement rural.

1391 CJCE, 5 octobre 1994, *X c. Commission,* aff 404/92, Rec. p. I-4737.

1392 CJUE, 17 octobre 2013, *M. Schwarz c. Stadt Bochum,* aff. C 291/12, §§ 61-62. Sur le contrôle de proportionnalité strict §48.

1393 Voy. § 48-53.

Dans l'arrêt *Tele2*, la Cour de justice évalue la légitimité des mesures restrictives du droit à la protection des données à caractère personnel afin de lutter contre la criminalité grave et le terrorisme à travers le principe de proportionnalité au sens strict[1394].
Ainsi la Cour affirme que, même si l'efficacité de la lutte contre la criminalité grave peut dépendre dans une large mesure de l'utilisation des techniques d'enquête les plus avancées, un tel objectif d'intérêt général ne peut en soi justifier une législation nationale prévoyant une conservation généralisée et indifférenciée de l'universalité du trafic et des données de localisation des utilisateurs. De plus, une des raisons qui a conduit la Cour de justice à émettre son avis négatif sur la conclusion de l'accord PNR UE-Canada concerne le non-respect de la proportionnalité des mesures, qui devraient être liées à une intensité et modulation différente selon que les données à caractère personnel concernent le franchissement des frontières, le séjour ou la période après le départ. Selon la Cour, lors du contrôle des frontières, le traitement des données peut être justifié par des raisons de sécurité. Autrement, pendant le séjour et après le départ du voyageur, la Cour exige la détermination préalable des conditions de fond et de procédure spécifiques régissant l'accès et l'utilisation des données PNR par les autorités publiques.

Section II. Les limites dérivant des interactions avec d'autres droits et intérêts légitimes

170 Un droit fondamental relatif. Le droit fondamental à la protection des données personnelles n'est pas un droit absolu. Ainsi il doit être pondéré avec d'autres droits et intérêts légitimes comme le droit à recevoir des informations, la liberté d'expression, etc. C'est l'hypothèse dans laquelle un individu invoque un autre droit fondamental à l'encontre du droit à la protection de ses données personnelles qu'il entend réduire ou auquel il entend renoncer[1395].
Dans le système de la CEDH, la protection des données personnelles garantie par l'article 8 doit être appliquée tout en respectant la portée d'autres droits concurrents. La possibilité de limiter les droits fondamentaux au nom des droits et libertés d'autrui est prévue à l'article 8.2 de la Convention européenne. De même, l'article 52.1 de la Charte des droits fondamentaux admet que le besoin de protection « des droits et libertés d'autrui » peut constituer une limite à l'exercice de droits consacrés tels que le droit à la protection des données personnelles. Ainsi, le droit à la protection des données personnelles n'apparaît pas comme une prérogative absolue mais doit être pris en compte par rapport à sa fonction dans la société [1396] conformément au

---

1394 L. WOODS, « Data Retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson *(Grand* Chamber) », EU Law Analysis, 21 December 2016, disponibile à l'adresse : http://eulawanalysis.blogspot.com/2016/12/data-retention-and-national-law-ecj.html.

1395 F. SUDRE, *Les conflits de droits. Cadre général d'approche dans la jurisprudence de la Cour européenne des droits de l'homme*, préc, spéc. p. 240-244.

1396 CJUE, *Volker und Markus Schecke c. Land de Hessen*, affaires jointes C-92/09 et C-93/09, 9 novembre 2010 § 48.

principe de proportionnalité. Le droit à la protection des données personnelles peut se voir limité au nom d'autres droits fondamentaux dont la finalité est antinomique. Ce conflit de droits est direct car il « oppose deux droits individuels concurrents garantis par le texte de référence, constitution, loi ou texte conventionnel, selon le système juridique considéré. Il s'agit là du "vrai" conflit de droits, qui met aux prises deux intérêts privés antinomiques tel que l'État ne peut garantir l'exercice d'un droit qu'au détriment de l'autre droit, par la limitation de celui-ci »[1397]. Le droit à la vie privée et à la protection des données personnelles constitue le terrain idéal pour explorer les antinomies entre les droits fondamentaux[1398]. Ce droit doit être mis en balance avec notamment la liberté d'expression (§1) et le droit de propriété (§2).

§1. La pondération avec le droit à la liberté d'expression

171 Le droit de recevoir et de communiquer des informations. Lorsque les données litigieuses sont diffusées par un tiers, les droits de ce dernier, tel que sa liberté d'expression, se heurtent bien souvent au droit à la protection des données personnelles[1399] et à la vie privée[1400] de la personne concernée. La liberté d'expression est souvent considérée comme étant la plus fondamentale des libertés et sans laquelle une société démocratique ne pourrait exister. Elle est susceptible de limiter le droit à la protection des données personnelles. Le conflit qui peut en résulter donne alors lieu à un exercice délicat de mise en balance des différents droits fondamentaux en présence[1401]. A cet égard, la Cour de justice de l'Union européenne laisse bien souvent le soin aux États membres d'adopter les mesures nécessaires afin de garantir leur protection[1402]. La liberté d'expression est garantie à plusieurs niveau par l'article 11 de la

---

1397 F. SUDRE, *Les conflits de droits. Cadre général d'approche dans la jurisprudence de la Cour européenne des droits de l'homme* , op. préc, spéc. p. 241.

1398 D'ailleurs, le problème inhérent au conflit entre droit à la protection des données personnelles et exercice d'autres droits fondamentaux a été pris en considération par la Directive 95/46. Ainsi l'art. 7/f), repris à l'art. 6.1/f) du Règlement, autorise le traitement de données personnelles si la satisfaction d'un intérêt légitime du responsable le rend nécessaire et à condition que les droits et les intérêts du titulaire des données ne prévalent pas ; l'art. 8 de la Directive (art. 9 du Règlement), qui, après avoir établi une interdiction générale concernant le traitement de certaines catégories de données, prévoit des exceptions relatives notamment à la sauvegarde d'un intérêt vital du titulaire des données et l'art. 9 de la Directive (art. 85 du Règlement) qui, de la manière la plus nette, reflète cette dispute en obligeant les États membres à prévoir des exemptions et des dérogations à certaines de ses dispositions afin de concilier le droit à la protection des données personnelles avec la liberté d'expression. Comme le relève la CJ dans l'affaire Bodil Lindqvist, le législateur européen s'est efforcé de concilier les dispositions de la Directive avec d'autres droits fondamentaux susceptibles d'être affectés par son application. Voy. CJCE (affaire C-101/01 « Bodil Lindqvist », §§ 84 et 90).

1399 Art. 8 de la Charte des droits fondamentaux de l'Union européenne, C 364, *J.O.C.E.*, 18 décembre 2000, p. 1.

1400 Art. 7 de la Charte des droits fondamentaux de l'Union européenne, C 364, *J.O.C.E.*, 18 décembre 2000, p. 1.

1401 M. FAZLIOGLU, « Forget me not : the clash of the right to be forgotten and freedom of expression on the Internet », International Data Privacy Law, 2013, p. 150 ; M. BASSINI et O. POLLICINO, *Reconciling the right to be forgotten and freedom of information in the digital age. Past and future of personal data protection in the EU*, 2014, disponible à l'adresse : http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wcclcmdc/ wccl/papers/ws14/w14-Pollicino&Bassini.pdf.

1402 D'ailleurs le législateur a prévu à l'art. du RGPD que relève aux États membres de concilier le droit à la protection des

Déclaration des droits de l'homme et du citoyen de 1789[1403]. Elle est consacrée à l'article 10 de la Convention européenne et ses limitations sont prévues par le paragraphe 2. Ainsi, une limitation doit être prévue par la loi et être nécessaire, dans une société démocratique, à la protection de la réputation ou des droits d'autrui. L'article 10 CEDH correspond à l'art. 11 de la Charte des droits fondamentaux (liberté d'expression et d'information). Ce droit comprend « la liberté d'opinion et la liberté de recevoir ou de communiquer des informations ou des idées sans qu'il puisse y avoir ingérence d'autorités publiques et sans considération de frontières ». Conformément à l'article 52.3 de la Charte, pour autant qu'elle contienne des droits correspondant à des droits garantis par la CEDH, « leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ». Ainsi la Cour de Strasbourg a affirmé que le droit à la protection des données doit être mis en balance[1404] tant sous l'angle de l'art. 11 de la Charte que de l'art 10 de la CEDH[1405]. De plus la problématique n'a pas échappé au législateur qui a introduit déjà dans la directive 95/46 une disposition garantissant certaines dérogations en faveur de la liberté d'expression[1406]. La liberté d'expression et d'accès à l'information constitue l'une des manifestations les plus emblématiques d'un État de Droit[1407]. Ledit droit peut entrer en conflit avec le droit à la protection des données personnelles. Un tel conflit se manifeste dans les intérêts opposés, d'une part, de ne pas voir ses données personnelles divulguées, d'autre part, du droit d'accéder aux informations, y compris aux données personnelles. De plus, d'autres questions ont été évoquées par l'arrivée d'Internet. Cela a conduit à multiplier les circonstances dans lesquelles ces deux droits peuvent se trouver en conflit. Le droit d'accès aux informations a d'ailleurs connu une évolution importante. Si l'on pense qu'on est passé de

---

données à caractère personnel avec la liberté d'expression et d'information. Les États membres peuvent également adopter des règles spécifiques en droit national pour concilier le droit à la protection des données à caractère personnel avec l'accès du public aux documents officiels et les obligations de secret professionnel.

1403 Cet article dispose que « la libre communication des pensées et des opinions est un des droits les plus précieux de l'homme ; tout citoyen peut donc parler, écrire, imprimer librement, sauf à répondre de l'abus de cette liberté dans les cas déterminés par la loi ».

1404 CEDH, 24 juin 2004, *Von Hannover c. Allemagne*, req. n°59320/00, Rec. 2004-VI, §§ 56-60 : la Cour livre à l'occasion de cet arrêt relatif à la publication de photographies ayant pour seul objet de satisfaire la curiosité d'un certain public sur la vie privée d'une personne, une grille d'analyse sur les limites au droit au respect de la vie privée au nom de la liberté d'expression ; P. Wachsmann, Secrets petits et grands. Sur deux arrêts de la Cour européenne des droits de l'homme (Société Plon c. France du 18 mai 2004 et Von Hannover c. Allemagne du 24 juin 2004), L'Europe des libertés, 2004, disponible à : http://leuropedeslibertes.ustrasbg. fr/article.php?id_article=141&id_rubrique=8.

1405 CEDH, Verlagsgruppe News GmBH c. Autriche (n°2), req. n°10520/02, 14 décembre 2006, § 40 : la Cour reprend dans cet arrêt relatif à la publication de photographies pour illustrer des articles sur un magnat de l'industrie accusé de fraude fiscale la même grille d'analyse que celle dégagée dans l'arrêt Von Hannover c/ Allemagne au titre de l'article 8,CEDH, Von Hannover c/ Allemagne, req. n°59320/00, 24 juin 2004.

1406 Comme l'a déjà exprimé la Cour de justice de l'Union Européenne, le législateur européen s'est efforcé de concilier les dispositions de la Directive avec d'autres droits fondamentaux susceptibles d'être affectés par son application (affaire C-101/01 « Bodil Lindqvist », §§ 84 et 90).

1407 L'importance attachée à cette liberté est telle que les restrictions établies par le législateur arrivent même à être examinées avec une présomption d'inconstitutionnalité. La CourEDH lui a consacré une étendue particulière en raison de l'ouverture d'esprit, sans laquelle une société ne pourrait être considérée comme démocratique. Voy. sur ce point l'arrêt de la CeDH du 16 décembre 2010 dans l'affaire Aleksey Ovchinnikov c. Russie (§ 39). L'idée est reprise par la CJCE dans l'affaire C-274/99 « Bernard Connolly c. Commission » (§ 39). De plus, aux États-Unis, les restrictions établies par le législateur arrivent même à être examinées avec une présomption d'inconstitutionnalité. Pour une vision générale sur la liberté d'expression aux États-Unis, voy. Muhlmann, Decaux & Zoller, *La liberté d'expression*, Dalloz, 2016, p. 179-224.

l'absence de l'obligation de diffusion de l'information de la part de l'État[1408] à la consécration d'un véritable droit d'accès à l'information[1409]. La liberté d'expression sur Internet a créé des nouveaux conflits permettant la diffusion sur Internet d'informations sur autrui conduisant à les mettre à disposition d'un nombre indéfini de personnes. Cela doit se concilier avec le droit à la protection des données personnelles[1410]. Ainsi Internet est un outil d'information différent de la presse écrite, posant des risques plus importants pour les droits protégés en vertu de l'article 8 de la Convention[1411]. Ce conflit se résout avec la pondération entre le droit à la protection des données personnelles et le droit à la liberté d'expression. Toutefois, une distinction est nécessaire entre la liberté d'expression dans la presse (A) et sur Internet (B).

A. La conciliation avec la liberté d'expression dans la presse

172 Les conditions de divulgation des données personnelles à travers la presse. C'est d'abord en matière de journalisme de presse que la liberté d'expression peut limiter le droit à la protection des données personnelles. Cela s'explique par l'intérêt du public d'être informé mais cela peut entrainer la divulgation des données personnelles. La CourEDH, à travers sa jurisprudence, admet des restrictions au droit à la protection des données personnelles en raison du droit à l'information du public si cela contribue au débat d'intérêt général[1412]. Toutefois cette liberté rencontre une limite lorsqu'il s'agit des données relatives à la santé [1413] ou à une procédure judiciaire impliquant un mineur[1414]. Les intrusions de la presse ou la divulgation dans les médias de détails de la vie privée mais non diffamatoires ont déjà été examinées par la CourEDH et par la Cour de justice qui ont rendu plusieurs arrêts illustrant cette mise en balance entre protection des données personnelles et intérêt du public à l'information. Ainsi, l'existence d'un débat d'intérêt général a permis la divulgation de données relatives à l'état de santé d'un

---

1408 Voy. sur cet aspet, l'Arrêt de la CEDH, Roche c. Royaume-Uni, 19 octobre 2005, § 172.

1409 CEDH, *Österreichische Vereinigung zur Erhaltung, Stärkung und Schaffung c. Autriche*, 28 novembre 2013, § 41.

1410 CJCE, Bodil Lindqvist, aff. C-101/01, 6 novembre 2003, Rec. I-12971, §§ 46-47.

1411 CEDH, *Węgrzynowski et Smolczewski c. Pologne*, no 33846/07, § 98, 16 juillet 2013.

1412 J.-F. FLAUSS, « La Cour européenne des droits de l'homme et la liberté d'expression journalistique », in E. ZOLLER (dir.), *La liberté d'expression aux États-Unis et en Europe*, Dalloz, coll. Thèmes et commentaires, 2008, pp. 97 et s., sp. p. 132

1413 Dans les affaires Armonienė c. Lituanie et Biriuk c. Lituanie (25 novembre 2008), la CourEDH a estimé que la divulgation de l'état de santé des requérants (qui étaient séropositifs) n'avait pas respecté les exigences de l'art. 8 de la CEDH (*cfr.* avec les arts. 8 de la Directive et 9 du Règlement).

1414 La publication de données relatives à la vie privée d'un mineur dans le contexte d'une procédure judiciaire a été jugée contraire à l'art. 8 de la CEDH (arrêt du 19 juin 2012 dans l'affaire *Kurier Zeitungsverlag und Druckerei GmbH c. Autriche*). Le Règlement n'est pas étranger à la problématique concernant le traitement de données appartenant à des mineurs et l'aborde dans plusieurs de ses articles (*cf.* arts. 6.1/f), 8, 12.1 et 57.1/b) du Règlement).

ancien président de la République[1415], la divulgation dans la presse d'informations relatives à la situation patrimoniale d'un homme politique[1416] ou encore la divulgation d'informations relatives à la situation fiscale d'un responsable du monde économique[1417]. Dans le droit de l'Union, on retrouve cette idée de la liberté d'expression comme intérêt du public à l'information. C'est l'article 9 de la directive 95/46 qui justifie la limitation du droit à la protection des données personnelles et qui impose aux États membres de prévoir des exemptions et dérogations à la protection des données personnelles lorsqu'elles sont utilisées aux seules fins de journalisme, d'expression artistique [1418] ou en matière de recherche scientifique[1419]. La liberté d'expression constitue selon la directive une justification possible à la collecte et la publication de données personnelles contenues dans des documents publics lorsque ces activités peuvent être qualifiées d'activités de journalisme, c'est-à-dire lorsqu'elles ont pour finalité la divulgation au public d'informations. Ainsi, la diffusion d'informations sur les revenus imposables des citoyens lorsque ceux-ci excèdent un certain seuil trouve un fondement dans la liberté d'expression[1420]. Dans la jurisprudence de la CEDH, le critère pour résoudre la mise en balance des droits en conflit est de savoir si l'expression en cause contribue à un débat d'intérêt général[1421]. La notion de vie privée comprend le droit à l'image d'une personne comme composante du droit à l'identité personnelle[1422] qui présuppose la maîtrise de son image, ce qui inclut la possibilité d'en refuser la diffusion. D'autre part, l'art. 10 CEDH permet à la presse de publier des photos d'un personnage public malgré l'absence de son consentement. Cela en raison de l'intérêt au débat général. La CourEDH dans l'affaire *Von Hannover c. Allemagne*[1423] a eu l'occasion de préciser le rapport entre les articles 8 et 10. Il

---

1415 CEDH, 18 mai 2004, Editions Plon c. France, req. n°58148/00, Rec. 2004-VI ; P. Wachsmann, « Secrets petits et grands. Sur deux arrêts de la Cour européenne des droits de l'homme (Société Plon c. France du 18 mai 2004 et Von Hannover c. Allemagne du 24 juin 2004) », préc. ; L. Dubouis, « Secret médical et liberté de la presse », RDSS, 2004, n° 4, pp. 841 et s. ; chron. F. Sudre, JCP-G, 2004, I, 161, n° 36 et C. Picheral, RDP, 2005, p. 702.

1416 CEDH, 26 février 2002, Krone Verlag Gmbh et Co. KG c/ Autriche, req. n° 34315/96.

1417 CEDH [GC], 21 janvier 1999, Fressoz et Roire c/ France, req. n° 29183/95, Rec. 1999-I ; CEDH, 14 décembre 2006, Verlagsgruppe News GmBH c/ Autriche (n°2), req. n°10520/02.

1418 La liberté artistique peut constituer une limite au droit à la protection des données personnelles. Elle a permis par exemple l'exposition d'un tableau contenant des photos de diverses personnalités publiques représentées dans des positions sexuelles. V. affaire CEDH, 25 janvier 2007, Vereinigung Bildender Kunstler c. Autriche, req. n°68354/01, §§ 26-34.

1419 La liberté de la recherche, qu'il s'agisse de la liberté de chercher et de la liberté de communiquer le résultat des recherches, est susceptible de limiter le droit à la protection des données personnelles. 95/46 CE, la Convention STE n° 108 et la législation française permettent la conservation de données personnelles pour des recherches scientifiques lorsqu'elles ne sont plus nécessaires au but initial de leur collecte. L'utilisation ultérieure des données personnelles pour des recherches scientifiques n'est pas considérée comme une finalité incompatible.

1420 CJCE, G. Ch., 16 décembre 2008, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, aff. C-73/07.

1421 En ce sens voy. K. Blay-Grabarczyk, « Précision de critères de résolution de conflits entre liberté d'expression et protection de la vie privée », *JCP*, 2012, p 292.

1422 CEDH, Sciacca c. Italie, no 50774/99, § 29.

1423 CEDH, Von Hannover c. Germany, no. 59320/00, §§ 56-81, ECHR 2004-VI, sur ce constat voy. A. SACCUCCI, « Libertà di informazione e rispetto della vita privata delle personalità politiche e di governo secondo la giurisprudenza della Corte di Strasburgo », in *Diritti umani e diritto internazionale*, 2010, n. 4, pp. 105-124.

s'agissait de la publication par des tabloïd allemands de photos de la princesse Caroline de Monaco prises illégalement dans sa résidence privée. Selon la Cour, pour savoir si l'on se trouve dans un cas de primauté de l'art. 10 sur l'art. 8 il faut tout d'abord prendre en compte le niveau de notoriété et l'exposition publique de la personne à qui les informations se réfèrent. Ensuite, il faut analyser le niveau de la vie privée auquel les informations se réfèrent (image, réputation). Troisièmement, il faut considérer l'existence d'un réel intérêt général du public à connaître certains aspects de la vie privée du personnage public. Ce dernier critère distingue l'intérêt général au débat dans une société démocratique d'une intrusion dans la vie privée d'une personne non publique. Malgré tout, si les personnalités publiques sont inévitablement exposées à une plus grande attention des médias, elles devraient être en mesure de voir leur vie privée respectée lorsque la publication de leurs photos et commentaires connexes est complètement détachée du « besoin de contribuer au débat des questions d'intérêt général » mais uniquement dédiée à satisfaire la curiosité d'une catégorie particulière de lecteurs. Ainsi la Cour a conclu à une violation de l'article 8. Toutefois, dans la deuxième affaire Von *Hanover c. Allemagne*[1424], la CourEDH a exclu la violation du droit au respect de la vie privée au titre de l'article 8 CEDH lorsque la princesse Caroline de Monaco s'est vue refuser une injonction contre la publication d'une photographie la représentant avec son mari pendant des vacances au ski et qui faisait référence à l'état de santé du prince Rainier. La qualification de la maladie du prince Rainier comme « événement de l'histoire contemporaine » par les juridictions nationales n'était pas déraisonnable et avait contribué au débat d'intérêt général. Suivant sa jurisprudence, la CourEDH a jugé, dans l'affaire *Axel Springer AG c. Allemagne*[1425] , que l'interdiction imposée par un tribunal de publier dans un journal, un article sur l'arrestation et la condamnation d'un acteur bien connu constituait une violation de l'article 10 de la CEDH[1426]. La Cour a dû déterminer si cette ingérence était nécessaire dans une société démocratique. La Cour a estimé que dans la mise en balance entre le droit à la liberté d'expression et le droit au respect de la vie privée le fait que les articles publiés concernaient l'arrestation et la condamnation d'une personne publique constituait des informations d'intérêt public. De plus, les faits judiciaires en général sont considérés comme des informations intéressant le public, et l'acteur avait déjà donné des nombreuses interviews laissant entendre que son atteinte à la protection de la vie privée était réduite. En ce qui concerne les méthodes d'obtention des informations et leur fiabilité, le premier article sur l'arrestation de l'acteur était fondé sur les informations fournies par le bureau du procureur. Il n'y avait pas eu de comportement intrusif

---

1424 CEDH, Von Hannover c. Allemagne, n° 40660/08 et 60641/08, § 118 and § 124, ECHR 2012, su cui A. SACCUCCI, cit.

1425 CEDH, Axel Springer AG c. Allemagne, n°39954/08, §§ 90 and 91, 7 février 2012.

1426 Le requérant a été rédacteur en chef d'un journal quotidien national largement diffusé dans lequel il avait publié un article en première page sur la star d'une série télévisée populaire qui avait été arrêté à Monaco, à la fête de la bière, pour possession de cocaïne. La pièce était accompagnée, sur une autre page, d'un article détaillé avec trois photos de l'acteur. Immédiatement après la publication, le demandeur avait obtenu une injonction pour empêcher la publication de l'article ou des photos. L'interdiction de la publication de l'article a été confirmée en appel (la société requérante n'a pas saisi l'interdiction de la publication des photos). En novembre 2005, la société requérante a été condamnée à payer une amende minimale. Pendant ce temps, le journal avait publié un deuxième article, qui rapportait la condamnation de l'acteur pour possession illégale de drogues après la confession. Le demandeur a interjeté l'appel et a obtenu une injonction qui limitait la publication du deuxième article sensiblement la même base de motifs que la première demande. La décision a été confirmée en appel. La société requérante a finalement été condamnée à payer pour les violations ultérieures de l'injonction.

de la part du journal. La Cour a conclu que le journal requérant n'avait pas agi de mauvaise foi et que compte tenu de toutes les circonstances, les journalistes avaient estimé qu'il n'y avait aucune raison de préserver l'anonymat de l'acteur. De plus, les articles publiés n'avaient pas révélé de détails sur la vie privée de l'acteur, mais portaient sur les circonstances de son arrestation et l'issue du procès pénal. La Cour a relevé également qu'il n'avait pas été démontré que la publication des articles avait donné lieu à des conséquences graves pour l'acteur. Par conséquent, la Cour a jugé que les restrictions à la publication imposées à la société n'étaient pas raisonnablement proportionnées au but légitime de la protection de la vie privée de l'acteur. La CourEDH a conclu à une violation de l'article 10 CEDH. L'affaire *Moseley c.Royaume-Uni*[1427] concernait la publication dans un journal des photographies intimes du requérant. Le requérant se plaignait de la violation de l'article 8 CEDH au motif qu'il n'avait pas été en mesure de demander une injonction avant la publication des photos en question afin d'en bloquer la diffusion, et ceci en raison de l'absence d'une obligation de notification préalable par le journal de la publication de l'article susceptible de porter atteinte au droit au respect de la vie privée. La Cour a estimé que la divulgation des photographies avait des finalités de divertissement et non de véritable information, mais qu'une attention particulière devrait être portée aux conséquences d'une notification avant la publication qui pourrait constituer une forme de censure. Compte tenu de la marge d'appréciation des États en matière de mesures de protection [1428]et du fait que l'allocation de dommages-intérêts offre une réparation adéquate en cas de violations du droit au respect de la vie privée résultant de la diffusion d'informations à caractère privé[1429], la Cour a conclu que l'article 8 n'exigeait pas une obligation de notification préalable. Par conséquent, la Cour a exclu la violation de l'article 8. Ainsi dans la mise en balance des droits garantis par les articles 8 (droit au respect de la vie privée) et 10 (droit à la liberté d'expression), la CourEDH a favorisé le droit à l'information, spécialement sur des sujets d'intérêt général[1430]. L'activité de journaliste renforce le droit à la liberté d'expression parfois au détriment du droit à la protection des données personnelles (1). En particulier, la liberté d'expression comprend la liberté de recevoir les informations en raison du principe de transparence et le droit à la protection des données personnelles peut se voir limité (2).

1) Des exceptions renforçant la liberté d'expression

1427 En 2008, le tabloïd « News of the World » avait publié un article concernant l'ancien président de l'une des instances dirigeantes de Formule 1, Max Rufus Mosley et révélant des photos et des vidéos de sa participation à une « orgie nazie avec cinq prostituées ». L'intéressé avait intenté une action en dommages-intérêts pour divulgation d'informations confidentielles et atteinte à la vie privée ; en outre, il avait demandé le retrait de la vidéo en question du site web du journal. Cette injonction avait été refusée au motif que les informations n'étaient pas de nature privée. Toutefois la High Court avait retenu que les images, qui ne comportaient aucune connotation nazie, ne représentaient aucun caractère d'intérêt public, et que leur diffusion avait donc méconnu le droit de M. Mosley au respect de sa vie privée. La High Court lui avait accordé des dommages-intérêts

1428 CEDH, *Mosley c. Royaume-Uni*, n° 48009/08, 10 mai 2011, § 108.

1429 Sur ce point la Cour rappelle sa jurisprudence *Von Hannover c. Allemagne*, no 59320/00, 24 juin 2004, §120.

1430 Voy. sur cet aspect F. SUDRE, *Les grands arrêts de la Cour européenne des droits de l'homme*, 5e éd., PUF, 2009, p. 623.

173 Les activités relevant du journalisme. La Directive 46/95/CE prévoit, dans son article 9, l'obligation de la part des É tats membres d'introduire des exceptions à certaines de ses normes de manière à concilier la protection des données personnelles avec la liberté d'expression. Il s'agit des exceptions à des fins de journalisme ou d'expression artistique ou littéraire. Toutefois, la directive ne précise pas le sens de « journalisme ». C'est la jurisprudence qui a interprété de façon la plus large possible l'expression « journalisme » [1431]. Toutefois la large marge d'appréciation laissée aux États pour établir les exceptions entraîne comme conséquence des disciplines différentes [1432]. La jurisprudence de la Cour de justice en matière de liberté d'expression journalistique ne semble pas si élaborée que celle de la CourEDH. Ainsi, les conditions pour bénéficier de la liberté d'expression sont examinées dans l'affaire *Satamedia*[1433]. La Cour de justice a estimé que la seule divulgation au public d'informations, d'opinions ou d'idées constitue un motif suffisant pour qu'une activité bénéficie du titre de journalisme, sans analyser si la publication remplit une mission d'intérêt général qui puisse justifier des restrictions au droit à la protection des données personnelles[1434]. Même si les
raisonnements de la Cour de justice et de la CEDH se ressemblent[1435], la jurisprudence de la CourEDH semble plus élaborée. Dans son jugement, la CourEDH analyse le fait que l'information divulguée soit d'intérêt public ou susceptible d'ouvrir un débat d'intérêt général[1436]. Au fil de sa jurisprudence, la CourEDH a ajouté d'autres critères tels que la sévérité de la sanction imposée à l'éditeur d'un quotidien[1437] ou l'objectivité et la bonne foi dans la présentation de l'information[1438]. Ainsi dans l'affaire *Nagla c. Latvia*[1439], elle a accordé à la

1431 Voy. CJCE, Tietosuojavaltuutettu c. Satakunnan Markkinapö rssi Oy et Satamedia Oy, C-73/07, § 56.

1432 Une avancée a été realisée par le nouveau Règlement qui reprend les concepts de journalisme et d'expression artistique et littéraire, et ajoute celui d'expression universitaire, mais sans qu'aucune définition qui permette de les préciser ne soit offerte. Toutefois, il impose aux É tats de prévoir des exemptions et des dérogations à certaines de ses dispositions afin de concilier la protection des données personnelles avec la liberté d'expression et l'obligation de notifier à la Commission les dispositions normatives adoptées en vertu de l'art. 85.1 (art. 85.3), ce qui aidera à mieux coordonner les règles nationales lorsqu'elles seront adoptées.

1433 CJCE, *Tietosuojavaltuutettu c. Satakunnan Markkinapö rssi Oy et Satamedia Oy*, C-73/07 préc.

1434 La CJCE rappelle que la liberté d'expression s'applique non seulement aux entreprises de média, mais également à toute personne exerçant une activité de journalisme (§ 58), qu'une fin lucrative n'exclut a priori pas sa compatibilité avec ladite liberté (§ 59) et que le support utilisé pour s'exprimer ne constitue pas un critère déterminant pour apprécier s'il s'agit d'une activité journalistique (§ 60).

1435 La CEDH vérifie l'existence d'une prévision légale expresse si l'ingérence est nécessaire à la protection de la liberté d'expression et conforme au principe de proportionnalité. La CJ d'abord détermine si le but poursuivi par la limitation est légitime et a été prévu par la loi ; ensuite, en examinant si l'application du principe de proportionnalité était adéquate.

1436 Voy. CEDH, Axel Springer AG c. Allemagne, § 90, dans laquelle la Cour a reconnu l'existence d'un intérê t général lorsque la publication portait sur des affaires politiques, pénales ou mê me sportives et artistiques. Voy. également l'arrê t von Hannover c. Allemagne (7 février 2012) dans laquelle elle expose les critères pour concilier la vie privée avec la liberté d'expression (§§ 109-113) : l'ouverture d'un débat public, le rô le joué par un individu dans la sphère publique, sa conduite préalable, le contenu, forme et conséquences de la publication ainsi que les circonstances dans lesquelles les données personnelles ont été traitées.

1437 CEDH, affaire *Axel Springer AG c. Allemagne* préc.

1438 CEDH, *Saaristo et autres c. Finlande*, 12 octobre 2010, § 65.

1439 CEDH, *Nagla c. Latvia*, req. no. 73469/10, 16 Juillet 2013.

liberté d'expression journalistique dans le cadre d'une enquête une étendue particulière. L'affaire concernait une perquisition, menée à l'initiative de la police et validée a posteriori par un juge, sur l'ordinateur d'un journaliste afin de saisir du matériel numérique. La source du journaliste était soupçonnée d'accès non autorisé aux systèmes informatiques et de diffusion illicite de données électroniques. Compte tenu de l'ingérence dans la liberté de recevoir et de communiquer des informations, la Cour a jugé que, si la perquisition était prévue par la loi et poursuivait un but légitime, elle ne remplissait pas le critère de « nécessité » dans une société démocratique. En fait, la perquisition urgente avait été ordonnée en raison du danger que le matériel soit effacé ou endommagé. Toutefois, il n'y avait aucune preuve que le journaliste disposait du matériel puisque des mois s'étaient écoulés depuis le dernier contact entre le journaliste et sa source. La Cour rappelle que le droit d'un journaliste de ne pas révéler sa source est un élément essentiel de la liberté d'expression[1440]. De plus il s'agit également du droit du public à recevoir des informations sur des sujets brûlants d'intérêt public. Par conséquent, les perquisitions de l'appartement du journaliste avaient méconnu son droit à la liberté d'expression, mais aussi celle de chaque individu à recevoir des informations.

2) Le principe de transparence comme limite au droit à la protection des données personnelles

174 La transparence. Un objectif d'intérêt général. En ce qui concerne le droit de recevoir des informations, qui fait également partie de la liberté d'expression, on se rend de plus en plus compte de l'importance de la transparence du gouvernement pour le fonctionnement d'une société démocratique. La transparence est un objectif d'intérêt général susceptible de justifier une ingérence dans le droit à la protection des données, si nécessaire et proportionnée. En conséquence, le droit d'accès aux documents détenus par les autorités publiques au cours des deux dernières décennies a été reconnu comme un droit important de tout citoyen de l'UE et de toute personne physique ou morale résidant ou ayant son siège dans un État membre. Le droit d'accès aux documents est lié au caractère démocratique de l'Union. La transparence garantit une plus grande légitimité et responsabilité de l'administration dans un système démocratique car la possibilité pour les citoyens de connaître le fondement des règles communautaires est une condition de l'exercice de leurs droits. De plus, l'article 11 de la Charte (liberté d'expression) protège non seulement le droit de communiquer, mais aussi celui de recevoir des informations[1441]. Ainsi, avec le traité de Lisbonne, le principe d'ouverture comme celui de

1440 Voy. en ce sens J.-F. FLAUSS, « La Cour européenne des droits de l'homme et la liberté d'expression journalistique », in E. ZOLLER (dir.), *La liberté d'expression aux États-Unis et en Europe*, Dalloz, coll. Thèmes et commentaires, 2008, pp. 97 et s.

1441 L'importance de la transparence gouvernementale pour le fonctionnement d'une société démocratique se fait de plus en plus ressentir. Dans le droit du CdE on peut renvoyer à la convention sur l'accès aux documents officiels, STE n° 205, 18 juin 2009. Dans le droit de l'UE, le droit d'accès est garanti par le règlement 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission. L'article 42 de la Charte et l'article 15, paragraphe 3, du TFUE ont étendu ce droit d'accès aux documents des institutions, organes, et organismes de l'Union.

transparence trouvent leur place dans le droit primaire de l'Union[1442]. Les demandes d'accès à des documents ou à des informations détenues par des autorités publiques peuvent donc nécessiter un équilibre avec le droit à la protection des données des personnes dont les données figurent dans les documents demandés[1443]. Ainsi l'UE a adopté le règlement 1049/2001/CE relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission[1444]. Toutefois, la divulgation de documents sur la base du droit d'accès peut entrer en conflit avec le droit à la protection des données si l'accès à un document révèle les données personnelles d'autres personnes. L'article 4 §1 du règlement 1049/2001 formule deux exceptions au droit d'accès. Elles sont relatives à la protection de l'intérêt public et au respect de la vie privée au cas où la divulgation du document leur « porterait atteinte ». Dans l'affaire *Bavarian Lager* [1445], la Cour de justice a défini l'étendue de la protection des données personnelles dans le contexte de l'accès aux documents des institutions communautaires, ainsi que les relations entre les règlements 1049/2001(relatif à l'accès aux documents) et le règlement 45/2001 (relatif à la protection des données)[1446]. Selon cette décision, une ingérence dans le droit à la protection des données personnelles à l'égard de l'accès à des documents requiert un motif spécifique et justifié. Le droit d'accès à des documents ne peut automatiquement pas écarter le droit à la protection des données. La Cour de justice a ensuite conclu que c'était à bon droit que la Commission avait rejeté la demande d'accès au procès-verbal complet de sa réunion. En l'absence du consentement des cinq participants à cette réunion, la commission avait dûment respecté son obligation d'ouverture en communiquant une version du document occultant leurs noms. Dans les affaires jointes *Volker und Markus Schecke et Harmut Eifer c. Land Hessen*[1447], la Cour de justice devait se prononcer sur la proportionnalité de la publication sur Internet, requise par la législation européenne, du nom des bénéficiaires d'aides agricoles

---

1442 L'article 11 §2 TUE s'adresse directement aux institutions qui doivent entretenir « un dialogue ouvert, transparent et régulier » avec la société civile et les associations représentatives. Il assigne ainsi une dimension active au principe d'ouverture. Le traité sur le fonctionnement de l'Union (TFUE) apporte un fondement supplémentaire au principe en fixant les conditions de sa concrétisation dans son article 15 §1 TFUE. Obligation est faite aux « institutions, organes et organismes de l'Union d'œuvrer « dans le plus grand respect possible du principe d'ouverture » et ce « afin de promouvoir une bonne gouvernance, et d'assurer la participation de la société civile».

1443 D'ailleurs l'article 86 du règlement général sur la protection des données dispose clairement que les données à caractère personnel contenues dans les documents officiels détenus par les autorités et organismes publics peuvent être divulguées par l'autorité ou l'organisme concerné conformément à la législation de l'Union européenne101 ou des États membres droit à la protection des données conformément à la réglementation.

1444 Règlement (CE) no1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission. JO L 145 du 31.05.2001 p. 43.

1445 CJUE, *Commission européenne c. The Bavarian Lager Co. Ltd*., C-28/08 P, 29 juin 2010, § 60,63,76,78, 79.

1446 La société Bavarian Lager importait de la bière allemande en bouteille au Royaume-Uni. Elle avait toutefois rencontré des difficultés car la législation britannique favorisait de fait les producteurs nationaux. En réponse à la plainte, la Commission européenne a décidé d'engager une procédure contre le Royaume-Uni pour manquement à ses obligations. Bavarian Lager demandait aussi à la Commission une copie du procès-verbal d'une réunion entre la Commission et les autorités britanniques. La Commission a accepté de communiquer certains documents relatifs à la réunion mais a occulté cinq noms dans le procès-verbal, car cinq personnes s'etaient opposées à la divulgation de leur identité. La commission a rejeté un nouveau recours de Bavarian Lager visant à obtenir le procès-verbal complet, citant la protection des données personnelles. Insatisfaite de cette décision, Bavarian lager a formé recours devant le tribunal de première instance, qui avait annulé la décision de la commission, considérant que la simple inscription des noms des personnes en question sur la liste des participants à une réunion ne constituait pas une atteinte à la vie privée. Sur pourvoi de la Commission, la CJUE a annulé la décision du tribunal de première instance.

1447 CJUE, *Volker und Markus Schecke et Harmut Eifer c. Land Hessen,* affaires jointes C-92/09 et C-93/09, 9 novembre 2010, §47 à 52, 58, 66, 75, 86, 92.

européennes et des montants qu'ils avaient reçus [1448] . La Cour, relevant que le droit à la protection des données personnelles n'est pas une prérogative absolue, a soutenu que la publication sur un site Internet des données nominatives relatives aux bénéficiaires de deux fonds agricoles européens et aux montants précis perçus par ceux-ci constituait une ingérence dans leur vie privée en général, et dans la protection de leurs données à caractère personnel en particulier. La Cour a considéré qu'une telle atteinte aux articles 7 et 8 de la Charte était prévue par la loi et répondait à un objectif d'intérêt général reconnu par l'Union, à savoir accroître la transparence de l'utilisation des fonds communautaires. Toutefois la Cour de justice a considéré que la publication des noms des bénéficiaires des deux fonds, avec le montant exact reçu, constituait une mesure disproportionnée et n'était pas partiellement justifiée au regard de l'article 52, §1 de la Charte. La Cour a donc jugé partiellement nulle la législation européenne sur la publication d'informations relatives aux bénéficiaires de fonds agricoles européens. Ainsi, l'application du principe de proportionnalité a conduit le juge dans lesdites affaires à annuler les mesures prévues dans la législation de l'Union[1449]. Toutefois dans l'affaire *Bavarian Lager*, la Cour de justice a concilié des instruments opposés de droit dérivé avec l'article 8 de la CEDH[1450]. Les objectifs de transparence et de contrôle public de l'activité administrative à travers l'accès à l'information constituent des raisons d'intérêt général qui peuvent limiter le droit à la protection des données. Ce contrôle a été mené par la CJ grâce à l'application du principe de proportionnalité au cas par cas. La CourEDH s'est penchée sur la question du droit d'accès dans l'affaire *M.G. c. Royaume-Uni*[1451]. Le requérant demandait à avoir accès à ses dossiers détenus par les services sociaux. Il se plaignait notamment d'avoir subi des sévices de la part de son père lorsqu'il entait enfant et se référait à son besoin d'obtenir toutes les informations pertinentes et au fait que l'autorité locale ne lui avait pas divulgué l'intégralité des dossiers le concernant détenus par les services sociaux. En outre, il n'avait pu se prévaloir d'aucun droit légal d'accès à ces dossiers, ni d'aucune indication précise, par la voie d'une circulaire ou législation contraignante, quant aux motifs pour lesquels il pouvait demander l'accès ou contester le refus de lui donner un tel accès. De plus, il ne disposait d'aucun recours devant un organe indépendant pour contester le refus de lui donner cet accès. Dès lors, la Cour a conclu que le gouvernement avait failli à son obligation positive de protéger la vie privée et

1448 Dans le droit de l'UE le principe de transparence est consacré aux articles 1 et 10 du TUE et à l'article 15, §1 du TFUE. Aux termes du considérant 2 du règlement CE n° 1049/2001, la transparence permet d'assurer une meilleure participation des citoyens au processus décisionnel, ainsi que de garantir une plus grande légitimité, efficacité et responsabilité de l'administration à l'égard des citoyens dans un système démocratique. Dans ce contexte le règlement CE n° 1290/2005 du Conseil relatif au financement de la politique agricole commune et le règlement CE n° 259/2008 de la Commission portant modalités de son application requièrent la publication d'informations sur les bénéficiaires de certains fonds européens dans le secteur agricole et des montantes perçus. La publication doit contribuer au contrôle public de l'utilisation approprié de fonds publics par l'administration. La proportionnalité de cette publication a été contestée par plusieurs bénéficiaires.

1449 Ainsi cette décision a entraîné l'annulation de l'art. 44 bis du Règlement n° 1290/2005 et du Règlement n° 259/2008.

1450 Dans son arrêt Bavarian Laeger du 29 juin 2010 (affaire C-28/08 P), la CJUE a conclu que l'accès aux documents en possession des institutions européennes (régi par le Règlement n° 1049/2001, relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission) et contenant des données personnelles n'est possible que si le destinataire démontre la nécessité de les obtenir (condition prévue par l'art. 8/b du Règlement n° 45/2001 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données), même si l'art. 6.1 du Règlement n° 1049/2011 ne prévoit pas l'obligation de justifier la demande d'accès.

1451 CEDH, *M.G. c. le Royaume-Uni*, requête n° 39393/98, 24 septembre 2002.

familiale du requérant quant à l'accès aux dossiers le concernant en possession des services sociaux. Dans l'affaire *Client Earth et PAN Europe c. EFSA*[1452], la Cour de justice a examiné si la décision de l'Autorité européenne de sécurité des aliments (EFSA) de refuser aux demandeurs un accès aux documents était nécessaire pour protéger les droits des personnes à qui les documents se référaient. Les documents concernaient un projet de rapport d'orientation préparé par un groupe de travail de l'EFSA en collaboration avec des experts externes sur la mise sur le marché de produits phytopharmaceutiques. Dans un premier temps, l'EFSA a accordé un accès partiel aux demandeurs, refusant l'accès à certaines versions de travail du projet de document d'orientation. Par la suite, il a donné accès à la version préliminaire qui comprenait les commentaires individuels des experts externes. Cependant, il a supprimé les noms des experts en invoquant l'article 4, paragraphe 1, point b), du règlement n ° 45/2001 sur le traitement des données à caractère personnel par les institutions et organes de l'Union et la nécessité de protéger la vie privée des experts externes. En première instance, le Tribunal de l'UE a confirmé la décision de l'EFSA. En appel, la CJUE a conclu que l'accès aux données à caractère personnel des experts dans ce cas était nécessaire pour vérifier l'impartialité de chacun des experts externes dans l'accomplissement de leurs tâches en tant que scientifiques et pour garantir la transparence du processus de prise de décision dans l'EFSA. Selon la Cour de justice, l'EFSA n'a pas précisé en quoi la divulgation des noms des experts externes ayant formulé des commentaires spécifiques sur le projet de document d'orientation compromettrait les intérêts légitimes des experts. Un argument général selon lequel la divulgation risque de porter atteinte à la vie privée ne suffit pas si elle ne s'appuie pas sur des preuves spécifiques à chaque cas. Selon ces jugements, une ingérence dans le droit à la protection des données dans le contexte de l'accès à des documents nécessite une raison spécifique et justifiée. Le droit d'accès aux documents ne peut pas automatiquement restreindre le droit à la protection des données. Nous venons de voir comme la liberté d'expression concerne tant le droit de s'exprimer que le droit d'accès aux informations. Souvent cette liberté se heurte au droit à la protection des données personnelles et en général au droit à la vie privée. Une mise en balance des intérêts en jeu est alors nécessaire. Or, la liberté d'expression concerne le contenu de l'information ainsi que les moyens de transmission, parmi lesquels Internet assume une position particulière. Ainsi la CourEDH a estimé que la fonction remplie par Internet est essentielle pour une société démocratique, car il s'agit d'un moyen qui contribue grandement à la préservation et à l'accessibilité de l'actualité et des informations[1453].

B. La liberté d'expression sur Internet

175 Un conflit exacerbé par les nouveaux médias. La protection des données personnelles à l'ère du numérique a remis des questions en cause. Internet présente de nouveaux enjeux et les

1452 CJEU, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA), European Commission*, C-615/13P, 16 Juillet 2015.

1453 CEDH, Times Newspapers Ltd c. Royaume-Uni, 10 mars 2009, § 45.

informations récoltées en ligne (sur des réseaux sociaux, par les moteurs de recherche) constituent une mine d'or pour les commerciaux[1454]. Avec Internet on est passé des données de nature nominatives (adresse postale, nom) à des données de plus en plus propres à la personne (données relatives aux goûts, habitudes, comportements, tendances). Les atteintes aux données personnelles sont donc de plus en plus intrusives : on touche l'identité, la dignité, l'intimité de la personne. Ainsi dans l'affaire de la Grande Chambre *Animal Defenders International c. Royaume-Uni,* la CourEDH a défini ces « nouveaux médias » comme un puissant outil de communication [1455] . En effet, le numérique renforce certaines libertés comme le droit d'expression, mais en fragilise d'autres tel que le droit à la vie privée car les informations sont colletées contre la volonté de l'individu. Si la jurisprudence a étendu le champ d'application de l'article 10 dans l'activité de journalisme, c'est-à-dire lorsqu'elle a pour finalité la divulgation au public d'informations, d'opinions ou d'idées, elle a opéré une distinction entre éditeur d'un site web et moteur de recherche. Si l'éditeur d'un site Internet peut revendiquer un droit à la liberté d'expression, tel n'est pas le cas d'un moteur de recherche [1456] qui indexe les informations contenues sur le site et qui ne peut invoquer qu'un seul intérêt économique en s'abstenant de fonder l'activité des moteurs de recherche sur la liberté d'expression[1457]. Comme le relève l'Avocat général dans ses conclusions relatives à l'affaire *Google Spain*, s'agissant d'Internet, il convient de distinguer trois situations afférentes aux données à caractère personnel. La première est la publication d'éléments de données à caractère personnel sur n'importe quelle page web de l'Internet. La deuxième concerne le cas dans lequel un moteur de recherche sur Internet fournit des résultats de recherche qui dirigent l'utilisateur Internet vers la page web source. La troisième opération, moins visible, survient lorsqu'un internaute effectue une recherche en utilisant un moteur de recherche et que certaines de ses données à caractère personnel, telles que l'adresse IP à partir de laquelle la recherche est effectuée, sont automatiquement transférées chez le fournisseur de services de moteur de recherche sur Internet[1458]. Dans le cas spécifique d'Internet, dans sa jurisprudence, la Cour de justice a affirmé une nuance entre éditeur de site web et moteur de recherche. Si d'une part, l'éditeur d'un site web peut revendiquer le droit à la liberté d'expression afin de ne pas effacer les contenus du site web, tel n'est pas le cas de la présentation des résultats par un moteur de recherche[1459].

1454 V.F. ROCHELANDET, *Économie des données personnelles et de la vie privée*, La Découverte, Repères, 2010.

1455 CEDH, *Animal Defenders International c. Royaume-Uni*, req. n° 48876/08, § 124.

1456 Diversement aux États-Unis, la liberté d'expression des moteurs de recherche est reconnue sous la base du Premier Amendement. Voy. O. Bracha, The Folklore of Informationalism: The Case of Search Engine Speech, Fordham Law Review, vol. 82, iss. 4, 2014, pp. 1629-1687.

1457 CJUE, 13 mai 2014, *Google Spain* SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12, § 85. Sur ce constat v. A. Debet, *Google Spain* : Droit à l'oubli ou oubli du droit ? », préc., § 4. Pour une critique de cette abstention au regard de la jurisprudence de la Cour relative à la liberté d'expression v. S. Peer, The CJEU's *Google Spain* judgment: failing to balance privacy and freedom of expression, préc.

1458 Voy. point 3 de ses conclusions.

1459 CJUE, 13 mai 2014, Google Spain SL et Google Inc. c. Agencia Española de Protección de Datos (AEPD) et Mario Costeja González, aff. C-131/12, § 85. Pour une critique de ce constat, voy. A. DEBET, « Google Spain : Droit à l'oubli ou oubli du droit ? », *Comm.com, électr*, Juillet 2014, n. 7-8, étude n°13; S. PEERS, « The CJEU's Google Spain judgment: failing to balance privacy and freedom of expression », 13 mai 2014, disponible sur http://eulawanalysis.blogspot.fr/2014/05/the-cjeusgoogle- spain-judgment-failing.html. Ainsi la CJ, dans l'affaire Google Spain a rejeté la possibilité que les moteurs de

***176* La responsabilité des éditeurs d'un site web.** Au fil de sa jurisprudence, la CourEDH a garanti le droit à la liberté d'expression (droit de communiquer et de recevoir des informations) dans les différents médias, à la fois traditionnels et modernes, y compris les publications électroniques. La Cour a, en fait, souligné que l'article 10 de la Convention couvre non seulement le contenu de l'information, mais aussi les moyens de transmission, étant donné que les restrictions qui concernent les moyens ont également un impact sur la liberté de recevoir et de communiquer des informations. Pour garantir l'équilibre entre les articles 10 et 8 face aux moyens de transmission technologiques elle s'est appuyée sur un paramètre externe à la CEDH, à savoir la Convention du Conseil 108/1981 sur la protection des personnes physiques à l'égard du traitement automatisé des données à caractère personnel[1460]. La première fois que la Cour de Strasbourg a pris en compte la pondération du respect de la vie privée avec la liberté d'expression sur Internet, c'était dans l'arrêt *Éditions Plon c. France*[1461] concernant la diffusion d'un livre sur l'état de santé du président Mitterrand via Internet. La CourEDH avait considéré que la justice française, en interdisant la diffusion du livre pour violation du secret médical, avait violé le principe du droit à la liberté d'expression édicté à l'article 10 de la Convention EDH, en prononçant une mesure d'interdiction définitive « disproportionnée » et ne répondant à « nul besoin social impérieux ». La Cour de justice dans sa jurisprudence a ainsi considéré que la diffusion sur Internet d'informations sur autrui beneficie à la liberté d'informatione d'expression consacrée à l'article 10 de la Convention EDH[1462]. Toutefois ces informations peuvent contenir des propos diffamatoires qui peuvent porter atteinte au droit au respect de la réputation conçu comme composante du droit au respect de la vie privée. Dans l'arrêt *Delfi AS c. Estonie*[1463], la Cour de Strasbourg s'est prononcée sur l'équilibre entre liberté d'expression et le droit à la réputation en cas de diffusion d'articles par Internet. Il s'agit donc de trouver un juste équilibre entre l'exercice de la liberté d'expression et le droit à la réputation et de l'honneur d'autrui. Cet équilibre devra alors être recherché par le juge. Il s'agit d'intérêts légitimes qui doivent être mis en balance dans une société démocratique. La Grande Chambre a tout d'abord indiqué que « c'est la première fois qu'elle est appelée à examiner un grief s'inscrivant dans ce domaine technologique en évolution et que la possibilité pour les individus de s'exprimer sur Internet constitue un outil sans précédent d'exercice de la liberté d'expression »[1464]. À cet égard, la Cour a rappelé sa jurisprudence antérieure[1465]. En particulier

recherche puissent bénéficier des exceptions prévues à l'art. 9 de la Directive, et que le droit à l'oubli ne soit pas applicable face aux propriétaires de sites web en raison de leur liberté d'expression.

1460 CEDH, Amann c. Suisse [GC], no. 27798/95: »That broad interpretation corresponds with that of the Council of Europe's Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data, which came into force on 1 October 1985 and whose purpose relating to an identified or identifiable individual (Article 2)".

1461 CEDH, Éditions Plon c. France Requête no 58148/00, 18 juillet 2004.

1462 CJCE, Bodil Lindqvist, aff. n. C-101/01, 6 novembre 2003, §§ 46-47.

1463 CEDH, Delfi AS c. Estonia no. 64569/09, 10 octobre 2013.

1464 Voy. §111 de la décision.

1465 CEDH, Von Hannover c. Allemagne (no. 2) Gr. Ch., réq.n. 40660/08 et 60641/08,

elle a cité l'affaire *Krone Verlag GmbH & Co. KG c. Autriche* (n. 4) [1466] concernant la responsabilité de l'entreprise de médias dans un tel contexte. Dans l'affaire *Delfi* précitée, l'un des principaux portails d'information estonien, avait été mis en cause à raison de messages insultants publiés par certains lecteurs de ce site sous l'un des articles de presse qui y figurait. La question à trancher n'était pas de savoir s'il avait été porté atteinte à la liberté d'expression des auteurs des commentaires, mais si le fait de juger Delfi AS responsable de ces commentaires déposés par des tiers avait porté atteinte à sa liberté de communiquer des informations. Sur cette question nouvelle, la Grande Chambre a décidé que l'ingérence subie poursuivait un objectif légitime : la protection de la réputation et des droits d'autrui et que « la décision des juridictions internes de tenir la société requérante pour responsable reposait sur des motifs pertinents et suffisants, eu égard à la marge d'appréciation dont bénéficie l'État défendeur » et que « la mesure litigieuse ne constituait pas une restriction disproportionnée du droit de la société requérante à la liberté d'expression »[1467]. La Cour a donc estimé qu'un portail d'actualités peut être tenu pour responsable de contenus produits par des tiers à l'égard de victimes et que sa condamnation d'un portail n'avait pas violé son droit à la liberté d'expression. Deux juges ont critiqué cette position en estimant un risque de « censure collatérale » de la part des « intermédiaires Internet actifs » par la surveillance systématique de ces contenus, voire la suppression pure et simple de la possibilité de laisser des commentaires[1468]. La Cour a estimé que le contenu des messages était principalement de haine et appelant directement à la violence[1469]. Deuxièmement, les mesures adoptées par la société requérante afin d'empêcher les commentaires illégaux s'étaient montrés défaillants et avaient permis que les commentaires restent en ligne pendant six semaines [1470] . Troisièmement, la Cour avait relevé que la responsabilité des auteurs des commentaires pouvait difficilement être recherchée faute pour les victimes de pouvoir les identifier vu leur nature anonyme[1471]. À cet égard, elle n'estime pas satisfaisante une mesure permettant un recours pour dommages-intérêts. En effet, pour garantir la protection de la vie privée de manière effective la responsabilité du portail d'actualité doit être engagée puisqu'il obtient un profit économique des messages publiés. Même s'il est difficile pour un portail d'information de filtrer les messages, il s'agit d'une tâche encore plus lourde pour les personnes diffamées. Ainsi, la Cour a conclu à la non violation de l'article 10. La décision des juridictions estoniennes de tenir Delfi AS pour responsable était justifiée et ne constituait pas une restriction disproportionnée de son droit à la liberté d'expression. Par conséquent, pour la première fois, la Cour a reconnu que la responsabilité de l'exploitant, à titre commercial, d'un portail d'actualités sur Internet était engagée en raison des commentaires injurieux laissés par les internautes. Toutefois, les devoirs et responsabilités des journalistes ne vont pas jusqu'à exiger le retrait des archives électroniques de toute trace de publications

---

1466 CEDH, Krone Verlag GmbH & Co. KG c. Autriche (no. 4), réq. no. 72331/01, §32, 9 Novembre 2006.

1467 Voy. § 162 de la décision.

1468 Voy. opinion contraire des juges Sajó et Tsotsoria.

1469 Voy. § 86 de la décision.

1470 Voy. § 87-90 et 156 de la décision.

1471 Voy. § 91-92 de la dècision.

passées qui, par des décisions judiciaires définitives, ont été jugées diffamatoires. Ainsi dans l'affaire *Węgrzynowski and Smolczewski c. Pologne*[1472], la Cour a estimé disproportionné la suppression d'un article sur le site Web d'un journal en ligne, alors que les tribunaux nationaux avaient jugé diffamatoire le texte publié dans la version imprimée. L'affaire portait sur deux journalistes travaillant pour un journal polonais qui avaient été condamnés pour diffamation pour avoir publié des articles dans lesquels ils estimaient que les requérants, les deux avocats, avaient obtenu des avantages suite à leur participation impliquant des hommes politiques. Un an après la décision de la Cour d'appel, qui avait confirmé celle de première instance, les requérants se sont plaints que l'article diffamatoire existait toujours en format électronique sur le site web du journal. Les requérants soulignaient qu'il était extrêmement facile, en utilisant le moteur de recherche Google, d'avoir accès à ces informations diffamatoires. Les avocats avaient demandé aux juges d'ordonner le retrait des articles du site Web du journal, mais les demandes avaient été rejetées puisque, selon les juges, la suppression de l'article du site équivaudrait à la censure et aurait conduit à une réécriture de l'histoire, par opposition aux principes d'archivage. Ainsi, la Cour a rappelé que, conformément à sa jurisprudence, les archives sur Internet rentrent dans le cadre de la protection de l'art. 10 de la CEDH. De plus elle a souligné la contribution importante de ces archives à rendre accessibles facilement et gratuitement des informations, ce qui constitue un outil important pour l'éducation et la recherche. La Cour a estimé que, plutôt que de supprimer des archives sur Internet qui concernaient des informations diffamatoires, il fallait ajouter une note dans l'article sur le site Web pour informer le public au sujet de la décision du tribunal dans lequel avait été constaté le caractère diffamatoire des informations stockées. La CEDH a estimé qu'il n'y avait pas eu violation de l'article 8 CEDU. Cette décision confirme le raisonnement de la CEDH en faveur du maintien des articles au sein des archives Internet même lorsque l'article a été déclaré diffamatoire. La Cour a donc rappelé sa jurisprudence selon laquelle, la liberté d'expression est un élément fondamental d'une société démocratique qui doit être observé surtout à l'égard des sanctions et des mesures restrictives imposées à la presse[1473]. Ainsi, dans son arrêt *Olafsson*[1474], la Cour européenne des droits de l'homme a jugé que la condamnation pour diffamation d'un responsable de publication qui n'a fait que relayer des propos, même si diffamatoires, porte atteinte à son droit à la liberté d'expression. En l'espèce, un responsable de publication islandais a diffusé des propos sur Internet prétendant qu'un candidat aux élections des membres de l'Assemblée constituante avait commis des actes de pédophilie. La Cour suprême islandaise l'a jugé coupable de diffamation. Le responsable de la publication a alors saisi la CourEDH, estimant que cette condamnation portait atteinte à son droit à la liberté d'expression garanti par l'article 10 de la Convention européenne des droits de l'homme. Il est bien de rappeler les critères de la violation du droit à la liberté d'expression : il y a violation du droit à la liberté d'expression lorsque se produit une ingérence dans l'exercice par un individu de son droit à la liberté d'expression et que cette ingérence n'est pas prévue par la loi, ne poursuit pas un but

---

1472 CEDH, Węgrzynowski and Smolczewski c. Pologne, req. n°. 33846/0, 16 Juillet 2013.

1473 Voy. § 57 de la décision.

1474 CEDH, *Olafsson c. Islande,* req. no 58493/13, 13 mars 2013.

légitime, ou n'est pas nécessaire dans une société démocratique. La Cour a jugé que la décision de déclarer M. Ólafsson responsable d'une diffamation n'était pas nécessaire dans une société démocratique, compte tenu des circonstances de l'affaire. Ainsi, selon la CEDH, la Cour suprême islandaise n'a pas ménagé un équilibre raisonnable entre les mesures ayant restreint la liberté d'expression de M. Ólafsson et le but légitime qu'est la protection de la réputation d'autrui. Dans son analyse, la CEDH a notamment vérifié que l'ingérence était prévue par la loi, elle a alors examiné si l'ingérence était « nécessaire dans une société démocratique ». Elle a ainsi recherché s'il avait été procédé à une mise en balance adéquate du droit à la liberté d'expression et du droit au respect de la vie privée. Concernant la nécessité d'un juste équilibre entre droit à la liberté d'expression et droit au respect de la vie privée, la CEDH a d'abord constaté que les allégations portaient sur des questions graves d'intérêt public et que le public avait un intérêt légitime à connaître l'existence des accusations concernant l'homme politique. En outre, l'homme étant candidat à une charge politique, la CEDH a estimé qu'il aurait dû anticiper le contrôle du public et que les limites de la critique admissible devaient être plus larges à son encontre qu'à celle d'un particulier. De plus, elle a constaté que les articles concernés avaient été publiés de bonne foi et dans le respect des normes journalistiques habituelles, notamment grâce aux efforts que le journaliste avait fourni pour vérifier la fiabilité des propos et accorder à l'homme politique la possibilité de répondre aux accusations. Enfin, elle a relevé que les allégations diffamatoires n'avaient pas été formulées par le responsable de la publication mais par deux sœurs ayant un lien familial avec l'homme politique. Pour autant que la condamnation du responsable de publication ait pu répondre à l'intérêt légitime de protéger la réputation de l'homme politique, cet intérêt a été largement protégé par la possibilité qui s'offrait à lui d'intenter une action pour diffamation à l'encontre des deux sœurs. Au regard de ces considérations, la CEDH a jugé que la Cour suprême islandaise n'a pas ménagé un équilibre raisonnable entre les mesures ayant restreint le droit à la liberté d'expression du responsable de la publication et le but légitime qu'est la protection de la réputation d'autrui. Partant, il y a eu violation de l'article 10 de la Convention européenne des droits de l'homme. Dans la jurisprudence de la CourEDH, la prévalence de la liberté d'expression est la règle et les limitations à cette liberté sont les exceptions qui doivent être interprétées de manière restrictive. En étendant le champ d'application de l'article 10, elle renforce ainsi la protection de la liberté d'expression sur Internet. Cependant, la recherche d'équilibre des droits entre protection de la vie privée et liberté d'expression est effectuée au cas par cas, sans une prévalence a priori de cette dernière.

177 La responsabilité des moteurs de recherche. À l'inverse, concernant la liberté d'expression sur Internet, la Cour de justice dans l'affaire *Google Spain*[1475] a fait prévaloir de façon nette le droit à la protection des données personnelles sur le droit d'accès des

1475 CJUE, *Google Spain SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González*, causa C-131/12, 13 mai 2014.

internautes[1476]. La Cour de justice avait déjà considéré dans l'affaire *Bodil Lindqvist* que la diffusion d'informations sur Internet conduit à les mettre à disposition d'un nombre indéfini de personnes, ce qui trouve un fondement dans la liberté d'expression mais doit se concilier avec le droit à la protection des données personnelles[1477]. C'est le droit à l'information, composante du droit à la liberté d'expression protégée par l'article 11 de la Charte des droits fondamentaux, et le droit à la liberté d'expression et la liberté d'entreprendre de Google qui était en jeu. La Cour a tranché elle-même la question de cet équilibre et a jugé que les droits de la personne concernée « prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche mais également sur l'intérêt [du] public » qui souhaiterait trouver des informations relatives à la personne concernée « lors d'une recherche portant sur le nom de cette personne »[1478] . Cette décision a été prise contre les conclusions de l'Avocat général Jääskinen qui avait préconisé la solution inverse [1479] . Cependant, l'exercice d'équilibriste effectué par la Cour se cantonne à l'affaire en cause et on ne pourrait en déduire qu'une solution identique trouverait à s'appliquer chaque fois qu'un internaute fait usage de son « droit à l'oubli ». Elle rappelle « que cet équilibre peut toutefois dépendre, dans des cas particuliers, de la nature de l'information en question et de sa sensibilité pour la vie privée de la personne concernée ainsi que de l'intérêt du public à disposer de cette information, lequel peut varier, notamment en fonction du rôle joué par cette personne dans la vie publique »[1480].
En ce sens, la Cour avait également jugé en 2006 « qu'il appartient aux autorités et aux juridictions nationales chargées d'appliquer la réglementation nationale transposant la directive 95/46 d'assurer un juste équilibre des droits et intérêts en cause, y compris les droits fondamentaux protégés par l'ordre juridique communautaire »[1481], cet équilibre devant être

1476 Voy. §81 de la décision *Google Spain*. Ce raisonnement se heurte à la position de la CEDH, qui considère que les droits contenus dans les arts. 8 et 10 de la CEDH méritent, comme règle générale, le mê me respect (affaire von Hannover c. Allemagne, § 106, préc).

1477 CJCE, Bodil Lindqvist, aff. C-101/01, Rec. I-12971, 6 novembre 2003, § 46-47.

1478 CJUE., *Google Spain* SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, C-131/12, 13 mai 2014, §97.

1479 Celui-ci s'était exprimé en ces termes : « Je dissuaderais également la Cour de conclure que ces intérêts concurrents pourraient être mis en balance de façon satisfaisante dans les situations individuelles, sur la base d'une analyse au cas par cas, en laissant aux fournisseurs de services de moteur de recherche sur Internet le soin de statuer. De telles «procédures de notification et de retrait», si elles étaient exigées par la Cour, conduiraient vraisemblablement soit au retrait automatique de liens vers tout contenu faisant l'objet d'une opposition, soit à un nombre ingérable de demandes traitées par les fournisseurs de services de moteur de recherche sur Internet les plus populaires et importants. » Voy. point 133 des conclusions de l'Avocat général sous l'arrêt *Google Spain*.

1480 CJCE, *Bodil Lindqvist*, C-101/01, 6 novembre 2003 § 90.

1481 CJCE, *Bodil Lindqvist*, C-101/01, 6 novembre 2003, § 88.

proportionné[1482] et devant tenir compte des circonstances de l'espèce[1483]. A cet égard, le fait que le responsable de traitement soit un moteur de recherche, lequel permet aisément de rassembler un grand nombre d'informations relatives à la personne concernée « et peut jouer un rôle décisif pour la diffusion desdites informations »[1484], constitue, d'après la Cour, un élément essentiel lors de la mise en balance des intérêts (au contraire des sites *Web qui* n'offrent bien souvent que des informations éparses). Si d'un côté, Internet est un excellent outil pour la recherche de l'information et du savoir, les données personnelles peuvent être divulguées par soi-même ou par des tiers, ce qui peut porter atteinte aux droits de la personne. Dans l'affaire *Google Spain*, la Cour de justice a consacré l'existence d'un droit à l'oubli numérique.

Ainsi, elle a jugé que Google, dans sa fonction de moteur de recherche, est bien un responsable de traitement au sens de la directive 95/46/CE relative à la protection des données à caractère personnel. Elle en tire la conclusion qu'il est, à ce titre, tenu de faire droit aux demandes de désindexation qui lui sont adressées, sauf quand la demande concerne une information d'intérêt public. Elle a anticipé certains principes du nouveau règlement notamment l'article 17 concernant le droit à l'oubli[1485]. Toutefois, les juges, dans la mise en balance entre droit d'accès à l'information et droit à la protection des données personnelles, ont opéré sur la base d'un renvoi préjudiciel sur l'interprétation des articles 12 et 14 de la directive 95/46/CE ayant comme objet le droit d'accès aux données et le droit d'opposition au traitement[1486].

1482 Afin de palier en partie aux difficultés liées à la mise en œuvre des différents éléments soulignés par la Cour, le G29 a publié des lignes directrices établissant une liste de treize critères à prendre en compte lors du traitement des plaintes. Voy. Groupe de travail « Article 29 » sur la protection des données, « Guidelines on the implémentation of the Court of Justice of the European Union judgement on *Google Spain* and Inc. v. Agencia española de protección de datos (AEPD) and Mario Costeja González C-131/12 », 26 novembre 2014, 14/EN WP : 1. Les résultats de recherche sont-ils liés au nom ou au pseudonyme d'une personne physique permettant facilement de l'identifier ? 2. La personne concernée joue-t-elle un rôle dans la vie publique ? S'agit-il d'une figure publique ? 3. La personne concernée est-elle mineure ? 4. Les données sont-elles erronées ? 5. Les données sont-elles pertinentes et non-excessives247 ? Sont-elles liées à la profession de la personne concernée ? Les résultats de la recherche mènent-ils à des informations pouvant être interprétées comme des discours de haine, à de la calomnie ou de la diffamation ou tout autre préjudice du même type à l'encontre de la personne concernée ? 6. L'information est-elle « sensible » au sens de l'article 8 de la directive 95/46/CE248 ? 7. Les données sont-elles à jour ? Ont-elles été disponibles pour une période supérieure à celle nécessaire à la réalisation des objectifs pour lesquels elles ont été traitées ? 8. Le traitement de ces données a-t-il causé un préjudice à la personne concernée ? Et si oui, est-il disproportionné ? 9. Les données mènent-elles vers des informations susceptibles de placer la personne concernée en danger ? 10. Dans quel contexte l'information a-t-elle été publiée ? Le contenu a-t-il été volontairement rendu public ? La personne concernée pouvait-elle raisonnablement s'attendre à ce que le contenu soit rendu public ? 11. Le contenu original de ces données a-t-il été publié à des fins journalistiques ? 12. L'éditeur des données a-t-il un droit ou une obligation légale de rendre ces données publiques ? 13. Les données sont-elles liées à une infraction pénale ?

1483 CJUE., 13 mai 2014 *Google Spain* SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, C-131/12, §87.

1484 CJUE., 13 mai 2014, *Google Spain* SL et Google Inc. c. Agencia Española de Protección de Datos et Mario Costeja González, C-131/12, §87.

1485 Le Règlement consacre dans son art. 17, la première réglementation formelle du droit à l'oubli au niveau européen et signale, comme exception, l'exercice du droit à la liberté d'expression (art. 17.3/a). Cependant, aucun critère pour faciliter la conciliation n'est énoncé de manière expresse. Voy. F.PIZZETTI, « Il prisma del diritto all'oblio », in AA.VV., Il caso del diritto all'oblio, F.Pizzetti (a cura di), Torino, 2013, p. 21 et s. Voy. en ce sens ICRI Working Paper Series, « Search engines after *Google Spain*: Internet liberty or privacy peril? », B.VAN ALSENOY, A.KUCZERAWY, J.AUSLOOS (ed.), no. 15, Interdisciplinary Center for Law and ICT, K.U. Leuven, 2013, p. 43.

1486 Article 7 : Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que si: a) la personne concernée a indubitablement donné son consentement ; ou b) il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ; ou c) il est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ; ou d) il est nécessaire à la sauvegarde de l'intérêt vital de la personne concernée ; ou e) il est nécessaire à l'exécution d'une mission d'intérêt public ou

Ainsi en cas d'opposition justifiée, le traitement mis en œuvre par le responsable du traitement ne peut plus porter sur ces données. Or, selon la Cour, les droits de la personne concernée, lus en lumière des articles 7 et 8 de la Charte, prévalent, en principe, non seulement sur l'intérêt économique de l'exploitant du moteur de recherche, mais également sur l'intérêt de ce public à trouver ladite information lors d'une recherche portant sur le nom de cette personne. Cependant, tel ne serait pas le cas s'il apparaissait, pour des raisons particulières, telles que le rôle joué par ladite personne dans la vie publique, que l'ingérence dans ses droits fondamentaux était justifiée par l'intérêt prépondérant dudit public à avoir, du fait de cette inclusion, accès à l'information en question[1487]. La Cour de justice aurait pu suivre les conclusions de l'Avocat général et conserver le *statu quo*[1488]. Ainsi, l'Avocat général, en rappelant l'avis du G29[1489], estimait qu'aucun droit généralisé à l'oubli ne saurait être invoqué sur la base de la directive. Cependant, les juges ont établi le droit de la personne concernée à s'opposer à l'indexation de ses données personnelles par un moteur de recherche lorsque la diffusion de ces données par l'intermédiaire de celui-ci lui porte préjudice et que ses droits fondamentaux à la protection desdites données et au respect de la vie privée, lesquels englobent le « droit à l'oubli », prévalent sur les intérêts légitimes de l'exploitant dudit moteur et l'intérêt général à la liberté d'information. Les juges, à juste titre, n'ont pas confondu le droit à l'effacement avec le droit à l'oubli : les informations permanent sur le site web mais elles sont inaccessibles car le moteur de recherche a l'obligation d'opérer le déréférencement des mots-clés. Ainsi, le droit à l'oubli n'est pas applicable face aux éditeurs de sites web en raison de leur liberté d'expression[1490]. La Cour invoque une triple justification à cette différence de traitement. D'une part, elle est due à l'importance actuelle de l'utilisation d'un moteur de recherche pour accéder à une information[1491]. D'autre part, elle permet de couvrir le cas où l'éditeur n'est pas connu ou est difficilement accessible parce qu'en dehors de l'Union européenne[1492] . Enfin, cela permet également de couvrir des hypothèses où l'information originelle ne peut pas véritablement faire

relevant de l'exercice de l'autorité publique, dont est investi le responsable du traitement ou le tiers auquel les données sont communiquées ;ou f) il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe.

1487 Pour une analyse du droit à l'oubli, voy. C. De TERWAGNE, *Droit à l'oubli, droit à l'effacement ou droit au déréférencement? Quand le législateur et le juge européens dessinent les contours du droit à l'oubli numérique, en Enjeux européens et mondiaux de la protection des données personnelles* (Dir. Alain Grosjean), Larcier, 2015, p. 245-275.

1488 Voy. les conclusions de l'Avocat Général Jääskinen, 25 Juin 2013, C 131/12 *Google Spain* SI, Google Inc. c. Agencia Española de Proteccion de Datos (AEPD) §134 : Plus particulièrement, les fournisseurs de services de moteur de recherche sur Internet ne devraient pas se voy. accablés d'une telle obligation. Celle-ci serait constitutive d'une ingérence dans la liberté d'expression de l'éditeur de la page web, qui ne jouirait pas, dans une telle situation, d'une protection juridique adéquate, puisque toute « procédure de notification et de retrait » non réglementée constituerait une affaire privée entre la personne concernée et le fournisseur de services de moteur de recherche. Cela reviendrait à ce qu'un particulier censure son contenu publié. C'est une chose totalement différente que les États aient des obligations positives de fournir un recours effectif à l'encontre de l'éditeur portant atteinte au droit à la vie privée, qui, dans le cadre de l'Internet, concernerait l'éditeur de la page web.

1489 Voy. l'Avis du Groupe de travail «Article 29», avis 1/2008, p. 14 et 15.

1490 Voy. §85 de l'arrêt.*Google Spain*.

1491 Voy. §80 de l'arrêt.

1492 Voy. § 83 de l'arrêt.

l'objet d'une désindexation parce qu'il s'agit d'une obligation légale[1493]. La Cour a conclu que « la personne concernée est dans certaines circonstances susceptible d'exercer les droits visés aux articles 12, sous b), et 14, premier alinéa, sous a) de la directive 95/46 contre l'exploitant du moteur de recherche, mais pas contre l'éditeur de ladite page web »[1494]. Autrement dit, la Cour exclut que le moteur de recherche puisse faire usage de la directive 95/46 et de dérogations aux exigences établies par celle-ci et pour ce faire elle cite l'arrêt *Satamedia*. Toutefois, elle « oublie » de mentionner le passage de l'arrêt dans lequel la Cour avait clairement indiqué que la référence à des fins journalistiques doit être comprise dans le sens le plus large possible, de telle sorte à inclure des « activités directes à la diffusion de l'information sous quelque moyen de transmission que ce soit »[1495] . La complexité de la question peut se résumer dans la reconnaissance de la prévalence des droits fondamentaux face aux droits économiques des entreprises[1496]. Ainsi, dans cette affaire, la règle est la primauté du droit au respect de la vie privée et à la protection des données personnelles sur le droit à l'information des internautes. Toutefois, cette règle /exception non seulement n'existe pas dans les conclusions de l'Avocat général Jääskinen, mais elle avait déjà été exclue par l'Avocat général Kokott[1497] dans l'affaire *Satamedia*. De plus, elle semble en contraste avec la solution adoptée par la CourEDH dans l'affaire *Węgrzynowski e Smolczewski*[1498] dans laquelle la CourEDH réaffirme son paramètre de la prévalence de la liberté d'expression comme règle et des restrictions à cette liberté comme des exceptions qui doivent être interprétées de manière restrictive. Et même dans les cas où le conflit entre l'accès à l'information sur le Web et l'intérêt du demandeur à ne pas voir publié des informations est préjudiciable à sa réputation. Il faut souligner que la CJ ne se réfère pas à la jurisprudence de la CEDH ce qui montre sa tendance à revendiquer son autonomie. Le risque est celui d'un désaccord d'interprétation avec la Cour européenne des droits de l'homme puisque la Cour de justice affirme qu'en règle générale le droit à la protection des données personnelles prévaut sur l'intérêt d'accès aux informations des internautes et que le traitement des données personnelles par le moteur de recherche est une ingérence plus importante que la publication par l 'éditeur de la page web (§87). Elle dit indirectement que le moteur de recherche ne bénéficie pas de la dérogation inscrite à l'art. 9 de la directive 95/46 concernant les traitements effectués aux seules fins de journalisme. Au contraire, la CourEDH reconnaît une interprétation large de la liberté d'expression de la presse et en ligne et elle pourrait reconnaître que les moteurs de recherche disposent d'un droit à la liberté d'expression comme les éditeurs d'une page web. Toutefois, la CourEDH n'a pas encore eu l'occasion de statuer sur

---

1493 Voy. §84.

1494 Voy. § 85 de la décision.

1495 CJCE, Tietosuojavaltuutettu c. Satakunnan Markkinapö rssi Oy et Satamedia Oy,, C-73/07, préc. §60-61.

1496 G. FINOCCHIARO, « Il diritto all'oblio nel quadro dei diritti della personalità », in *Dir. Inf*, 2014, p. 591 ets.

1497 Voy. les conclusions de l'Avocat général Kokott, 8 mai 2008, concernant l'affaire Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, C-73/07, point 43 : « Une application stricte de la protection des données pourrait sensiblement restreindre la liberté d'expression. Ainsi, le journalisme d'investigation serait largement exclu, si les médias ne pouvaient traiter et publier les informations à caractère personnel qu'après accord ou information des intéressés. D'autre part, il est évident que les médias peuvent blesser la vie privée de l'individu. Il convient par conséquent de trouver un équilibre ». L'Avocat général cite ainsi l'arrêt de la CEDH von Hannover, précité (§ 61 et suiv.)

1498 CEDH, Węgrzynowski et Smolczewski c. Pologne, req. n. 33846/07, 16 juillet 2013.

la question du droit à l'oubli[1499] sur Internet comme l'a fait la Cour de Luxembourg dans l'arrêt *Google Spain*. Une affaire concernant le droit à l'oubli sur Internet est cependant pendante devant la Cour de Strasbourg[1500] et concerne des personnes condamnées ayant purgé leurs peines ; celles-ci se plaignent du refus d'anonymisation des données personnelles figurant dans des reportages sur leur procès pénal accessibles sur des pages d'archives en ligne. Toutefois, une première décision a été rendue dans l'affaire *Brunet c. France*[1501] : ainsi, la CourEDH a estimé que l'État a outrepassé sa marge d'appréciation en ne respectant pas le juste équilibre entre les intérêts publics et privés. La conservation des données du requérant au fichier STIC pendant 20 ans constitue donc une violation de l'article 8, puisqu'il s'agit d'une ingérence qui n'est pas nécessaire dans une société démocratique. La Cour a en quelque sorte affirmé, d'une manière indirecte, le droit pour tout citoyen de maîtriser son identité numérique afin d'établir le droit à l'oubli dans une époque où la conservation perpétuelle des informations personnelles de chaque individu est disponible sur le Web. Ainsi le nouveau Règlement 679/2016/CE, offre, dans son article 17, la première réglementation formelle du droit à l'oubli au niveau européen et signale, comme exception, l'exercice du droit à la liberté d'expression (art. 17.3/a). Cependant, aucun critère pour faciliter la conciliation n'est énoncé de manière expresse. Les innovations introduites par Internet bénéficiant aux consommateurs, aux entreprises et à la société en général ont donné lieu à une situation dans laquelle un équilibre doit être trouvé entre plusieurs droits fondamentaux, tels que la liberté d'expression et la liberté d'entreprise, d'une part, et la protection des données à caractère personnel et de la vie privée des individus, d'autre part. Ainsi, d'autres droits pouvant entrer en conflit avec le droit à la protection des données personnelles, la CEDH consacre dans son article 17.2 une attention particulière à la propriété intellectuelle. Également, le droit dérivé de l'UE dispose de toute une série d'instruments normatifs afin de protéger le droit à la propriété intellectuelle.

§2. La pondération avec le droit à la propriété intellectuelle

178 Des restrictions relevant du droit de propriété. D'autres droits fondamentaux peuvent limiter le droit à la protection des données personnelles dès lors que ces restrictions apparaissent

---

1499 S'agissant de l'obligation imposant au responsable du traitement d'effacer les informations dès qu'elles ne sont plus nécessaires au traitement.

1500 M.L. contre l'Allemagne et W.W. contre l'Allemagne, n° 60798/10 et n° 65599/10, communiquées au gouvernement défendeur sous l'angle de l'article 8 de la Convention le 29 novembre 2012.

1501 CEDH, *Brunet c. France*, req. n°21010/10, 18 septembre 2014. La Cour estime que le délai de conservation des données du requérant au fichier STIC pendant 20 ans en l'absence de déclaration judiciaire de culpabilité est très certainement excessif et disproportionné en raison de l'absence de possibilité effective de ce dernier d'en demander l'effacement anticipé. La CEDH estime donc que le régime de conservation des fiches dans le STIC, tel qu'il a été appliqué au requérant, ne traduit pas un juste équilibre entre les intérêts publics et privés concurrents en jeu et constitue une atteinte disproportionnée au droit du requérant au respect de sa vie privée et une violation de l'article 8 de la CESDH.

comme un moyen de garantir leur respect. Tel est le cas du droit de propriété[1502] qui peut constituer une limite au droit à la protection des données personnelles. Le droit de propriété est consacré par l'art. 1 du Protocole Additionnel n° 1 à la CEDH (« le Protocole ») et par l'art. 17 de la Charte des droits fondamentaux et fait partie intégrante des principes généraux du droit de l'UE [1503] . Ainsi dans le droit secondaire, l'art. 7/f de la Directive 95/46 [1504] prévoit le traitement licite des données dans le cas d'un intérêt légitime du responsable du traitement. Ainsi le responsable du traitement pourrait limiter le droit à la protection des données personnelles afin d'exercer son droit de propriété. Il peut s'agir d'un conflit « indirect » car il « est médiatisé par l'intervention des pouvoirs publics, adoptant une mesure restrictive d'un droit individuel afin de protéger un autre droit individuel »[1505].Toutefois, la jurisprudence en matière de pondération entre droit de propriété et droit à la protection des données personnelles est encore peu nombreuse. Il est néanmoins possible d'en tirer des conclusions. Au-delà de la propriété corporelle (A), tant le Protocole 1 de la CEDH que l'art. 17.2 de la Charte confèrent une attention particulière à la propriété intellectuelle. Ce droit peut également restreindre le droit à la protection des données personnelles (B)[1506].

A. Le droit à la protection des données personnelles face au droit de propriété

179 La protection de biens patrimoniaux. Les affaires concernant le conflit entre droit de propriété et droit à la protection des données personnelles portent sur la surveillance vidéo afin de protéger des biens patrimoniaux. Dans l'affaire *Ryneš* [1507], la Cour de justice a considéré que le traitement de données relatives à des tiers (dans le cas d'espèce, l'enregistrement d'images à travers un système de surveillance vidéo) était justifié lorsque la finalité du traitement consiste à protéger les biens du responsable. Ainsi elle rappelle que les articles 7, f), 11, paragraphe 2, ainsi que 13, paragraphe 1, d) et g) de la directive 46/95 posent des dérogations au droit à la protection des données personnelles lorsque les intérêts légitimes du responsable du traitement consistent à protéger les biens, la santé et la vie de ce responsable ainsi que ceux de sa famille.

1502 Le droit à la protection de la propriété est consacré à l'article 1 du premier protocole à la CEDH et à l'article 7 §1 de la Charte des droits fondamentaux.

1503 Voy. CJUE, *Hauer c. Rheinland-Pfalz*, C-44/79, 13 décembre 1979, § 13-16.

1504 Les États membres prévoient que le traitement de données à caractère personnel ne peut être effectué que s'il est nécessaire à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement ou par le ou les tiers auxquels les données sont communiquées, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentales de la personne concernée, qui appellent une protection au titre de l'article 1er paragraphe 1.

1505 Voy. sur ce constat F. SUDRE, « Les conflits de droits. Cadre général d'approche dans la jurisprudence de la Cour européenne des droits de l'homme », préc., spéc p. 241.

1506 Le rôle des moteurs de recherche sur Internet dans le cadre des droits de propriété intellectuelle et de la compétence juridictionnelle a également été examiné par la Cour dans ses arrêts Google France et Google, Portakabin, L'Oréal e.a., Interflora et Interflora British Unit, et Wintersteiger.

1507 CEDH, a Františ ek Ryneš c. Ú ř ad pro ochranu osobních údajů , C-212/13, § 34.

Toutefois, dans ses conclusions, l'avocat général [1508] estimait que l'activité exercée par M. Ryneš visait à protéger sa jouissance d'autres droits fondamentaux, tels que le droit de propriété et le droit à la vie familiale, et proposait à la CJ d'interpréter telles activités comme ne relevant pas du traitement des données aux seuls finalités domestiques au titre de l'article 3, paragraphe 2 de la Directive 46/95 puisque la vidéosurveillance s'étendait à l'espace public. Ainsi, la Cour a suivi le raisonnement de l'Avocat général et a conclu que l'article 3, paragraphe 2, second tiret, de la directive 95/46/CE devait être interprété en ce sens que l'exploitation d'un système de caméra, donnant lieu à un enregistrement vidéo des personnes stocké dans un dispositif d'enregistrement continu tel qu'un disque dur, installé par une personne physique sur sa maison familiale afin de protéger les biens, la santé et la vie des propriétaires de la maison, ce système surveillant également l'espace public, ne constituait pas un traitement des données effectué pour l'exercice d'activités exclusivement personnelles ou domestiques, au sens de cette disposition. La décision d'irrecevabilité pour défaut manifeste de fondement dans l'affaire *Kopke c. Allemagne* [1509] concernait une requérante qui travaillait comme caissière dans un supermarché. Elle avait été licenciée sans préavis pour vol, à la suite d'une mesure de surveillance vidéo secrète mise en œuvre par son employeur avec l'aide d'une agence de détectives privés. Elle avait contesté en vain son licenciement devant les juridictions du travail. De même, son recours constitutionnel avait été rejeté. La Cour a dû vérifier si l'État, eu égard à ses obligations positives découlant de l'article 8, avait ménagé un juste équilibre entre, d'une part, le droit de la requérante au respect de sa vie privée et, d'autre part, l'intérêt de son employeur à la protection de ses droits patrimoniaux en vertu de l'article 1 du Protocole n° 1, et l'intérêt général lié à une bonne administration de la justice. Comme l'ont relevé les tribunaux allemands, la surveillance vidéo de la requérante n'a été effectuée qu'après découverte de pertes à l'occasion de l'inventaire et d'irrégularités dans les comptes du service pour lequel l'intéressée travaillait, ce qui avait fait naître des soupçons défendables de vols commis par elle et l'un de ses collègues, les seuls employés visés par la mesure de surveillance. Cette mesure a été limitée dans le temps (deux semaines) et n'a concerné que la zone accessible au public et entourant la caisse. De plus, les éléments vidéo obtenus ont été traités par un nombre limité de personnes travaillant pour l'agence de détectives et par des collègues de l'intéressée. L'ingérence dans la vie privée de la requérante s'est donc bornée à ce qui était nécessaire pour atteindre les buts poursuivis par la surveillance vidéo. Les tribunaux nationaux ont par ailleurs considéré que l'intérêt de l'employeur à la protection de ses droits patrimoniaux ne pouvait être sauvegardé de manière effective que par la recherche de preuves tendant à démontrer devant le tribunal que la requérante avait eu une conduite répréhensible. Cela a également servi l'intérêt général lié à une bonne administration de la justice. Cependant, la Cour souligne que l'équilibre ménagé par les autorités nationales entre les intérêts en cause ne semble pas constituer la seule manière pour elles de satisfaire à leurs obligations en vertu de la Convention. En effet, les intérêts concurrents en jeu pourraient se voir accorder un poids différent à l'avenir, compte tenu de la mesure dans laquelle les intrusions dans la vie privée ont été rendues possibles par des technologies nouvelles et plus sophistiquées. Bien que le but

1508 Voy. les conclusions de l'Avocat général M. NIILO JÄÄSKINEN présentées le 10 juillet 2014 Affaire C-212/13 František Ryneš contreÚřad pro ochranu osobních údajů.

1509 CEDH, Kopke c. Allemagne, req. n. 420/07, 5 October 2010.

principal de l'art. 8 porte sur la protection de l'individu contre l'ingérence arbitraire des autorités publiques, il n'impose pas simplement à l'État de s'abstenir d'une telle ingérence, mais prévoit des obligations positives concernant le respect effectif de la vie privée. À cet égard, la limite entre les obligations positives et négatives de l'État ne permet pas une définition précise. En tout cas, il faut assurer un juste équilibre entre les intérêts en jeu qui peuvent inclure des intérêts ou des droits concurrents privés et publics prévus par la CEDH[1510]. Enfin, la Cour rappelle qu'il existe diverses façons d'assurer le respect de la vie privée et que la nature des obligations de l'État dépend de l'aspect particulier de la vie privée concernée. Le choix des moyens d'assurer la conformité conventionnelle dans le domaine de la protection contre les actes des individus est, en principe, dans la marge d'appréciation de l'État[1511]. En conclusion, rien n'indique que les autorités nationales aient manqué à ménager un juste équilibre, dans le cadre de leur marge d'appréciation, entre, d'une part, le droit de la requérante au respect de sa vie privée et, de l'autre, l'intérêt de son employeur à la protection de ses droits patrimoniaux et l'intérêt général lié à la bonne administration de la justice. Malgré l'absence d'une jurisprudence consolidée, cette affaire laisse la porte ouverte à un futur examen approfondi de la part de la Cour de justice.

1510 CEDH, Evans c. Royaume-Uni, Gr.Ch., réq. no. 6339/05, §§ 75 et 77, v. aussi, Von Hannover c. Germany, réqno. 59320/00, § 57 et Reklos et Davourlis c. Greece, no. 1234/05, § 36, 15 January 2009.

1511 CEDH, X and Y c. Ollande, 26 Mars 1985, § 24; M.C. c. Bulgarie, req. no. 39272/98, § 150; K.U. c. Finlande, req. no. 2872/02, § 43, ECHR 2008.

B. Le droit à la protection des données personnelles face à la propriété intellectuelle

180 La protection de la propriété artistique. Le droit à la propriété intellectuelle est rattaché au droit de propriété[1512]. Il est explicitement mentionné à l'article 17§2 de la Charte[1513]. Le droit d'auteur, composante de la propriété intellectuelle, est encadré dans le droit secondaire par plusieurs directives[1514]. La CEDH et la CJ, dans leur jurisprudence, ont souligné que la protection fondamentale à la propriété doit être mise en balance avec la protection d'autres droits fondamentaux, en particulier avec le droit à la protection des données personnelles[1515]. L'évolution constante des nouvelles technologies entraîne de nouvelles menaces pour la propriété intellectuelle[1516]. La propriété intellectuelle à son tour peut restreindre et entrer en conflit avec le droit à la protection des données personnelles[1517]. De telles restrictions ont été mises en place pour faire face au téléchargement illégal sur Internet et ont donné lieu à plusieurs contentieux dans les jurisprudences européennes. En effet, Internet facilite la violation de la propriété intellectuelle (films, ouvrages, musique partagés). Ceci est un inconvénient pour les titulaires des droits d'auteurs mais un avantage pour les utilisateurs. Face au téléchargement illégal sur Internet d'enregistrements musicaux et audiovisuels, les sociétés et organismes de protection des droits d'auteur ont cherché à collecter les données de connexion et ont réclamé des fournisseurs d'accès à Internet qu'ils divulguent l'identité des utilisateurs de plateformes de partage de fichiers en ligne afin d'intenter des actions contre ceux-ci. Les réseaux P2P (*peer-to-peer*) permettent le partage de fichiers entre ordinateurs entraînant une menace importante pour la violation de la propriété intellectuelle. Ainsi, afin de combattre ces pratiques illégales, l'identification des contrefacteurs devient indispensable. Cependant, l'acquisition des données des potentiels contrefacteurs s'oppose à l'obligation de confidentialité pesant sur les tiers qui les conservent (les fournisseurs d'accès Internet) puisqu'elle requiert la communication de

---

1512 La Convention du 14 juillet 1967 créant l'Organisation mondiale de la propriété intellectuelle énonce les droits protégés par cette notion : les œuvres littéraires, artistiques, les interprétations, les inventions, découvertes scientifiques, les dessins et modèles, les marques de fabrique, de commerce, de service, etc. Se trouvent ainsi protégées non seulement les idées, mais également la forme d'expression de l'idée elle-même. L'auteur d'une œuvre de l'esprit dispose : d'une part, d'un droit moral qui lui permet de jouir du droit de divulgation du bien ; un tiers doit obtenir une autorisation de sa part pour l'utiliser, le reproduire, etc. ; d'autre part, d'un droit patrimonial qui lui permet d'exploiter son œuvre (lors d'une interprétation, d'une reproduction, etc.).

1513 Plusieurs directives ont encadré la matière : Directive 2000/31, 2001/29, 2004/48.

1514 Directive 2001/29/CE du Parlement européen et du Conseil du 22 mai 2001, sur l'harmonisation de certains aspects du droit d'auteur et des droits voisins dans la société de l'information et la Directive 2004/48/CE du Parlement européen et du Conseil du 29 avril 2004, relative au respect des droits de propriété intellectuelle.

1515 CEDH, *Ashby Donald et autres c. France*, n°36769/08, 10 janvier 2013.

1516 Parmi les menaces pour la propriété intellectuelle, les réseaux P2P (peer-to-peer) qui permettent le partage de fichiers entre ordinateurs sont potentiellement responsables de la circulation illicite de contenus protégés par un droit de propriété intellectuelle.

1517 Voy. sur la relation entre droits fondamentaux et propriété intellectuelle, voy. L. R. HELFER, « Human Rights and Intellectual Property: Conflict or Coexistence », *Minnesota Intellectual Property Review*, 2003, vol. 5, n° 1, pp. 47-61.

données personnelles de la part des fournisseurs d'accès à Internet. La Cour de justice a été confrontée pour la première fois à un tel conflit des droits dans l'affaire *Promusicae c. Telefonica de España* [1518] . Dans le cas d'espèce, le fournisseur d'accès Internet espagnol, Telefonica, refusait de communiquer à Promusicae (une organisation à but non lucratif de producteurs et éditeurs d'enregistrement musicaux et audiovisuels) les données à caractère personnel (adresses IP) concernant certaines personnes auxquelles il avait fourni des services d'accès à Internet. En effet, de telles plateformes permettaient à des internautes de télécharger gratuitement des titres musicaux, alors que ces titres étaient protégés par le droit d'auteur détenu par Promusicae. La juridiction espagnole, en renvoyant l'affaire devant la CJ, demandait si en vertu du droit communautaire sur le droit d'auteur[1519] , les données des utilisateurs de la plateforme devaient être communiquées dans le contexte de poursuites de procédure civile destinées à assurer la protection effective du droit d'auteur. La CJ a estimé que les trois directives concernant le droit d'auteur ainsi que la directive 2002/58 sur la vie privée et les communications électroniques n'empêchaient pas les États membres de prévoir une législation qui poserait l'obligation de communiquer de telles données dans le cadre d'une procédure civile en vue d'assurer la protection effective du droit d'auteur[1520]. Toutefois, l'art. 5.1 de la Directive 2002/58/CE, relative à la protection des données dans le secteur des communications électroniques, impose la confidentialité des données qu'ils détiennent. Les États membres peuvent formuler des exceptions (art. 15.1 de la Directive 2002/58/CE) lorsqu'elles sont nécessaires pour sauvegarder certains intérêts, parmi lesquels ne figure pas la protection civile de la propriété intellectuelle. En effet l'art. 15. 1 de la directive 2002/58/CE prévoit la possibilité de limiter la confidentialité des données seulement afin de sauvegarder la sécurité nationale, la défense et la sécurité publique ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou des utilisations non autorisées de systèmes de communications électroniques comme le prévoit l'art. 13.1 de la Directive 95/46/CE. Malgré tout, la Cour de justice conclut qu'il revient aux États membres, lors de la transposition de la directive, de veiller au juste équilibre entre les différents droits fondamentaux protégés par l'ordre juridique communautaire. Les États membres doivent interpréter leur droit national d'une manière conforme auxdites directives en assurant le juste équilibre entre lesdits droits fondamentaux et les autres principes généraux du droit communautaire[1521], tels que le principe de proportionnalité[1522]. Ainsi la Cour de justice a évité de répondre de manière expresse sur l'obligation de la communication de données personnelles pour assurer la protection de la

1518 CJCE, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, 29 janvier 2008 C-275/06, §54 et 60.

1519 Voy. les dispositions des directives 2000/31, 2001/29, 2004/48.

1520 CJCE, aff. C-275/06, Productores de Música de España c. Telefónica de España SAU, §§ 53 et 54. Selon l'art. 15.1 de la Directive 2002/58/CE, la confidentialité des données peut être limitée afin de sauvegarder la sécurité nationale, la défense et la sécurité publique ou pour assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou l'utilisation non autorisée de systèmes de communications électroniques comme le prévoit l'art. 13.1 de la Directive 95/46/CE.
1521 Sur ce point voy. aussi CJUE, C-360/10, SABAM c. Netlog N.V.,16 février 2012.

1522 CJCE, G. Ch., *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, aff. C-275/06, 29 janvier 2008, § 65 et 68.

propriété intellectuelle[1523]. Dans l'affaire *Bonnier Audio*[1524], la CJUE a exercé un contrôle de légalité sur une disposition qui permettait la communication de l'identité d'une personne soupçonnée de contrefaçon. Selon la CJUE, la disposition garantissait un juste équilibre entre le droit à la protection des données et le droit de propriété intellectuelle. Elle a jugé que les conditions imposées par la disposition en question (présence d'indices réels de contrefaçon, le fait que l'information demandée soit susceptible de faciliter l'enquête et que les raisons motivant l'ingérence soient d'un intérêt supérieur aux inconvénients occasionnés à son destinataire) respectaient les exigences résultant du principe de proportionnalité et parvenaient à un juste équilibre entre les intérêts opposés. À l'inverse, dans les deux affaires *Sabam*[1525], la Cour de justice a abordé le problème du piratage informatique, qui consiste à violer le droit d'auteur sur Internet par le biais du téléchargement illégal de fichiers et d'œuvres protégées. Elle a considéré qu'une injonction obligeant un fournisseur d'accès à Internet à une supervision illimitée de la totalité des communications électroniques afin de prévenir des infractions à la propriété intellectuelle ne garantissait pas l'équilibre entre le droit de propriété intellectuelle et la protection des données personnelles, en plus d'être contraire à l'art. 15.1 de la Directive 2000/31/CE sur le commerce électronique. Dans la première affaire elle devait établir si la mise en place d'un système de filtrage des communications électroniques afin d'empêcher l'échange des fichiers portant atteinte aux droits d'auteur était contraire aux droits de l'UE[1526]. La Société belge des auteurs compositeurs et éditeurs (Sabam) avait, dans le cadre de la loi du 30 juin 1994 relative au droit d'auteur et aux droits voisins, saisi le président du tribunal de première instance de Bruxelles, statuant en référé, d'une demande en cessation dirigée contre Scarlet Extended SA, puisque en sa qualité de fournisseur d'accès Internet Scarlet était idéalement placée pour prendre des mesures en vue de faire cesser les atteintes au droit d'auteur commises par ses clients, les internautes qui téléchargent illégalement des œuvres reprises dans son catalogue au moyen de logiciels « *peer-to-peer* » sans acquitter de droits[1527].

1523 CJCE, C-275/06, Productores de Música de España c. Telefónica de España SAU, §§ 61-70.

1524 CJCE, C-461/10, Bonnier Audio AB et autres c. Perfect Communication Sweden AB, §§ 58-60.

1525 CJUE, Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, 24 novembre 2011. v. aussi, CJ, Netlog NV c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-360/10, 16 février 2012.

1526 La Cour est principalement interrogée sur l'interprétation des directives 2001/29/CE (10) et 2004/48/CE (11), relatives à la protection de la propriété intellectuelle, des directives 95/46/CE (12) et 2002/58/CE (13), relatives à la protection des données personnelles et de la directive 2000/31/CE (14) sur le commerce électronique.

1527 Le président du tribunal de première instance de Bruxelles a, le 29 juin 2007, rendu un second jugement par lequel il a condamné Scarlet à faire cesser les atteintes au droit d'auteur constatées dans le jugement du 26 novembre 2004 en rendant impossible toute forme d'envoi ou de réception par ses clients, au moyen d'un logiciel «peer-to-peer», de fichiers électroniques reprenant une œuvre musicale du répertoire de la Sabam sous peine d'une astreinte de 2 500 € par jour dans l'hypothèse où Scarlet ne respecterait pas le jugement, après l'expiration d'un délai de six mois. Scarlet a interjeté l'appel de ce jugement devant la cour d'appel de Bruxelles le 6 septembre 2007, ainsi la Cour d'appel de Bruxelles a décidé de surseoir à statuer et de poser à la Cour les questions préjudicielles suivantes: les directives 2001/29 et 2004/48, lues en combinaison avec les directives 95/46, 2000/31 et 2002/58, interprétées notamment au regard des articles 8 et 10 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, permettent-elles aux États membres d'autoriser un juge national, saisi dans le cadre d'une procédure au fond et sur la base de la seule disposition légale prévoyant que « [le juge national peut] également rendre une injonction de cessation à l'encontre des intermédiaires dont les services sont utilisés par un tiers pour porter atteinte au droit d'auteur ou à un droit voisin », à ordonner à un Fournisseur d'Accès à l'Internet (en abrégé FAI) de mettre en place, à l'égard de toute sa clientèle, in abstracto et à titre préventif, aux frais exclusifs de ce FAI et sans limitation

Comme l'a relevé l'Avocat général dans ses conclusions[1528], la mesure envisagée par Sabam était sans limitation *ratione temporis* et *rationae personae*. Ainsi, la mesure sollicitée imposait à Scarlet, et plus largement aux FAI en général, une obligation à la fois permanente et perpétuelle de rechercher, de tester, de mettre en place et de mettre à jour un système de filtrage et de blocage concernant l'universalité des communications. De plus, une telle mesure serait caractérisée « *in abstracto*» et « à titre préventif »[1529]. Par ailleurs, la Cour a eu pour la première fois à déterminer si les adresses IP constituent des données personnelles[1530]. Sur ce point, le contrôleur européen de la protection des données avait déjà indiqué que la surveillance des comportements des internautes et la collecte de leur adresse IP équivalaient à une interférence dans leur droit au respect de leur vie privée et de leurs correspondances[1531]. Il en va de même du Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, lequel avait considéré que les adresses IP constituaient sans l'ombre d'un doute des données à caractère personnel au sens de l'article 2, point a), de la directive 95/46[1532]. Dans cette perspective, une adresse IP peut être qualifiée de donnée à caractère personnel dans la mesure où elle peut permettre l'identification d'une personne, par référence à un numéro d'identification ou à tout autre élément qui lui soit propre.

Ainsi, la Cour de justice rappelle sa jurisprudence *Promusicae*[1533] en déclarant que la protection du droit fondamental de propriété, dont font partie les droits liés à la propriété intellectuelle, doit être mise en balance avec celle d'autres droits fondamentaux. Plus précisément, elle estime qu'il incombe aux autorités et aux juridictions nationales, dans le cadre des mesures adoptées pour protéger les titulaires de droits d'auteur, d'assurer un juste équilibre entre la protection de ce droit et celle des droits fondamentaux de personnes qui sont affectées par de telles mesures. Ce qui manque dans l'arrêt *Sabam* est une prise de position sur le rapport entre droit d'auteur

---

dans le temps, un système de filtrage de toutes les communications électroniques, tant entrantes que sortantes, transitant par ses services, notamment par l'emploi de logiciels peer-to-peer, en vue d'identifier sur son réseau la circulation de fichiers électroniques contenant une œuvre musicale, cinématographique ou audio-visuelle sur laquelle le demandeur prétend détenir des droits et ensuite de bloquer le transfert de ceux-ci, soit au niveau de la requête soit à l'occasion de l'envoi?

1528 Voy. les conclusions de l'Avocat général M. PEDRO CRUZ VILLALÓN présentées le 14 avril 2011, Affaire C 70/10, §56-59.

1529 Voy. §63 des conclusions de l'Avocat général.

1530 Auparavant la Cour avait eu à connaître que de cas dans lesquels des données nominatives liées aux adresses IP Arrêt Promusicae, précité point 45.

1531 Voy. l'Avis du Contrôleur européen de la protection des données du 22 février 2010 sur les négociations en cours au sein de l'Union européenne pour un accord commercial anti-contrefaçon (ACAC) (JO 2010, C 147, p. 1, point 24); avis du Contrôleur européen de la protection des données du 10 mai 2010 sur la proposition de directive du Parlement européen et du Conseil relative à l'exploitation et aux abus sexuels concernant des enfants et à la pédopornographie, abrogeant la décision-cadre 2004/68/JAI (JO 2010, C 323, p. 6, point 11).

1532 Voy. l'avis du G29, 4/2007, du 20 juin 2007, sur le concept de données à caractère personnel, WP 136, disponible à l'adresse <http://ec.europa.eu/justice/policies/privacy/>. Voy. également, plus largement, la recommandation n° 3/97, du 3 décembre 1997, L'anonymat sur l'Internet, WP 6, et le document de travail intitulé «Le respect de la vie privée sur Internet – Une approche européenne intégrée sur la protection des données en ligne», adopté le 21 novembre 2000, WP 37, spécialement p. 22.

1533 Voy. l'arrêt du 29 janvier 2008, Promusicae, C 275/06, § 62-68.

et droit à la protection des données personnelles[1534]. La Cour se limite à dire que les mesures prises par la société Sabam étaient disproportionnées. Concernant la liberté d'expression, la Cour déclare uniquement [1535] que ladite injonction risquerait de porter atteinte à la liberté d'information puisque ce système de filtrage risquerait de ne pas distinguer suffisamment entre un contenu illicite et un contenu licite, de sorte que son déploiement pourrait avoir pour effet d'entraîner le blocage de communications à contenu licite [1536] . Dans la deuxième affaire *Sabam*[1537], la Cour arrive à la même conclusion en estimant que l'injonction de mettre en place le système de filtrage litigieux doit être considérée comme ne respectant pas l'exigence d'assurer un juste équilibre entre, d'une part, la protection du droit de propriété intellectuelle dont jouissent les titulaires de droits d'auteur, et, d'autre part, celle de la liberté d'entreprise dont bénéficient les opérateurs tels que les prestataires de services d'hébergement[1538]. La Cour a considéré qu'une injonction obligeant un fournisseur d'accès à Internet à une supervision illimitée de la totalité des communications électroniques afin de prévenir des infractions à la propriété intellectuelle ne garantissait pas l'équilibre entre le droit de propriété intellectuelle et la protection des données personnelles. Cependant selon l'art. 9.1/a) de la Directive 2004/48/CE, les États membres doivent garantir que les autorités judiciaires puissent rendre des ordonnances de référé visant à prévenir toute atteinte imminente à un droit de propriété intellectuelle ou à empêcher des récidives. Concernant les contrefacteurs faisant usage de réseaux P2P, le nouveau règlement 679/2016/CE semble fournir dans son art. 23 une nouvelle solution : il prévoit que les législations des États membres établissent des restrictions à certaines prévisions du Règlement lorsque celles-ci sont nécessaires pour garantir l'exécution de demandes de droit civil. Ces restrictions doivent constituer une mesure nécessaire et proportionnée dans une société démocratique ainsi que respecter l'essence des libertés et des droits fondamentaux. Ainsi ces restrictions doivent contenir la finalité du traitement, les catégories de données traitées ou la durée de leur conservation. Dans l'affaire *UPC Telekabel Wien*[1539], la CJ s'occupe à nouveau de la responsabilité des FAI concernant l'accès des abonnés aux contenu protégés par le droit d'auteur et mis en ligne par des tiers. La CJ admet qu'un fournisseur d'accès à Internet peut se voir ordonner de bloquer à ses clients l'accès à un site web qui porte atteinte au droit d'auteur. Toutefois, une telle injonction et son exécution doivent

---

1534 A. SPAGNOLO, op. cit., p. 131; S. KULK, « Filtering for Copyright Enforcement in Europe after the Sabam cases », in European Intellectual Property Review, 2012, p. 794.

1535 PSYCHOGIOPOULOU, « Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers after Scarlet », in European Intellectual Property Review, 2012, p. 554.

1536 Aff. C-360/10, cit., §. 52

1537 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) c. Netlog NV, C 360/10,16 février 2012.

1538 Ainsi la Cour renvoie par analogie à l'arrêt Scarlet Extended, précité, § 49.

1539 CJUE, *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH e Wega Filmsproduktionsgesellschaft mbH*, aff. C-314/12, 27 mars 2014. Deux entreprises allemandes qui détenaient les droits de certains films se sont aperçues que leurs films pouvaient, sans leur consentement, être visionnés, voir téléchargés à partir d'un site Internet. Sur demande de ces deux entreprises, les tribunaux autrichiens ont interdit au fournisseur d'accès à Internet, établi en Autriche, de fournir à ses clients l'accès à ce site. Pour sa part, le fournisseur d'accès Internet considère qu'une telle injonction ne peut pas lui être adressée car elle n'entretenait aucune relation commerciale avec les exploitants du site Internet.

assurer un juste équilibre entre les droits fondamentaux concernés. Or, lorsque plusieurs droits fondamentaux sont en conflit, il incombe aux É tats membres de veiller à se fonder sur une interprétation du droit de l'Union et de leur droit national qui permette d'assurer un juste équilibre entre ces droits fondamentaux. La Cour rappelle sa jurisprudence dans laquelle elle a jugé que le droit de l'Union s'oppose à toute injonction, prise par une juridiction nationale, vers un fournisseur d'accès à internet dans la mise en place d'un système de filtrage afin de prévenir les téléchargements illégaux de fichiers, à titre préventif, à ses frais exclusifs, et sans limitation dans le temps[1540]. Elle a également jugé disproportionné la mise en place d'un système de filtrage général visant l'ensemble des utilisateurs dans le but de prévenir l'usage illicite des œuvres musicales et audiovisuelles[1541]. La Cour estime dès lors que les droits fondamentaux concernés ne s'opposent pas à une telle injonction, à la double condition que les mesures prises par le fournisseur d'accès ne privent pas inutilement les utilisateurs de la possibilité d'accéder de façon licite aux informations disponibles, afin de garantir la liberté d'information des utilisateurs d'Internet et que ces mesures aient pour effet d'empêcher ou, au moins, de rendre difficilement réalisables les consultations non autorisées des objets protégés et de décourager sérieusement les utilisateurs de consulter les objets mis à leur disposition en violation du droit de propriété intellectuelle. Le juste équilibre entre droit et conflit doit être trouvé de la part des autorités nationales [1542] . En facilitant la communication de l'information, les sites Internet peuvent notamment partager des musiques, des films et des jeux informatiques en violation des droits d'auteur. La CourEDH s'est penchée sur la question du droit d'auteur dans l'affaire *Neij et Sunde Kolmisoppi c. Suède*[1543]. L'affaire concernait la condamnation d'exploitants d'un site Internet qui permettait aux tiers de partager des fichiers en violation des droits d'auteur. La requête a été rejetée et la Cour a notamment indiqué que l'ingérence poursuivait un but légitime, à savoir la protection des parties civiles titulaires de droits d'auteur sur les œuvres litigieuses et que la condamnation des requérants à des peines d'emprisonnement poursuivait les buts légitimes de « protection des droits d'autrui » et de « prévention des infractions » au sens de l'article 10 § 2. La Cour a estimé que l'obligation des autorités nationales de protéger le droit de propriété des plaignants, tant au regard de la loi sur le *copyright* qu'au regard de la Convention, constituait une raison valable de restreindre la liberté d'expression. En outre, les intéressés n'avaient rien fait pour supprimer les fichiers *torrent* litigieux, alors qu'on les avait enjoint de les effacer. Selon la Cour, l'État défendeur doit mettre en balance d'un côté, l'intérêt des sites Internet à faciliter le partage de l'information au sens de l'article 10 de la Convention, et, de l'autre, le respect des droits des auteurs d'œuvres protégées qui relèvent de l'article 1 du Protocole no 1. La jurisprudence de la Cour européenne des droits de l'homme en matière de propriété intellectuelle sur Internet sous l'angle de l'art. 8 de la Convention est peu fournie. Cela permet de constater que, nonobstant l'importance de son usage contemporain, les litiges

1540 Voy. arrê t de la Cour du 24 novembre 2011, Scarlett Extended, C-70/10.

1541 Voy. arrê t de la Cour du 16 février 2012, SABAM, C-360/10.

1542 Voy. § 24 de l'arrêt.

1543 CEDH, *Neij et Sunde Kolmisoppi c. Suède* req. no 40397/12, 13 mars 2013.

liés à Internet sont encore peu nombreux sous l'angle de l'article 1er du Protocole no 1 à la Convention.

CONCLUSION DU CHAPITRE I

A l'instar de la quasi-totalité des autres droits fondamentaux, le droit à la protection des données personnelles est susceptible d'être restreint lorsqu'il entre en conflit avec des contraintes collectives relevant de l'intérêt général ou d'autres intérêts individuels également protégés. Ainsi les deux juridictions européennes utilisent des méthodes similaires quant à l'application et l'interprétation du droit à la protection des données personnelles. Il a été possible d'établir une analogie interprétative dans la mise en œuvre normative du droit fondamental à la protection des données personnelles entre la Cour de justice et la CourEDH. Toutefois, l'étude de l'application des justifications formelles a montré que le contrôle effectué par la CourEDH est plus étendu que celui effectué par la Cour de justice, ce dernier se traduisant souvent par une simple vérification de l'existence d'une base légale et comme le démontre la jurisprudence récente, parfois le juge ne se penche même pas sur la question[1544]. Ainsi, l'importance du contrôle formel dans l'ordre juridique de l'Union européenne semble moindre. En revanche, pour la CourEDH, la condition de l'existence d'une base légale encadrant l'ingérence a souvent constitué un moyen suffisant pour conclure à la violation de la CEDH sans avoir besoin de se prononcer sur le fond de l'affaire. Elle a ainsi développé le principe de « qualité de la loi » qui a été repris par la jurisprudence de la Cour de justice[1545] . Concernant le contrôle de type matériel, l'étude de son application s'avère plus poussée au sein de l'Union européenne avec plusieurs degrés de contrôle. En effet, la Cour européenne des droits de l'homme exerce un contrôle qui va de l'absence de marge nationale d'appréciation à la vérification que l'ingérence de l'État n'est pas déraisonnable. Diversement le contrôle opéré par la Cour de justice comporte plusieurs degrés et exige, que les actes pris par l'Union afin de réaliser les objectifs légitimes prévus, « ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs »[1546], sachant que « l'étendue du pouvoir d'appréciation »[1547] du législateur de l'Union peut être limitée, en fonction de la nature du droit garanti, ainsi que de la nature, la gravité et la finalité de l'ingérence. Cela souligne la capacité du juge de Luxembourg à graduer et renforcer la protection face à l'augmentation et à l'aggravation des atteintes. Ces différents degrés du contrôle de proportionnalité ont montré que le contrôle est pour la plupart limité. Seuls des motifs liés à la nature particulièrement sensible des données ou aux atteintes particulièrement graves peuvent justifier un contrôle de proportionnalité approfondi *stricto sensu*. Ainsi le droit à la protection des données personnelles peut faire l'objet de mesures de

---

1544 Voy. sur cet aspect les Conclusions de l'Avocat général P. CRUZ VILLALON, 12 décembre 2013, sous les affaires Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C 293/12 et C 594/12 dans lesquelles il se penche sur une analyse détaillée de l'existence de la base légale de la directive 24/2006. Analyse laissée de côté par la CJ dans ses motivations.

1545 Voy. CJCE, Rechnungshof c. Österreichischer Rundfunk et autres, aff. C-465/00, C-138/01, C-139/01, 20 mai 2003, §77-79.

1546 Voy. §46 de la décision Digital Rights.

1547 Voy. §47 de la décision Digital Rights.

limitation non seulement provenant de l'État mais également des restrictions provenant de la mise en balance avec les droits et intérêts d'autrui. Le principe de proportionnalité se retrouve systématisé par la jurisprudence récente de la Cour de justice. D'une part, elle a indiqué aux juridictions nationales comment examiner les restrictions au droit à la protection des données personnelles prises au nom de la liberté d'expression[1548]. C'est aussi à travers ce principe qu'elle donné des indications aux juridictions nationales sur la manière d'examiner les restrictions au droit à la protection des données personnelles au nom du droit à la protection de la propriété intellectuelle[1549]. D'autre part, dans l'affaire *Volker und Markus* elle a soumis au respect du principe de proportionnalité les restrictions prises par les institutions de l'Union européenne elles-mêmes, et elle a mis en balance le principe de transparence avec le respect des art. 7 et 8 de la Charte[1550]. Dans cette affaire elle a invalidé, sur le fondement du principe de proportionnalité, les dispositions de deux règlements qui imposaient de publier le nom des personnes physiques bénéficiaires des aides attribuées dans le cadre de la politique agricole commune[1551]. Le droit à la protection des données n'est ni absolu ni intangible et doit être mis en balance avec d'autres droits, dont le droit à la protection de la propriété intellectuelle, à la liberté d'entreprise des fournisseurs de services de télécommunication électronique et à la liberté d'expression. Ainsi le droit à la protection des données a fait l'objet d'une assez importante jurisprudence de la part la Cour de justice. En effet le droit à la protection de la propriété intellectuelle et à la liberté d'expression est protégé par la Charte des droits fondamentaux de l'Union européenne. Face au droit à la propriété intellectuelle, dans le cadre de la lutte contre le téléchargement illégal, certains États membres ont adopté des mesures prévoyant la transmission à des personnes privées tierces des données personnelles relatives au trafic. Cette transmission ayant pour objectif que ces personnes tierces puissent engager des procédures civiles contre les atteintes au droit d'auteur doit être prévue par la loi. Ainsi le présent chapitre a analysé les restrictions dont le droit à la protection des données peut faire l'objet lorsqu'il entre en conflit avec des contraintes collectives relevant de l'intérêt général et d'autres intérêts individuels également protégés. Face aux difficultés de pondération entre le droit à la protection des données et l'intérêt public ou les droits d'autrui, il est possible d'apporter des observations d'ordre général. Si les restrictions au nom de l'intérêt général sont longtemps apparues comme les plus régulières, celles au nom des intérêts individuels se sont également développées. La révolution numérique constitue un moyen de renforcer la capacité de l'État à garantir la sécurité publique, l'ordre publique, la recherche et la poursuite

---

1548 CJCE, G. Ch., 16 décembre 2008, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, aff. C-73/07, Rec. I-09831, § 56.

1549 CJCE, G. Ch., 29 janvier 2008, Productores de Música de España (Promusicae) c. Telefónica de España SAU, aff. C-275/06, Rec. I-00271 ; confirmé par CJCE (ord.), 19 février 2009, LSG-Gesellschaft zur Wahrnehmung von Leistungsschutzrechten GmbH c. Tele2 Telecommunication GmbH, aff. C-557/07.

1550 CJUE, G. Ch., 9 novembre 2010, Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, aff. C-92/09 et C-93/09, § 72 : Il convient également de vérifier si la limitation apportée aux droits consacrés par les articles 7 et 8 de la charte est proportionnée au but légitime recherché.

1551 D. SIMON, « Transparence et vie privée », *Europe*, 2011, n° 1, pp. 11 et s. Voy. également E. DEGRAVE, « Arrêt Volker und Markus Schecke et Eifert : le droit fondamental à la protection des données à caractère personnel et la transparence administrative », préc., spéc. p. 98.

d'infractions pénales, grâce à l'enregistrement et la conservation de la vie de l'individu. La surveillance secrète, le fichage se révèlent un instrument utile de la politique de sécurité publique. Cependant cela ne cesse de créer de nouveaux risques pour les droits et libertés des individus. Le droit fondamental à la protection des données personnelles exerce donc un rôle primordial et permet de pondérer l'action de l'État. Nous avons mis en évidence les problématiques associées à la conciliation entre le droit à la protection des données personnelles et d'autres droits fondamentaux et l'importance du rôle joué par la liberté d'expression dans une société démocratique. Cependant, celle-ci doit céder lorsque l'ingérence a pour objet des données relatives à la santé [1552] ou à une procédure judiciaire impliquant un mineur [1553] . Toutefois, lorsque la publication affecte des individus appartenant à la sphère publique, la protection accordée par l'article 8 de la CEDH cède face à la liberté d'expression en raison du fait que l'information s'insère dans un débat d'intérêt général[1554]. À travers l'analyse de la jurisprudence, il résulte que la CJUE priorise la protection des données personnelles face à l'accès à l'information alors que la CourEDH effectue une mise en balance plus équilibrée. Cela s'explique par la réalisation d'un long développement jurisprudentiel dont les arrêts se révèlent plus élabores que ceux de la CJUE. Il faut relever que le Règlement 967/2016, encadrant le droit à l'oubli, apporte certaines nouveautés dans la relation entre le droit à la protection des données personnelles et la liberté d'expression. Toutefois, les critères de pondération restent dans les mains des États membres, en prévoyant les exceptions aux normes du Règlement de sorte qu'un équilibre entre les deux droits soit trouvé. Le droit à la protection des données personnelles peut se voir restreint par la protection du droit de propriété intellectuelle. Sur cet aspect, il manque une jurisprudence de la Cour européenne des droits de l'homme alors que la Cour de justice s'est prononcée d'une manière timide estimant qu'il incombait aux autorités et aux juridictions des États membres, non seulement d'interpréter leur droit national d'une manière conforme au droit de l'Union européenne, mais également de veiller à ne pas se fonder sur une interprétation de celles-ci qui entrerait en conflit avec lesdits droits fondamentaux ou avec les autres principes généraux du droit communautaire, tels que le principe de proportionnalité.

1552 Dans les affaires *Armonienė c. Lituanie* et *Biriuk c. Lituanie* (25 novembre 2008), la CEDH a estimé que la divulgation de l'état de santé des requérants (qui étaient séropositifs) n'avait pas respecté les exigences de l'art. 8 de la CEDH (*cfr.* avec les arts. 8 de la Directive et 9 du Règlement).

1553 La publication de données relatives à la vie privée d'un mineur dans le contexte d'une procédure judiciaire a été jugée contraire à l'art. 8 de la CEDH dans l'arrêt du 19 juin 2012 dans l'affaire *Kurier Zeitungsverlag und Druckerei GmbH c. Autriche*). Le Règlement n'est pas étranger à la problématique concernant le traitement de données appartenant à des mineurs et l'aborde dans plusieurs de ses articles (*cf.* arts. 6.1/f), 8, 12.1 et 57.1/b) du Règlement).

1554 CEDH, *Von Hannover c. Allemagne*, 7 février 2012, expose les critères généralement cités par la CeDH pour concilier la vie privée avec la liberté d'expression (§§ 109-113) : l'ouverture d'un débat public, le rôle joué par un individu dans la sphère publique, sa conduite préalable, le contenu, la forme et les conséquences de la publication ainsi que les circonstances dans lesquelles les données personnelles ont été traitées.

CHAPITRE II. L'AUTONOMISATION DU STANDARD DE PROTECTION

181 La Cour de justice consolide le rôle constitutionnel en matière de données à caractère personnel. En matière de droit à la protection des données personnelles, le rôle de la Cour de justice semble être central et stratégique pour la dimension globale de la société numérique. La Cour de justice ne se limite pas à jouer le rôle de juge d'intégration et d'instance d'appel dans le système juridique de l'Union, mais elle joue le rôle de « gardienne constitutionnelle »[1555]. La présente analyse veut déterminer si l'adoption de la Charte a produit une vague de constitutionnalisation de la part de la Cour de justice qui a soumis les instruments juridiques relatifs à la protection des données personnelles déjà existants à un test de cohérence avec les valeurs proclamée dans la Charte elle-même. La constitutionnalisation du droit à la protection des données personnelles (son inscription dans le droit primaire) a comporté l'autonomisation de la Cour de justice dans sa fonction constitutionnelle vis-à-vis de la CEDH. Le rôle de garant des droits fondamentaux de la Cour de justice est confirmé par la jurisprudence récente[1556]. Le présent chapitre analyse empiriquement la « constitutionnalisation du droit à la protection des données » à travers l'étude de quatre affaires récentes rendues par la Cour de justice. Il s'agit de l'affaire *Digital Rights Ireland*, concernant les métadonnées de communication, l'affaire *Schrems*, concernant la surveillance des données sur Internet, l'affaire *Google Spain* consacrant le droit à l'oubli, et, pour finir, l'avis de la Cour de justice concernant l'accord PNR avec le Canada sur la collecte des données de voyage. Dans ces mêmes affaires, la Cour de justice a une lecture constitutionnelle du droit à la protection des données personnelles, c'est-à-dire de paramètre de légitimité de la directive 2006/24, de l'accord *Safe Harbor* avec les États-Unis, et de l'accord PNR avec le Canada. Ainsi les actes de l'Union sont lus à la lumière des articles 7 et 8 de la Charte des droits fondamentaux et à eux seuls. Dans ces affaires concernant la protection des données personnelles, la Cour de justice a montré son émancipation de la ConventionEDH en disposant désormais d'un titre propre pour mener son analyse. Ainsi cette vague de *constitutionnalisation* du droit à la protection des données personnelles a produit une autonomisation progressive du raisonnement de la Cour de justice vis-à-vis de la ConventionEDH et de la jurisprudence de la CourEDH qui l'ont pourtant longtemps inspirée. L'inscription des droits fondamentaux dans le droit primaire de l'Union européenne a nécessairement renforcé le rôle de la Cour de justice (Section I). Cela a comporté l'autonomisation du raisonnement de la Cour de justice[1557]. Ainsi sa grille d'analyse est basée désormais uniquement sur la Charte des droits fondamentaux (Section II).

[1555] M. CLAES, M. DE VISSER, « The Court of Justice as a Federal Constitutional Court: A Comparative Perspective », in Elke Cloots et al. Eds, *Federalism In The European Union*, 2012, p. 83-100.

1556 F. SUDRE et R. TITINIERE, *Droit communautaire des droits fondamentaux*, Ed. Nemesis, Bruxelles 2012, p. 17.

[1557] D.DERO BUGNY, *Les rapports entre la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme*, Bruxelles, Bruylant, 2015, p. 46-55.

Section I. Une protection spécifique inscrite dans le droit primaire de l'Union européenne

182 La protection des données à caractère personnel, inscrite à l'article 16 TFUE. Afin de comprendre la qualité et la complexité de l'intervention de la Cour de justice, il convient de définir le cadre juridique du droit de l'Union européenne en matière de protection des données personnelles.

Le traité de Lisbonne a introduit une base juridique spécifique pour la protection des données personnelles (article 16 TFUE)[1558]. En effet, avant l'entrée en vigueur du traité de Lisbonne, la législation relative à la protection des données était divisée entre le premier pilier (protection des données collectées à des fins privées et commerciales, en utilisant la méthode communautaire) et le troisième pilier (protection des données collectées à des fins répressives, au niveau intergouvernemental)[1559]. En conséquence, les processus décisionnels applicables à chacun de ces deux domaines suivaient des règles différentes. La structure en piliers a disparu avec le traité de Lisbonne qui renforce les bases nécessaires à l'élaboration d'un système de protection des données plus clair et plus efficace, tout en prévoyant de nouveaux pouvoirs pour le Parlement européen, celui-ci devenant colégislateur. L'article 16 du TFUE dispose que le Parlement européen et le Conseil fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union.

Toutefois, une base juridique spécifique persiste en ce qui concerne la politique étrangère et de sécurité commune (article 39 TFUE) avec l'adoption de décisions *ad hoc* du Conseil. Ainsi, l'article16 TFUE, attribue au législateur européen une compétence concourante avec les États pour l'adoption, selon la procédure ordinaire, des règles relatives à la protection des personnes physiques à l'égard du traitement des données personnelles[1560].

Cet article est issu de l'article 286 du traité CE, introduit par le traité d'Amsterdam et entré en vigueur le 1er janvier 1999, qui prévoyait l'application aux institutions et organes de l'Union des actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[1561]. Sur cette base, le règlement 45/200134 a été adopté, qui institue notamment une autorité de contrôle indépendante, le Contrôleur européen, chargée de surveiller le traitement des données à caractère personnel par les institutions et organes de l'Union. Se fondant sur l'article 16 TFUE,

---

1558 Voy. sur l'article 16 TFUE : H. HIJMANS, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Heidelberg, 2016.

1559 Voy. Ancien article 95 TCE.

1560 B. CORTESE, « La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona », in *Dir. Un. eur.*, 2013, n. 2.

1561 AVoy. article 286 TCE : « 1. À partir du 1er janvier 1999, les actes communautaires relatifs à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sont applicables aux institutions et organes institués par le présent traité ou sur la base de celui-ci. 2. Avant la date visée au paragraphe 1, le Conseil, statuant conformément à la procédure visée à l'article 251, institue un organe indépendant de contrôle chargé de surveiller l'application desdits actes communautaires aux institutions et organes communautaires, et adopte, le cas échéant, toute autre disposition utile. »

la Commission européenne a proposé en janvier 2012 une réforme globale en matière de protection des données, à travers deux textes : un règlement général sur la protection des données à caractère personnel et une directive sur le traitement et la circulation de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière, ou d'exécution de sanctions pénales. Le changement relatif au statut juridique de la Charte a été possible grâce à la révision du Traité de Lisbonne. L'article 6(1) TUE stipule que l'Union « reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux de l'Union européenne du 7 décembre 2000, telle qu'adaptée le 12 décembre 2007 à Strasbourg, laquelle a la même valeur juridique que les traités ». A la différence d'autres droits fondamentaux de la Charte, la protection des données personnelles est inscrite dans le droit primaire et relève de celui-ci. Ainsi l'article 16 du TFUE dans son §1 reconnaît à toute personne physique un droit à la protection de ses données personnelles. Dans son § 2, il consacre la compétence du législateur communautaire pour l'adoption de règles en matière de protection des données personnelles. Le droit à la protection des données personnelles est ainsi renforcé dans son contenu et dans l'extension du contrôle judiciaire grâce aux autorités de contrôle indépendantes (les seules autorités administratives de contrôle prévues par la Charte). Cette compétence du législateur communautaire est désormais reconnue dans toutes les matières, même pour la coopération judiciaire en matière pénale et pour la coopération policière. Par conséquent, le législateur a accueilli favorablement ce nouveau cadre juridique et ces nouvelles compétences, avec l'élaboration d'un chantier de réformes en matière de protection des données personnelles, à travers la révision de la directive n° 95/46 CE et l'adoption d'un règlement relatif à la protection des données personnelles (Règlement 679/2016 RGPD) [1562], à travers la révision de la décision-cadre n° 2008/977 JAI[1563] et à travers l'adoption d'une directive relative à la protection des données personnelles en matière de justice et de police. Ainsi grâce au paragraphe 2 de l'art. 16 TFUE, les deux nouveaux instruments législatifs ont été examinés à travers la procédure de codécision[1564]. Toutefois, la jurisprudence de la Cour de justice a dû trancher sur la base légale des actes de l'Union en matière de données personnelles (§1). Nous verrons que dans son raisonnement elle dispose d'une grille d'analyse propre à son ordre juridique (§2).

1562 Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, COM/2012/011 final - 2012/0011 (COD).

1563 Cons. CE, déc.-cadre 2008/977/JAI, 27 nov. 2008 relative à la protection des données à caractère personnel traitées dans le cadre de la coopération policière et judiciaire en matière pénale : JOCE n° L 350, 30 déc. 2008, p. 60 à 71.

1564 Proposition de directive du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données COM(2012) 10 final - 2012/0010 (COD).

§1. Une nouvelle base juridique

183 Le statut de droit primaire de la Charte à travers une clause de renvoi. L'hétérogénéité de la législation et la *summa divisio* entre premier et troisième pilier ont comporté une protection modulée. En effet dans le cadre du marché intérieur et dans l'ELSJ, les objectifs n'étaient pas les mêmes. Une protection différente a d'ailleurs été mise en place. De plus, la Cour de justice, ne disposant pas originairement d'une source autonome, a utilisé comme grille d'analyse la ConventionEDH et la jurisprudence de la CourEDH. Toutefois, la situation a changé depuis l'entrée en vigueur du traité de Lisbonne : la protection des données personnelles a été érigée à droit fondamental dans l'Union européenne et, parallèlement au droit à la vie privée, elle est désormais inscrite dans la Charte des droits fondamentaux de l'Union européenne et possède la même valeur juridique que les traités grâce à la clause de renvoi de l'article 6 du TUE. Il est intéressant de rappeler la formulation de l'article 6 TUE : « L'Union reconnaît les droits, les libertés et les principes énoncés dans la Charte des droits fondamentaux (…) laquelle a la même valeur juridique que les traités »[1565]. Ainsi, l'entrée de la Charte des droits fondamentaux dans le droit primaire s'est faite par la petite porte[1566], c'est-à-dire que le changement de statut juridique de la Charte a été fait par le biais d'un « renvoi ». Cependant, le changement de paradigme a eu des conséquences décisives. En effet, après avoir proclamé le droit au respect de la vie privée et familiale dans son article 7, la Charte, avec son article 8, est sans doute le premier texte général sur les droits fondamentaux qui consacre une disposition spéciale à la protection des données à caractère personnel (A). Or, non seulement la protection des droits fondamentaux ne constituait pas un champ de compétence originaire de l'Union européenne[1567], mais elle n'est devenue une compétence confiée au législateur communautaire que récemment, à partir du traité de Lisbonne[1568] (B).

1565 Cette affirmation est renforcée par le processus d'adhésion de l'Union européenne à la Convention européenne des droits de l'homme prévu par le même article (6.2 TUE).

1566 Voy. l'article « La protection des droits fondamentaux dans l'Union européenne après le traité de Lisbonne », publié sur le site Fondation Robert Schuman, disponible à l'adresse: https://www.robert-schuman.eu/fr/questions-d-europe/0173-la-protection-des-droits-fondamentaux-dans-l-union-europeenne-apres-le-traite-de-lisbonne

1567 C'est d'abord la Cour de justice qui, dans son célèbre avis n° 2/94 sur l'adhésion de l'Union à la Convention européenne des droits de l'homme, a écarté une telle compétence au profit de l'Union. Cette position est confirmée par les articles 6 du TUE et 51 de la Charte qui interdisent explicitement toute compétence générale de l'Union dans ce domaine.

1568 Le traité de Lisbonne a créé une nouvelle base juridique (article 16 TFUE) en matière de droit à la protection des données personnelles.

A - L'influence de l'article 8 de la Charte sur l'évolution constitutionnelle de l'Union européenne

184 L'article 8 de la Charte comme norme de référence. La Charte consacre, dans son article 8, le droit à la protection des données à caractère personnel comme un droit fondamental, distinct du droit au respect de la vie privée et familiale, du domicile et des communications, formulé dans l'article 7. Cependant, la Cour de justice a souligné que les articles 7 et 8 de la Charte était étroitement liés[1569]. Toutefois, l'article 8 ne concerne pas uniquement les données relatives à la vie privée, mais comprend toutes les données relatives à des personnes. Ainsi, il peut s'agir de données qui identifient de manière indirecte la personne. De plus, les explications de la Charte établies sous la responsabilité du *praesidium* ne font pas figurer l'article 8 de la Charte des droits fondamentaux de l'Union européenne parmi les dispositions qui, aux fins de l'application de l'article II-112 §3 de la Constitution européenne[1570], sont considérées comme ayant le même sens et la même portée que les articles correspondants de la CEDH. Dans l'intention du législateur, il n'y aurait donc pas une correspondance directe entre l'article 8 de la CEDH (respect de la vie privée et familiale) et l'article 8 de la Charte. La Charte se différencie de la CEDH, puisque cette dernière protège les données personnelles comme composantes du plus ample droit à la vie privée et familiale. En effet, pour la Cour de Strasbourg, le droit à la protection des données personnelles « relève de la protection de la vie privée », dans une interprétation extensive elle « englobe le droit pour l'individu de nouer et développer des relations avec ses semblables » [1571] , alors que le législateur de l'Union européenne a voulu consacrer un droit spécifique à la protection des données personnelles. Il s'agit d'un droit qui connaît un « fabuleux destin », fortement lié à l'évolution de la Cour de justice de l'Union européenne [1572] . L'article 8 de la Charte a deux sources principales : premièrement, l'acquis communautaire primaire et dérivé (l'article 16 TFUE et 39 TUE et la directive 95/46/CE), deuxièmement, les sources propres au Conseil de l'Europe, l'article 8 CEDH et la Convention n°108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. Le §1 de l'article 8 de la Charte consacre le principe de protection[1573], le §2, énonce les modalités de mise en œuvre de cette

---

1569 Voy. CJUE, Volker und Markus Shecke §47 : « il importe de relever que l'article 8, paragraphe 1, de la charte énonce que « Toute personne a droit à la protection des données à caractère personnel la concernant ». Ce droit fondamental est étroitement lié au droit au respect de la vie privée consacré à l'article 7 de cette même charte ». CJUE, Asociación Nacional de Establecimientos Financieros de Crédito aff. C 468/10 et C 469/10, § 41.

1570 « Dans la mesure où la présente Charte contient des droits correspondant à des droits garantis par la Convention européenne de sauvegarde des Droits de l'homme et des libertés fondamentales, leur sens et leur portée sont les mêmes que ceux que leur confère ladite convention ».

1571 CEDH Z c. Finlande, 25 février 1997, §99.

1572 Pour un commentaire sur la question de savoir si la Cour de justice est « au cœur de la gouvernance européenne » voy. S. SAURUGGER et F. TREPAN, « La Cour de justice au cœur de la gouvernance européenne », Pouvoirs, n°149, 2014, pp.59-75.

1573 «Toute personne a droit à la protection des données à caractère personnel la concernant».

protection (exigence de loyauté, spécialité, consentement ou fondement légitime, droit d'accès et de rectification) [1574] . Dans le §3 est posé le principe de contrôle confié à une autorité indépendante, en lui offrant un rôle para-constitutionnel[1575]. De telles autorités constituent le seul exemple d'autorité indépendante inscrit dans la Charte. Cependant, les droits proclamés par la Charte ne sont pas inconditionnels et, dans une logique analogue à celle de la CEDH, l'article 52, paragraphe 1, de la Charte prévoit les limites aux droits protégés[1576]. La Charte présente donc l'avantage de consacrer un droit spécifique à la protection des données à caractère personnel, alors que la CourEDH le fait dériver de l'article 8 relatif au droit au respect de la vie privée. Toutefois, dans un premier temps, la CJUE se réfère souvent cumulativement aux articles 7 et 8 de la Charte sans reconnaître l'autonomie du droit à la protection des données personnelles par rapport au droit au respect de la vie privée. Dans une première phase, les éventuelles limites ne relèvent pas de l'article 52 de la Charte mais plutôt de l'article 8§2 de la CEDH. Intéressante sur ce point est l'affaire *Volker* de 2010[1577]. Ici, toute référence à l'article 8 de la CEDH souligne que, dans cette première phase, le droit à la protection des données personnelles est considéré comme purement accessoire au droit au respect de la vie privée. Les articles 7 et 8 de la Charte sont certes étroitement liés[1578], mais selon l'avocat général Cruz Villalon, dans l'affaire *Digital Rights*, on peut distinguer des données qui sont « personnelles en tant que telles », relatives au nom et à ses accessoires et plus au moins neutres si bien qu'on pourrait parler d'« d'informations nominatives » et des données « qui sont plus que personnelles », susceptibles de « cerner l'individualité psychologique de la personne telle qu'elle se manifeste à travers ses comportements ». Ces dernières se rapportent à la vie privée et à l'intimité[1579]. Cependant, la Cour de justice n'a pas suivi cette distinction et considère plus simplement que l'obligation imposée aux fournisseurs des communications électroniques de

---

1574 L'article 8 ne se contente pas de garantir, d'une manière générale, le droit à la protection des données personnelles. Il consacre quelques principes et droits contenus dans la directive 95/46/CE : les principes de loyauté, de finalité et de légitimation du traitement. Il assure aussi un droit d'accès et de rectification et l'existence d'une autorité indépendante chargée de faire respecter ces principes.

1575 Voy. Art 8 §3.

1576 Art. 51§1 « Toute limitation de l'exercice des droits et libertés reconnus par la présente Charte doit être prévue par la loi et respecter le contenu essentiel desdits droits et libertés. Dans le respect du principe de proportionnalité, des limitations ne peuvent être apportées que si elles sont nécessaires et répondent effectivement à des objectifs d'intérêt général reconnus par l'Union ou au besoin de protection des droits et libertés d'autrui ».

1577 CJUE, Volker und Markus Schecke GbR (C-92/09) et Hartmut Eifert (C-93/09) contre Land Hessen. Volker précit. §. 52 « Dans ces conditions, il doit être considéré, d'une part, que le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la Charte, se rapporte à toute information concernant une personne physique identifiée ou identifiable (voy., notamment, Cour eur. D. H., arrêts Amann c. Suisse du 16 février 2000, Recueil des arrêts et décisions 2000-II, § 65, ainsi que Rotaru c. Roumanie du 4 mai 2000, Recueil des arrêts et décisions 2000-V, § 43) et, d'autre part, que les limitations susceptibles d'être légitimement apportées au droit à la protection des données à caractère personnel, correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH ».

1578 La Cour l'a déjà souligné dans les affaires jointes C-92/09 et C-93/09, Volker und Markus Schecke & Eifert §47 : « À cet égard, il importe de relever que l'article 8, §1, de la charte énonce que « toute personne a droit à la protection des données à caractère personnel la concernant ». Ce droit fondamental est étroitement lié au droit au respect de la vie privée consacré à l'article 7 de cette même Charte.

1579 Voy. les § 64,65 et 68 de ses conclusions. Si les deux catégories, font l'objet de l'article 8 de la Charte, seule la seconde catégorie permettrait, selon l'avocat général, de qualifier une ingérence dans le droit à la vie privée garanti par l'art 7, dans la mesure où les données collectées peuvent permettre « l'établissement d'une cartographie aussi fidèle qu'exhaustive d'une fraction importante des comportements d'une personne relevant strictement de sa vie privée, voy.e d'un portrait complet et précis de son identité privée », v. §74 de l'arrêt Digital Rights.

conserver les données « constitue en soi une ingérence au sens des articles 7 et 8 de la Charte des droits fondamentaux »[1580]. Ainsi les deux droits sont distincts mais étroitement liés.

B – L'influence de l'article 16 du TFUE sur les compétences de l'Union européenne

185 Une base juridique incertaine. L'article 16 du TFUE[1581] donne désormais une base juridique unique à l'adoption des actes en matière de protection des données à caractère personnel, mettent fin à la question complexe des compétences[1582].
L'article 16 du TFUE reprend la formulation de l'article 8§1 de la Charte et dispose que toute personne a le droit à la protection des données à caractère personnel. Il crée également un fondement juridique nouveau et général en faisant référence à la procédure législative ordinaire pour déterminer les règles encadrant les traitements de données dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union. Il s'agit donc d'une base juridique englobant les anciens premier et troisième piliers. Seul le domaine de la politique étrangère et de la sécurité commune y échappe, selon les termes de l'article 16§3 TFUE[1583] ; ce domaine est régi par l'article 39 TUE. En effet, cet article vient ajouter une dérogation aux dispositions de l'article16 §2 du TFUE en prévoyant qu'il incombe au Conseil d'adopter « une décision fixant les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du présent chapitre, et à la libre circulation de ces données »[1584]. De plus, au contraire d'autres droits fondamentaux de la Charte, la protection des données personnelles relève du droit primaire. Ainsi, l'article 16 TFUE attribue au législateur européen une compétence concourante avec les États pour l'adoption, selon la procédure ordinaire, des règles relatives à la protection des personnes physiques à l'égard du traitement des données

---

1580 Voy. point 34 de l'arrêt.

1581 Le traité de Lisbonne supprime l'ancienne structure en piliers: le premier pilier étant la Communauté européenne, plus intégré, le deuxième, la politique étrangère et de défense commune, reposant sur des mécanismes intergouvernementaux, le troisième désignant la coopération policière et judiciaire en matière pénale. Les nouveaux traités contiennent quelques dispositions spécifiques sur la protection des données personnelles: l'article 16 TFUE, nouvelle base juridique générale dans le domaine, et l'article 39 TUE concernant plus spécifiquement la politique étrangère et de sécurité commune.

1582 Voy. l'affaire 10 février 2009, Irlande c. Conseil C-301/06, où le juge s'était fixé sur l'objectif prépondérant de la directive 2006/24/CE « vie privée et communications électroniques » pour trouver sa base juridique dans les dispositions relatives à la réalisation du marché intérieur. Il estimait que l'objectif de la directive était l'intérêt général de lutter contre le terrorisme et les formes graves de criminalité afin de garantir la sécurité publique, en la rattachant à l'ELSJ. Voy. sur le traité F.X. PRIOLLAUD et D. SIRITZKY, *Le traité de Lisbonne, Texte et Commentaire article par article des nouveaux traités européens* (TUE-TFUE), La documentation française, 2008, 528 p, sp. p. 84 etss.

1583 Aux termes de l'article 39TUE, c'est le Conseil seul qui adoptera des règles en ma matière.

1584 Voy. article 39. Conformément à l'article 16 du traité sur le fonctionnement de l'Union européenne et par dérogation à son paragraphe 2, le Conseil adopte une décision fixant les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les États membres dans l'exercice d'activités qui relèvent du champ d'application du présent chapitre, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes.

personnelles[1585]. Toutefois, il est possible de constater la permanence de la *summa divisio* dans le choix d'utiliser deux instruments juridiquement distincts : pour l'ex-premier pilier le règlement 679/2016 et pour l'ex-troisième pilier la directive 680/2016.

Selon la jurisprudence consolidée de la Cour de justice, le choix de la base juridique d'un acte de l'Union, y compris celui adopté aux fins de la conclusion d'un accord international, doit être fondé sur des facteurs objectifs susceptibles de contrôle juridictionnel, y compris la finalité et le contenu de cet acte[1586]. Toutefois, par exception, si l'acte poursuit à la fois plusieurs finalités ou que plusieurs éléments sont indissociables, sans que l'un soit accessoire à l'autre, un tel acte doit reposer sur les différentes bases juridiques correspondantes[1587]. Néanmoins le recours à une double base juridique est exclu lorsque les procédures énoncées dans les règles respectives sont incompatibles[1588].

La Cour de justice s'est exprimée à nouveau sur la base juridique en matière de protection des données personnelles dans l'Avis 1/2015[1589] concernant le projet d'accord UE-Canada sur l'échange des données PNR. La Cour estime que vue la double finalité de l'accord PNR avec le Canada, à savoir : d'une part, assurer la sécurité public et, d'autre part, prescrire les moyens par lesquels les données PNR seront protégées, l'accord envisagé poursuit des finalités indissociables les unes des autres. La décision du Conseil relative à la conclusion de cet accord pourrait alors être fondée à la fois sur l'article 16 et l'article 87, paragraphe 2, sous a), TFUE[1590]. En effet, dans le domaine pénal, les informations sont échangées entre les autorités publiques ou entre ces autorités et des organismes privées pour analyser des menaces, identifier des activités criminelles ou évaluer des risques. En termes de compétences et de bases légales, l'action de l'Union s'est développée dans trois domaines matériels. Le premier concerne le développement de la coopération entre les autorités de la justice pénale, par la reconnaissance

---

1585 B. CORTESE, « La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona », in *Dir. Un. eur*., 2013, n. 2.

1586 Voy.CJUE, C-43/12, *Commissione c. Parlamento e Consiglio*, 6 mai 2014, §29, et aff. C-263/14, *Parlamento c. Consiglio*, 14 juin 2016, § 43.

1587 Voy. CJUE, aff. C-263/14, Parlamento c. Consiglio, 14 juin 2016, § 44.

1588 Voy. CJUE, aff. C-155/07, Parlamento c. Consiglio, 6 novembre 2008, § 37.

1589 Voy. Avis 1/2015 de la Cour de justice Gr. Chambre.

1590 Voy. Point 95 à 98 de l'Avis : Eu égard aux considérations qui précèdent, la décision relative à la conclusion de l'accord envisagé se rattache, en premier lieu, directement à l'objectif poursuivi par l'article 16, paragraphe 2, TFUE. En effet, cette disposition constitue, sans préjudice de l'article 39 TUE, une base juridique appropriée lorsque la protection des données à caractère personnel est l'une des finalités ou des composantes essentielles des règles adoptées par le législateur de l'Union, y compris de celles s'insérant dans le cadre de l'adoption de mesures relevant des dispositions du traité FUE relatives à la coopération judiciaire en matière pénale et à la coopération policière, ainsi que le confirment l'article 6 bis du protocole n° 21 et l'article 2 bis du protocole n° 22, de même que la déclaration mentionnée au point 32 du présent avis. Il en résulte que la décision du Conseil relative à la conclusion de l'accord envisagé doit être fondée sur l'article 16 TFUE. En second lieu, cette décision doit également être fondée sur l'article 87, paragraphe 2, sous a), TFUE. En effet, cette disposition prévoit que, aux fins de l'article 87, paragraphe 1, TFUE, selon lequel l'Union « développe une coopération policière qui associe toutes les autorités compétentes des États membres », le Parlement et le Conseil peuvent établir des mesures portant sur « la collecte, le stockage, le traitement, l'analyse et l'échange d'informations pertinentes ». En revanche, cette décision ne saurait être fondée sur l'article 82, paragraphe 1, second alinéa, sous d), TFUE, lequel prévoit la possibilité pour le Parlement et le Conseil d'adopter des mesures visant « à faciliter la coopération entre les autorités judiciaires ou équivalentes des États membres dans le cadre des poursuites pénales et de l'exécution des décisions ». En effet, ainsi que l'a relevé M. l'avocat général au point 108 de ses conclusions, aucune des dispositions de l'accord envisagé ne vise à faciliter une telle coopération. S'agissant de l'autorité canadienne compétente, celle-ci ne constitue ni une autorité judiciaire ni une autorité équivalente.

mutuelle des décisions judiciaires et des décisions des autorités nationales, et l'harmonisation des lois et règlements des États membres (article 82, paragraphe 1, du TFUE)[1591]. Le second concerne le développement de « la coopération policière » qui regroupe toutes les autorités compétentes des États membres, y compris les services de police, les services douaniers et les autres services répressifs spécialisés dans le secteur de la prévention ou de la détection des crimes et des enquêtes connexes (article 87, paragraphe 1, du TFUE)[1592]. Le troisième volet « coordination, soutien et achèvement » concerne l'action de l'Union visant à « encourager et soutenir l'action des États membres dans le domaine de la prévention du crime »[1593]. La position de la Commission et du Conseil (ainsi que de la France, du Royaume-Uni, de l'Estonie et de la Bulgarie) devant la Cour de justice était favorable au choix des bases juridiques selon un objectif de sécurité reposant sur les articles 82 et 87 TFUE. Au contraire, dans sa demande d'avis, le Parlement européen a plutôt soutenu la base juridique de l'article 16 TFUE [1594]. La Cour a estimé que la solution de la double base juridique était applicable par rapport à l'objectif double et inséparable de l'accord (articles 16, paragraphe 2, et 87, paragraphe 2, a), du TFUE), tout en rejetant la base juridique de l'article 82 (coopération judiciaire en matière pénale), considérée comme non conforme au cas d'espèce [1595]. Selon la Cour, entre les deux bases légales on ne peut pas identifier une base principale, ni une base accessoire à l'autre[1596]. Cette double base juridique n'implique pas de procédures d'adoption différentes car les deux règles prévoient la procédure législative ordinaire. Ce qui implique le vote à la majorité qualifiée du Conseil et la participation du Parlement en tant que colégislateur. En fin de compte, le choix de la Cour attribue une importance sans précédent à la base juridique de l'article 16 du TFUE, y compris dans le domaine de la coopération pénale. La solution développée de manière très articulée par la Cour de justice a des conséquences politico-institutionnelles évidentes.

1591 À cette fin, le TFUE prévoit que le Parlement européen et le Conseil, agissant conformément à la procédure législative ordinaire, peuvent adopter une série de mesures visant à harmoniser le droit pénal procédural.

1592 Dans ce cas, il est prévu que l'Union adopte, par la procédure ordinaire de décision, les mesures appropriées, qui concernent : « a) la collecte, le stockage, le traitement, l'analyse et l'échange des informations pertinentes ; b) le soutien à la formation du personnel et à la coopération en matière d'échange de personnel, d'équipement et de recherche dans le domaine de la criminologie ; c) des techniques d'enquête communes pour la détection des formes graves de criminalité organisée ».

1593 Voy. article 84 du TFUE.

1594 Voy. § 55.

1595 Selon une jurisprudence constante de la Cour, le choix de la base juridique d'un acte de l'Union, y compris celui adopté en vue de la conclusion d'un accord international, doit se fonder sur des éléments objectifs susceptibles de contrôle juridictionnel, parmi lesquels figurent la finalité et le contenu de cet acte (arrêts du 6 mai 2014, Commission/Parlement et Conseil, C 43/12, EU:C:2014:298, point 29, ainsi que du 14 juin 2016, Parlement/Conseil, C 263/14, EU:C:2016:435, point 43 et jurisprudence citée). Si l'examen d'un acte de l'Union démontre qu'il poursuit deux finalités ou qu'il a deux composantes et si l'une de ces finalités ou de ces composantes est identifiable comme étant principale tandis que l'autre n'est qu'accessoire, l'acte doit être fondé sur une seule base juridique, à savoir celle exigée par la finalité ou la composante principale ou prépondérante. À titre exceptionnel, s'il est établi, en revanche, que l'acte poursuit à la fois plusieurs objectifs ou a plusieurs composantes qui sont liés de façon indissociable, sans que l'un soit accessoire par rapport à l'autre, de telle sorte que différentes dispositions des traités sont applicables, une telle mesure doit être fondée sur les différentes bases juridiques correspondantes (arrêt du 14 juin 2016, Parlement/Conseil, C 263/14, EU :C:2016:435, point 44 et jurisprudence citée). Toutefois, le recours à une double base juridique est exclu lorsque les procédures prévues pour l'une et l'autre de ces bases sont incompatibles (arrêt du 6 novembre 2008, Parlement/Conseil, C 155/07, EU :C:2008:605, point 37 et jurisprudence citée). C'est à la lumière de ces considérations qu'il y a lieu de déterminer la base juridique appropriée pour la décision du Conseil relative à la conclusion de l'accord envisagé.

1596 Voy. §77 de l'arrê.

Dorénavant, l'équilibre des intérêts impliqués entre les droits fondamentaux et le besoin de sécurité dans la coopération policière ne seront pas contournés. De plus, preuve de l'effectivité du nouveau cadre juridique fourni par le traité de Lisbonne, la Cour de justice a commencé à s'exprimer régulièrement en matière de protection des données personnelles grâce au renvoi préjudiciel.

§2. L'influence de l'article 8 de la Charte sur le contrôle « constitutionnel » opéré par la Cour de justice

186 La Cour de justice comme gardienne des droits fondamentaux. La question de la nature de la Cour de justice de l'Union européenne n'est pas nouvelle. En 1963, l'avocat général Maurice Lagrange s'interrogeait déjà : « qu'est-ce donc que cette Cour de justice ? Cour internationale ? Cour fédérale ? Juge administratif ? Juge constitutionnel ? Probablement une combinaison de tous ces caractères »[1597]. En effet, la Cour de justice emprunte certains traits caractéristiques de chacun de ces modèles juridictionnels, mais dans le cadre de cette étude, il est intéressant de souligner la ressemblance entre la Cour de justice et une Cour constitutionnelle à travers les affaires concernant le droit fondamental à la protection des données personnelles[1598]. Or, la Cour de justice s'est montrée garante du droit constitutionnel à la protection des données à caractère personnel, mais la question de savoir si la juridiction de l'Union exerce ou non la justice constitutionnelle implique donc de rechercher les critères d'identification de cette notion, et relever ainsi les caractéristiques communes des juridictions constitutionnelles. Ainsi, il n'est pas possible d'oublier l'absence de Constitution formelle au sein de l'Union européenne, le défaut de cadre étatique ou la différence de nature des actes contrôlés. Cependant, certaines fonctions exercées par la juridiction de l'Union sont révélatrices de l'existence d'une justice constitutionnelle [1599] . Ainsi la Cour de justice s'élève comme gardienne des droits fondamentaux et interprète des textes fondateurs de son ordre juridique à travers le renvoi préjudiciel [1600] (A) et à travers le contrôle des actes externes de l'Union européenne passés avec des États tiers[1601] (B).

1597 M. LAGRANGE, *La Cour de justice des Communautés européennes*, E.D.C.E., 1963, p. 55.

1598 G. CAGGIANO, « La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali », *Studi sull'integrazione europea*, 2018, fasc.1, p. 3 et ss.

1599 Voy. en ce sens V. LEBON, « Le constitutionnalisme européen », Pulim, Coll. Droit public, 2007, p. 107.

1600 Voy. art 267 TFUE Le renvoi préjudiciel est la procédure qui permet à une juridiction nationale d'interroger la Cour de justice de l'Union européenne sur l'interprétation ou la validité du droit communautaire dans le cadre d'un litige dont cette juridiction est saisie. Le renvoi préjudiciel offre ainsi le moyen de garantir la sécurité juridique par une application uniforme du droit de l'Union européenne. Grace au renvoi en interprétation de la norme européenne (droit primaire et droit secondaire), le juge national demande à la Cour de justice de préciser un point d'interprétation du droit européen afin de pouvoir l'appliquer correctement. A travers le renvoi en validité d'une norme européenne du droit secondaire, le juge national demande à la Cour de justice de contrôler la validité d'un acte de droit européen.

1601 M. CREMONA, A. THIES, *The European Court of Justice and external relations law: constitutional challenges*, Oxford, 2014, p. 23; R. MASTROIANNI, « Le garanzie dei valori nell'azione esterna e il ruolo della Corte di giustizia » , in E. SCISO, R. BARATT, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Torino, 2016, p. 213 ss.;

A. Le contrôle constitutionnel à travers le renvoi préjudiciel

187 Le monopole interprétatif de la Cour de justice. La Cour de justice de l'Union européenne bénéficie, à l'instar d'une Cour constitutionnelle nationale, du monopole de l'interprétation des textes fondateurs de son ordre juridique (bien que s'exerçant sur des objets distincts du constitutionnalisme classique). En ce sens, elle s'apparente à une juridiction constitutionnelle. Il n'y a pas de justice constitutionnelle sans l'attribution centrale qu'est le contrôle de constitutionnalité [1602]. Il s'ensuit qu'il ne peut y avoir de justice constitutionnelle sans Constitution à protéger. A l'instar d'une Cour constitutionnelle européenne, la juridiction de l'Union détient le monopole de l'interprétation authentique de la « Charte constitutionnelle »[1603]. En effet, en vertu de l'article 344 TFUE, « les États membres s'engagent à ne pas soumettre un différend relatif à l'interprétation où à l'application des traités à un mode de règlement autre que ceux prévus par ceux-ci ». En contrepartie de ce dessaisissement, inconnu en droit international classique, les traités prévoient un dispositif complet de voies de recours permettant l'accès à l'interprétation authentique délivrée par la Cour, au premier rang desquelles le mécanisme du renvoi préjudiciel. Le maintien de l'unité et de la cohérence de l'ordre juridique de l'Union par la force de l'interprétation authentique relève du caractère constitutionnel du rôle de la Cour de justice. En effet, la Cour de justice demeure la seule juridiction habilitée à interpréter de façon authentique le droit de l'Union [1604] . L'unité d'interprétation du droit primaire et dérivé est la condition *sine qua non* de l'unité et de la cohérence de l'ordre juridique de l'Union[1605]. Pour rendre l'ensemble opératoire, le mécanisme préjudiciel est progressivement devenu le vecteur privilégié de la coopération entre la Cour de justice et les juridictions nationales. Le renvoi en validité [1606] est un mécanisme tout à fait

T. HORSEY, « Reflections on the role of the Court of Justice as the « motor » of European integration: Legal limits to judicial lawmaking », *in Common Market Law Review,* 2013, p. 931 ss.; R. SCHÜTZE, *Constitutionalism and the European Union*, in C. BARNARD, S. Peers (eds), *European Union Law*, Oxford, 2014, p. 71 ss.

1602 L. FAVOREU, *Les cours constitutionnelles*, Dalloz, 2016, p. 24.

1603 Il s'agit d'une qualification prétorienne employée par la Cour de justice pour désigner les traités. Voy. en ce sens : CJCE, 23 avril 1986, Parti écologique « Les Verts » c/Parlement, aff. 294/83, Rec., 1986, p. 1365 (cf. pt. 23) ; CJCE, Avis 1/91, 14 décembre 1991, Rec., 1991, p. 6079.

1604 Voy. article 19 TUE selon lequel la Cour de justice de l'Union européenne « assure le respect du droit dans l'interprétation et l'application des traités ».

1605 F. BESTAGNO, « Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali », *in Diritto dell'Unione europea*, 2015, p. 21 ss.

1606 Toute juridiction nationale, saisie d'un litige dans lequel l'application d'une règle de droit européen soulève des questions (litige principal), peut décider de s'en remettre à la Cour de justice pour résoudre ces questions. Il existe deux types de renvoi préjudiciel : le renvoi en interprétation de la norme européenne (droit primaire et droit secondaire) : le juge national demande à la Cour de justice de préciser un point d'interprétation du droit européen afin de pouvoir l'appliquer correctement ;le renvoi en validité d'une norme européenne du droit secondaire : le juge national demande à la Cour de justice de contrôler la validité d'un acte de droit européen. Pour un commentaire Voy. : F. BESTAGNO, « Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali », in *Diritto dell'Unione europea*, 2015, p. 21 ss.; ID., « I rapporti tra la Carta e le fonti secondarie di diritto dell'UE nella giurisprudenza della Corte di giustizia », in Diritti umani e diritto internazionale, 2015, p. 259 ss.

comparable à celui des Cours constitutionnelles qui se prononcent sur la constitutionnalité des lois nationales par rapport à la constitution[1607].

La Cour de justice a eu sa première occasion de se prononcer à travers un renvoi en interprétation de validité en matière de protection des données personnelles, dans l'affaire *Schecke*[1608]. Ici, la Cour de justice a dû vérifier si les actes législatifs de l'UE respectent l'article 8 de la Charte et visent un juste balancement entre les exigences de respect des données personnelles et les objectifs à atteindre par les mêmes actes juridiques. Ainsi, dans l'affaire *Schecke*, la Cour de justice a annulé deux règlements relatifs à la politique agricole commune car, sur la base du principe de transparence sur l'attribution des fonds, ils violaient le droit à la protection des données personnelles[1609].

Deux affaires historiques ont confirmé le rôle de la Cour de justice comme gardienne constitutionnelle du droit fondamental à la protection des données. Il s'agit des affaires *Digital Rights*[1610] et *Schrems*[1611]. Ici, il est intéressant de souligner la radicalité des choix opérés par la Cour de justice. En effet, dans l'affaire *Digital Rights*, elle a préféré déclarer l'invalidité totale et *ab initio* de l'acte de droit dérivé car incompatible avec le droit fondamental à la protection des données personnelles. Dans l'affaire *Scherms*, la Cour de justice a déclaré l'invalidité totale de l'acte exécutif concernant la décision de protection « adéquate » de la Commission vis-à-vis de la législation américaine, sans que dans le procès principal ni le requérant, ni le juge national de renvoi en ait fait mention. Ici, la Cour de justice souligne l'importance de l'instrument de renvoi préjudiciel d'invalidité, elle réaffirme la jurisprudence constante de la Cour selon laquelle « l'Union est une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité avec, notamment, les traités, les principes généraux du droit ainsi que les droits fondamentaux ».

Dans l'affaire *Schrems*, les décisions de la Commission adoptées au titre de l'article 25, paragraphe 6, de la directive 95/46 ne sauraient donc échapper à un tel contrôle. Cela étant, la Cour est seule compétente pour constater l'invalidité d'un acte de l'Union, tel qu'une décision

---

1607 G. CAGGIANO, « La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali », Studi sull'integrazione europea, 2018, fasc.1, p. 3 et ss.

1608 CJUE, 9 novembre 2010, C-92/09 et C-93/09, Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen. Pour le commentaire Voy. I. ANDOULSI, « L'arrêt de la Cour du 9 novembre 2010 dans les affaires jointes Volker und Markus Schecke GBR et Hartmut Eifert contre Land d'Hessen (C-92/09 et C-93/09): une reconnaissance jurisprudentielle du droit fondamental à la protection des données personnelles *?* », in Cahiers de droit européen,2011, n° 2, p.471-522.

1609 En particulier certaines dispositions du Règlement n. 1290/2005 (CE) n. 1290/2005 du Conseil, du 21 juin 2005, et dans son ensemble le règlement n. 259/2008 du18 mars 2008.

1610 Voy. sur l'arrêt Digital Rights: M. P. GRANGER, K. IRION, « The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection », in *European Law Review*, 2014, p. 835 ss.; O. LYNSKEY, « The Data Retention Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety: Digital Rights Ireland », in *Common Market Law Review*, 2014, p. 1789 ss.; M. NINO, « L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia Ue: prospettive ed evoluzioni future del sistema europeo di Data Retention », in *Il diritto dell'Unione europea*, 2014, p. 803 ss.; E. ROSSI, « Il diritto alla »privacy" nel quadro giuridico europeo ed internazionale alla luce delle recenti vicende sulla sorveglianza di massa », in *Diritto comunitario e degli scambi internazionali*, 2014, p. 331 ss.; M. MESSINA, « La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità », in *Ordine internazionale e diritti umani*, 2014, p. 396 ss. Sui seguiti della sentenza, v. S. CARRERA, E. GUILD, « Safe Harbour or into the Storm? EU-US Data Transfers after the Schrems Judgment », in *CEPS Liberty and Security in Europe Papers*, November 2015 ; V. ZENO-ZENCOVICH, G. RESTA (a cura di), *La protezione transnazionale dei dati personali dai "safe harbour principles" al "privacy shield"*, Roma, 2016.

1611 CJUE, Gr. Ch. *Schrems*, C-362/14, 6 octobre 2015.

de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46. Le caractère exclusif de cette compétence ayant pour objet de garantir la sécurité juridique en assurant l'application uniforme du droit de l'Union. Si les juridictions nationales sont, certes, en droit d'examiner la validité d'un acte de l'Union, tel qu'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46, elles ne sont toutefois pas dotées de la compétence pour constater elles-mêmes l'invalidité d'un tel acte[1612]. Les motifs d'invalidité ont été trouvés dans les méthodes effectives de traitement des données personnelles. En effet, contrairement à ce que les autorités américaines avaient garanti [1613] , dans l'ordre juridique des États-Unis manquaient des règles adéquates pour limiter l'ingérence « strictement nécessaire » pour atteindre l'objectif de protection de la sécurité nationale, et aucun recours spécifiques de nature judiciaire ou administrative ne protégeait les parties concernées. Surtout, lorsque l'ingérence était nécessaire, il n'existait ni mécanisme de surveillance indépendant ni de recours adéquats. Dans le cas d'espèce, les interférences constatées affectent le contenu essentiel du droit à la protection des données personnelles. En tout état de cause, selon la Cour de justice, de telles ingérences dépassent de loin la stricte nécessité[1614]. Ici, la Cour rappelle sa jurisprudence selon laquelle un tel contrôle rentre dans sa structure constitutionnelle puisque l'Union européenne est une Union de droit dans laquelle tout acte de ses institutions est soumis au contrôle de la conformité avec, notamment, les traités, les principes généraux du droit ainsi que les droits fondamentaux [1615] . Les décisions de la Commission adoptées au titre de l'article 25, paragraphe 6, de la directive 95/46 ne sauraient donc échapper à un tel contrôle. Cela étant, la Cour est seule compétente pour constater l'invalidité d'un acte de l'Union[1616]. Cette compétence relève du caractère exclusif ayant pour objet de garantir la sécurité juridique en assurant l'application uniforme du droit de l'Union. Si les juridictions nationales sont, certes, en droit d'examiner la validité d'un acte de l'Union, tel qu'une décision de la Commission adoptée au titre de l'article 25, paragraphe 6, de la directive 95/46, elles ne sont toutefois pas dotées de la compétence pour constater elles-mêmes l'invalidité d'un tel acte[1617].

Il est possible de parler d'arrêts historiques car, auparavant, les autres arrêts sur la protection des données dans le cadre du renvoi préjudiciel n'ont pas donné lieu à une déclaration d'invalidité. En effet, dans une première phase de la jurisprudence, la Cour de justice s'est limitée à clarifier l'équilibre avec d'autres droits fondamentaux, tels que le droit de propriété

1612 Voy. CJUE, *Schrems* préec. § 60-62.

1613 La décision d'adéquation de la Commission s'appelait improprement « accord sur la sphère de sécurité entre l'UE et les États-Unis », dite « *Safe Harbor* » alors qu'en réalité, il s'agissait essentiellement d'un acte unilatéral de la Commission suite à la présentation de documents par l'administration américaine.

1614 Voy. CJUE, Scherms, § 93, 94 et 95.

1615 Voy. la jurisprudence citée dans l'arrêt CJUE, *Schrems* § 60 : arrêts Commission e.a./Kadi, C 584/10 P, C 593/10 P et C 595/10 P, EU : C:2013:518, point 66; Inuit Tapiriit Kanatami e.a./Parlement et Conseil, C 583/11 P, EU:C:2013:625, point 91, ainsi que Telefónica/Commission, C 274/12 P, EU:C:2013:852, point 56).

1616 Voy. §61 de la décision. La Cour de justice cite les arrêts Melki et Abdeli, C 188/10 et C 189/10, EU : C:2010:363, point 54, ainsi que CIVAD, C 533/10, EU:C:2012:347, point 40.

1617 Voy., en ce sens, arrêts Foto Frost, 314/85, EU : C:1987:452, points 15 à 20, ainsi que IATA et ELFAA, C 344/04, EU:C:2006:10, point 27

intellectuelle ou la liberté d'expression[1618]. Plus récemment, dans l'arrêt *Tele2*[1619], la Cour de justice a réaffirmé avec force et sans ambiguïté la jurisprudence *Digital Rights Ireland* à travers un renvoi en interprétation. En effet, depuis la déclaration d'invalidité de la directive 2006/24 qui imposait aux opérateurs Internet et Télécoms la conservation des données de trafic de la totalité des utilisateurs de leurs services, alors jugée incompatible avec la Charte des droits fondamentaux de l'Union européenne en raison de l'atteinte disproportionnée qu'elle porte au droit au respect de la vie privée et à la protection des données personnelles, de nombreux États membres avaient abrogé leur dispositif national de conservation généralisée des données, les jugeant incompatibles avec le droit européen. La Cour de justice, investie de deux renvois préjudiciels de la part du Royaume-Uni et de la Suède, a considéré que les mesures nationales imposant aux opérateurs de conserver des données de connexion entraient dans le champ d'application de la directive 2002/58 dite « *e-privacy* »[1620]. La Cour estime que toute solution inverse aurait privé l'article 15, paragraphe 1, de la directive 2002/58 de tout effet utile. Pour rappel, l'article 15, paragraphe 1, de la directive 2002/58 permet aux États membres d'imposer aux opérateurs de conserver les données de connexion de leurs utilisateurs « lorsqu'une telle limitation constitue une mesure nécessaire, appropriée et proportionnée, au sein d'une société démocratique, pour sauvegarder la sécurité nationale, c'est-à-dire la sûreté de l'État, la défense et la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales ou d'utilisations non autorisées du système de communications électroniques ». Cet article introduit donc une dérogation à d'autres droits énoncés par la directive « *e-privacy* » comme le droit à la confidentialité des communications ou l'effacement des données de trafic. Toutefois cette dérogation est autorisée à titre exceptionnel, par conséquent elle ne saurait devenir une règle de principe en droit national. À cet égard, la Cour de justice pose un principe fort d'interdiction pour les États membres d'imposer aux opérateurs la conservation généralisée des données. Elle indique extrêmement clairement que l'article 15 de la directive 2002/58 « s'oppose à une réglementation nationale prévoyant, à des fins de lutte contre la criminalité, une conservation généralisée et indifférenciée de l'ensemble des données relatives au trafic et des données de localisation de tous les abonnés et utilisateurs inscrits concernant tous les moyens de communication électronique ». La Cour constate que les données de connexion occupent une place primordiale dans la vie quotidienne : « Prises dans leur ensemble, ces données sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci. En particulier, ces données fournissent les moyens d'établir, ainsi que l'a relevé M. l'avocat général aux points 253, 254 et 257 à 259 de ses conclusions, le

1618 Voy. les affaires CJUE, Promusicae, C-275/06, 29 janvier 2008, CJUE, Satamedia C-73/07, 16 décembre 2008, CJUE, Scarlet, C-70/10, 24 novembre 2011, CJUE, Bonnier, C-461/10, 19 avril 2012.

1619 CJUE, Gr. Ch., Tele2 Sverige e Watson e a., aff. Jointes C-203/15 et C-698/15, 21 décembre 2016.

1620 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques).

profil des personnes concernées, information tout aussi sensible, au regard du droit au respect de la vie privée, que le contenu même des communications »[1621]. La Cour de justice constate que l'ingérence d'une telle réglementation dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère d'une vaste ampleur et doit être considérée comme particulièrement grave. La circonstance où la conservation des données est effectuée sans que les utilisateurs des services de communications électroniques en soient informés est susceptible de générer dans l'esprit des personnes concernées le sentiment que leur vie privée fait l'objet d'une surveillance constante[1622]. De plus, elle souligne que même si une telle réglementation n'autorise pas la conservation du contenu d'une communication et, partant, n'est pas de nature à porter atteinte au contenu essentiel desdits droits, la conservation des données relatives au trafic et des données de localisation pourrait toutefois avoir une incidence sur l'utilisation des moyens de communication électronique et, en conséquence, sur l'exercice par les utilisateurs de ces moyens de leur liberté d'expression, garantie à l'article 11 de la Charte[1623]. La Cour de justice a ainsi donné des indications aux législateurs nationaux et a défini des conditions très strictes dans lesquelles la conservation des données de connexion peut être imposée aux opérateurs. Selon la Cour de justice, si les États membres peuvent imposer une conservation préventive des données de connexion, ce n'est que dans le cadre de conditions très restrictives ; à savoir que cette obligation de conservation ne peut être que : ciblée, mise en œuvre à des fins de lutte contre la criminalité grave, et limitée au strict nécessaire en ce qui concerne les catégories de données à conserver, les moyens de communication visés, les personnes concernées ainsi que la durée de conservation retenue. Dans cet affaire, l'article 15, paragraphe 1, de la directive 2002/58, telle que modifiée par la directive 2009/136, est lu à la lumière des articles 7, 8 et 11 ainsi que de l'article 52, paragraphe 1, de la Charte des droits fondamentaux.

B. Le contrôle constitutionnel de la Cour de justice vis-à-vis des actes externes de l'Union

188 L'incompatibilité du projet d'accord UE-Canada avec les droits fondamentaux. Dans son avis 1/2015[1624], concernant le projet d'accord UE-Canada sur l'échange des données PNR, la Cour a statué pour la première fois sur la compatibilité d'un projet d'accord international avec la Charte des droits fondamentaux[1625]. Dans son avis, elle a déclaré que le système de transfert de données personnelles, tel que prévu dans l'accord, ne peut être conclu en raison de l'incompatibilité de certaines de ses dispositions avec les droits fondamentaux. En effet, l'accord envisagé vise, en particulier, à permettre à une ou à plusieurs autorités publiques d'un

1621 Voy., par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, § 27.

1622 Voy., par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, §37.

1623 Voy., par analogie, en ce qui concerne la directive 2006/24, arrêt Digital Rights, §39.

1624 Voy. Avis de la Cour (grande chambre) du 26 juillet 2017, rendu en vertu de l'article 218, paragraphe 11, TFUE, concernant le projet d'accord entre le Canada et l'Union européenne sur le transfert des données des dossiers passagers aériens depuis l'Union vers le Canada.

1625 Pour une analyse compléte du contentieux UE- États-Unis sur les accords PNR voy. P. PUOTI, « Lotta al terrorismo, sicurezza del trasporto aereo e protezione dei dati personali nel recente contenzioso Usa/Ue », in Le scommesse dell'Europa: diritti, istituzioni, politiche, 2009, p. 421 ss.

pays tiers de traiter et de conserver les données à caractère personnel de passagers aériens. La légalité d'un tel acte est conditionnée au respect des droits fondamentaux protégés dans l'ordre juridique de l'Union, en particulier de ceux garantis par les articles 7 et 8 de la Charte. Selon l'avocat général P. Mengozzi, l'accord envisagé est incompatible avec les articles 7, 8 et l'article 52, paragraphe 1, de la charte des droits fondamentaux de l'Union européenne dans la mesure où l'accord envisagé : permet, au-delà de ce qui est strictement nécessaire, d'élargir les possibilités de traitement de données des dossiers passagers, indépendamment de la finalité, indiquée à l'article 3 dudit accord, de prévention et de détection des infractions terroristes et des actes graves de criminalité transnationale ; prévoit le traitement, l'utilisation et la conservation par le Canada de données des dossiers passagers contenant des données sensibles ; accorde au Canada, au-delà de ce qui est strictement nécessaire, le droit de divulguer toute information pour autant qu'il se conforme à des exigences et à des limites juridiques raisonnables ; autorise le Canada à conserver des données des dossiers passagers pour une période maximale de cinq ans pour, notamment, toute action spécifique, vérification, enquête ou procédure juridictionnelle, sans que soit requis un lien quelconque avec la finalité, indiquée à l'article 3 dudit accord, de prévention et de détection des infractions terroristes et des actes graves de criminalité transnationale ; et admet que le transfert de données des dossiers passagers à une autorité publique d'un pays tiers puisse être réalisé sans que l'autorité canadienne compétente, sous le contrôle d'une autorité indépendante, se soit préalablement assurée que l'autorité publique destinatrice du pays tiers en question ne puisse pas elle-même ultérieurement communiquer lesdites données à une autre entité, le cas échéant, à un autre pays tiers.

Pour la conclusion d'un nouveau texte d'accord UE-Canada, la Cour établit des critères précis : déterminer plus clairement et plus précisément les données PNR concernées ; prévoir que les critères utilisés sont spécifiques et fiables ainsi que non discriminatoires ; prévoir que l'inclusion dans les bases de données soit limitée à celles qui sont gérées en relation avec la lutte contre le terrorisme et les crimes transnationaux graves ; prévoir que les données PNR peuvent être divulguées aux autorités publiques d'un autre pays tiers uniquement si ces dernières sont liées par un accord équivalent avec l'Union ou suite à une décision d'adéquation de la Commission ; prévoir un droit à l'information individuelle pour les passagers aériens lors de l'utilisation des données PNR ou dans le cas de communications à d'autres autorités ou individus et assurer le contrôle d'une autorité de contrôle indépendante. Bien que les traités ne puissent être assimilés à une constitution et étant donné qu'une comparaison n'implique pas une assimilation, rien n'empêche de relever des points de convergence quant aux attributions et fonctions exercées par la Cour de justice et celles attribuées à une cour constitutionnelle nationale. Ainsi la Cour de justice bénéficierait-t-elle, à l'instar d'une juridiction constitutionnelle, du monopole de l'interprétation authentique des textes fondateurs de son ordre juridique[1626].

Le contrôle sur le respect des droits fondamentaux par la Cour de justice n'est plus celui de la délimitation du champ de protection mais celui de la fixation d'un degré de protection[1627].

1626 O. DORD, « Ni absolue, ni relative, la primauté. Du Droit communautaire procédé de la Constitution », in H. GAUDIN (Dir.), Droit constitutionnel-Droit communautaire, vers un respect constitutionnel réciproque ?, Economica, Droit Public Positif, 2001, pp. 123-125.

1627 Voy. E. DUBOUT, « Le Défi de la Délimitation du Champ de la Protection des Droits Fondamentaux par la Cour de justice de l'Union Européenne », *ELSJ*, 2013, vol I. 6, n.1, pp. 5-23.

Une fois vérifié que l'inscription du droit à la protection des données personnelles dans la Charte des droits fondamentaux a octroyé à la Cour de justice à exercer son rôle de garante constitutionnel et à pousser le niveau d'intégration[1628] , il est possible de s'intéresser à la technique selon laquelle la Cour de justice exerce son pouvoir, notamment, en s'affranchissant de toute référence à la ConventionEDH et à la jurisprudence de la CourEDH et en utilisant la Charte des droits fondamentaux, et elle seule, comme grille d'analyse.

1628 Voy. E. DUBOUT « Le Défi de la Délimitation du Champ de la Protection des Droits Fondamentaux par la Cour de justice de l'Union Européenne », *ELSJ*., 2013, vol I. 6, n.1, pp. 5-23. Selon l'auteur, le sens de la protection des droits fondamentaux dans l'Union européenne a changé. A l'origine destinés à s'assurer de la légitimé de l'exercice du pouvoir européen, ils servent désormais de support à une nouvelle contrainte sur l'exercice du pouvoir national.

Section II. L'émancipation du raisonnement de la CJUE à l'égard de la CEDH

189 L'affirmation du standard plus élevé. Si sur le plan normatif il existe une législation hétérogène, sur le plan juridictionnel s'ajoute une protection hétéronome. En effet, la Cour de justice s'est inspirée, dans un premier temps, d'une source externe à l'Union européenne, à savoir, la ConventionEDH et la jurisprudence de la CourEDH à travers les principes généraux de droit. Toutefois, la constitutionnalisation de la Charte, c'est-à-dire la consécration de la Charte des droits fondamentaux dans le droit primaire, a permis à l'article 8, garantissant la protection des données personnelles, de doter l'Union européenne d'un droit fondamental spécifique distinct du droit au respect de la vie privée et familiale[1629]. La constitutionnalisation de la Charte est un évènement majeur pour la Cour de justice qui dispose désormais d'un titre propre de compétence lui permettant de développer une « interprétation autonome de la protection des données personnelles » [1630] et de jouer son rôle de gardienne des droits fondamentaux [1631] . Ainsi, elle a sanctionné le législateur de l'Union, invalidant dans son intégralité et avec effet rétroactif la directive 2006/24/CE[1632] sur la « rétention des données », car les ingérences vis-à-vis de l'article 8 de la Charte des droits fondamentaux étaient disproportionnées. Dans l'affaire *Google Spain* [1633] , elle a affirmé un « droit à l'oubli numérique » au dam du géant du web Google et dans l'affaire *Schrems* elle a annulé la décision de la Commission européenne sur l'adéquation du transfert des données vers les États-Unis[1634] en se basant uniquement sur la Charte des droits fondamentaux et en abandonnant toute références à la CEDH. Ainsi l'article 8 de la Charte devient la norme de référence de l'analyse de la Cour de justice (§1) lui permettant de remplir le rôle de juge « constitutionnel » dans la protection du droit fondamental à la protection des données personnelles (§2).

1629 Voy. l'article 7 de la Charte.

1630 R. TINIERE, « La cohérence assurée par l'article 52§3 de la Charte des droits fondamentaux de l'Union - Le principe d'alignement sur le standard conventionnel pour les droits correspondants », in C. Picheral et L. Coutron (dir.) Charte fondamental de l'Union européenne et Convention européenne des droits de l'homme, p. 14.

1631 S. SAUGGER et F. TERPAN, « La Cour de justice au cœur de la gouvernance européenne », Pouvoirs, n° 149, 2014, p. 59-75.

1632 Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE.

1633 CJ (GR. Ch), *Google Spain SL, Google Inc. Contre Agencia Española de Protección de Datos (AEPD), Mario Costeja González*, affaire C 131/12, 13 mai 2014.

1634 CJUE, *Maximillian Schrems c. Data Protection Commissioner,* C-362/14, 6 October 2015.

§1. Une autonomisation graduelle

190 Le changement de sens de la protection des droits fondamentaux dans l'Union européenne. Avant de se doter de son propre texte en matière de droits fondamentaux, la Cour de justice faisait référence aux principes généraux du droit communautaire. Elle étayait principalement son raisonnement sur la jurisprudence de la CourEDH par le biais de l'article 8 sur la vie privée et familiale. Toutefois le mouvement d'émancipation de la Cour de justice commence dès le traité d'Amsterdam [1635] qui a permis le passage « d'une conception fonctionnelle à une conception constitutionnelle des droits fondamentaux »[1636] et a entrainé « une mutation de l'ordre juridique communautaire ouvrant la perspective de la formation d'un droit communautaire des droits fondamentaux »[1637]. Avec la proclamation de la Charte des droits fondamentaux de l'Union européenne comme source de droit primaire, la Cour de justice commence son parcours d'autonomisation et d'émancipation vis-à-vis de la CEDH et de sa jurisprudence. L'article 8 de la Charte consacre un droit spécifique à la protection des données personnelles distinct de l'article 7 garantissant le respect de la vie privée. On assiste à une première phase de la jurisprudence de la Cour de justice fondée sur l'art. 8 de la CEDH (A) et à une nouvelle phase où e juge de l'Union dispose d'un titre propre, l'art. 8 de la Charte des droits fondamentaux pour fonder son raisonnement (B).

A. La redevance vis-à-vis de la jurisprudence de la CEDH

191 L'article 8 de la CEDH comme norme de référence. Avant l'existence d'un catalogue communautaire des droits et l'inscription de la Charte des droits fondamentaux dans le droit primaire, la Cour de justice a pallié ce manque en s'appuyant, à défaut de source autonome, sur la ConventionEDH. Toutefois elle semble progressivement s'affranchir de toute référence à cette convention. Ce mouvement d'émancipation est progressif. Ainsi, dans l'affaire *Osterreichischer Rundfunk* concernant l'interprétation de la directive 95/46, la norme de référence de la Cour de justice est l'article 8 de la Convention EDH. Ainsi la Cour de justice vérifie que la réglementation communautaire respecte les garanties et les conditions posées par l'article 8 de la Convention EDH[1638]. Elle va rechercher si la réglementation contestée constitue bien une ingérence dans la vie privée des requérants et si cette ingérence est justifiée à l'aune

1635 Voy. l'article 6 §1 du traité d'Amsterdam: « l'Union est fondée sur les principes de la liberté, de la démocratie, du respect des droits de l'homme et des libertés fondamentales, ainsi que de l'État de droit, principes qui sont communs aux États ».

1636 F. SUDRE, et T. TINIERE, *Droit communautaire des droits fondamentaux*, éd. Nemesis, Bruxelles, 2012, p. 17.

1637 Voy. F. SUDRE et T. TINIERE préec.

1638 CJUE, aff. jtes. C-465/00, C-138/01 et C_139/01, 20 mai 2003, Voy. §71-72.

des restrictions prévues à l'article 8§2 de la Convention. Dans cette affaire, elle reconnaît d'abord une ingérence dans la communication par un employeur à un tiers (l'autorité publique) de données nominatives relatives à la rémunération de ses salariés. Ensuite, elle base son raisonnement sur celui de la CourEDH dont elle cite la jurisprudence et vérifie si l'ingérence est justifiée, à savoir si elle « est prévue par la loi », c'est-à-dire si elle est formulée avec suffisamment de précision et si les objectifs poursuivis par l'ingérence sont proportionnés ; ce qui l'a conduit à examiner la nécessité de l'ingérence dans une société démocratique pour atteindre l'objectif poursuivi. Dans l'affaire *Lindqvist* [1639] , la ConventionEDH et la jurisprudence de la CourEDH figure encore comme norme de référence de la Cour de justice. Celle-ci doit confronter les droits garantis par la directive 95/46 avec la liberté d'expression proclamée par l'article 10 de la Convention EDH. Ici, une fois de plus, elle va couler son raisonnement sur la ConventionEDH, et ne voir dans la directive aucune restriction contraire à la liberté d'expression consacrée par l'article 10. Toutefois, elle renvoie aux juridictions nationales le soin d'assurer le juste équilibre des droits et intérêts en cause. Dans l'arrêt *Commission c. Allemagne*[1640], concernant la question de l'indépendance des autorités nationales de contrôle en matière de protection des données, la Cour de justice souligne que le double objectif de la directive 95/46 (à savoir, la libre circulation des données et la protection des données) est susceptible de porter atteinte au droit à la vie privée tel que reconnu à l'article 8 de la ConventionEDH. Au contraire, dans l'affaire *Commission c. The Bavarian Lager*[1641] concernant la pondération entre un règlement concernant l'accès aux documents par les institutions de l'UE et un autre relatif à la protection des données par les institutions, la Cour de justice procède à une interprétation basée sur l'article 8 de la Charte, ce qui illustre la « volonté d'autonomisation du droit communautaire par rapport à l'article 8 de la CEDH et à la jurisprudence s'y rapportant »[1642]. Il est possible de remarquer que cette affaire datant de 2010, donc lorsque la Charte des droits fondamentaux a déjà acquis force juridique de droit primaire, se réfère encore et exclusivement à la ConventionEDH et que la Charte passe sous silence le raisonnement de la Cour de justice. Toutefois, dans d'autres affaires antérieures à l'entrée en vigueur de la Charte, la Cour de justice s'inspire de manière indirecte de la jurisprudence de la CourEDH en rappelant uniquement les principes posés dans ses arrêtés précédents pour souligner l'importance de la protection de la vie privée (et non de la protection des données personnelles). C'est notamment le cas dans l'arrêt *Satamedia* [1643] lorsque pour guider les autorités nationales en la matière le Cour ne fait pas de référence explicite à la ConventionEDH. La référence indirecte à la ConventionEDH est encore plus subtile dans l'arrêt *Rijkeboer* où la Cour de justice se limite à renvoyer à sa jurisprudence, et dans les affaires *Osterreichischer Rundfunk* et *Lindqvist* dans lesquelles elle fonde son raisonnement sur celui de la CourEDH. Cependant, ce processus d'autonomisation est progressif et pas totalement abouti. Ainsi dans les affaires *Volker und Markus Schecke* et *Eifert*, concernant la publication sur Internet de

1639 CJUE, *Bodil Lindqvist*, aff. C-110/01, 6 novembre 2003.

1640 CJUE, *Commission c. Allemagne*, aff. C-518/07, 9 mars 2010.

1641 CJUE, Gr. Ch. Aff. C-28/08 P, 29 juin 2010.

1642 Commentaire de F. KAUFF-GAZIN, Europe, n°1à, octobre 2010, comm. 299.

1643 CJUE, *Satamedia*, aff.C-73/07, 16 décembre 2008.

données personnelles de bénéficiaires d'aides de fonds agricoles, la Cour de justice procède à l'interprétation de l'article 8 de la Charte mais à la lumière de l'article 8 de la CEDH et sous l'angle de la jurisprudence correspondante. Dans un premier temps, la Cour indique que le droit au respect de la vie privée et le droit à la protection des données personnelles consacrés aux articles 7 et 8 de la Charte sont « étroitement » liés[1644]. Dans un deuxième temps, elle souligne que ce droit n'est pas absolu et peut admettre des limitations au titre de l'article 8 paragraphe 2 et 52 paragraphe 1 de la Charte. Enfin, dans un dernier temps, la Cour s'appuie sur l'article 53 paragraphe 2 pour mettre en évidence la correspondance entre les articles 7 et 8 de la Charte et l'article 8 de la Convention tel qu'interprété par la jurisprudence de la Cour européenne. La Cour en conclut « d'une part, que le respect du droit à la vie privée à l'égard du traitement des données à caractère personnel, reconnu par les articles 7 et 8 de la Charte, se rapporte à toute information concernant une personne physique identifiée ou identifiable […] et, d'autre part, que les limitations susceptibles d'être légitimement apportées au droit à la protection des données à caractère personnel, correspondent à celles tolérées dans le cadre de l'article 8 de la CEDH »[1645]. La Cour de justice a donc associé ces deux droits malgré leur distinction au sein de la Charte. Toutefois, dans l'affaire *Scarlet Extended*[1646], le juge de Luxembourg abandonne toute référence à la CEDH. Ainsi, lorsque la Cour d'appel de Bruxelles a saisi la Cour de justice d'un renvoi préjudiciel à propos de la question de l'interprétation, par rapport au droit de l'Union, des directives communautaires sur l'obligation de filtrage ou de blocage des communications électroniques vis-à-vis d'un fournisseur d'accès à Internet, la Cour de justice a répondu en se référant exclusivement à la Charte[1647] alors que la juridiction de renvoi avait posé la question au regard des articles 8 et 10 de la CEDH. Cette idée d'autonomisation de la Cour de justice dans l'interprétation des normes relatives à la protection des données personnelles est confirmée dans les décisions plus récentes où tout le raisonnement de la Cour de justice est basé sur la Charte des droits fondamentaux.

B. Le dialogue constant des juges

192 Le progressif intérêt de l'Union européenne pour les droits fondamentaux. Il est indéniable que l'article8 CEDH a eu un rôle précurseur dans le droit de l'Union en matière de

1644 CJUE, G. Ch., Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen, aff. C-92/09 et C-93/09, Rec. I-11063, 9 novembre 2010, § 47.

1645 Voy. 652 de la décision.

1646 CJUE, aff. C-70/10, 24 novembre 2011.

1647 De plus, l'avocat général Cruz Villalon, dans ses conclusions du 1er avril 2011 avait souligné : »Les droits et les libertés et principes énoncés dans la Charte ayant par eux-mêmes une valeur juridique, qui plus est le de premier rang, le recours aux principes généraux du droit n'est, pour autant que les premiers puissent s'identifier aux seconds, plus aussi nécessaire ». Voy. §30.

protection des données personnelles[1648]. Il est ainsi possible de souligner le constant dialogue entre les solutions adoptées par les deux Cours[1649]. Cependant, l'Union européenne s'est dotée d'un texte distinct de celui de la CEDH afin de mener à bien sa politique en matière de droits fondamentaux. Un mécanisme de cohérence est prévu afin d'articuler la protection des droits fondamentaux entre la CEDH et l'Union. Ainsi, les articles 52§2[1650] et 53[1651] de la Charte établissent une interaction entre l'Union européenne et la Convention européenne des droits de l'homme. Cette interaction permet de favoriser la communicabilité et la cohérence des normes européennes[1652] et d'enrichir la portée des droits fondamentaux en Europe[1653]. La CourEDH a elle aussi reconnu une protection équivalente des droits fondamentaux garantis par l'UE[1654]. Désormais, l'Union européenne reconnaît les droits fondamentaux et la Cour de justice demeure l'« architecte » de leur protection[1655]. Toutefois, la protection opérée par la Cour de justice ne correspond pas parfaitement à celle opérée par la CourEDH. En effet au contraire de la CourEDH, la Cour de justice doit concilier des intérêts contradictoires entre préservation des

1648 Sur le rapport entre Charte et CEDH voy.: arrêt CJUE, 26 fevrier 2013, aff. C-617/10, Åkerberg Fransson, § 44. Concernant leur rapport en matière de protection des données personnelles voy: Arrêt Tele2, § 127-129. Concernant la jurisprudence de l'article 8 CEDH, voy.S. BARTOLE, P. DE SENA, V. ZAGREBELSKI (a cura di), *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, p. 297 ss. Concernant la jurisprudence des deux cours en matière de protection des données perosnnelles voy. A. TERRASI, « Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo », in M. DI STEFANO S (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, p. 127 ss.

1649 Voy. CJUE, 9 novembre 2010, aff. Jointes C-92/09 e C-93/09, Volker und Markus Schecke GbR, Hartmut Eifert c. Land Hessen, § 59; CJUE, Digital Rights,§ 35; CJUE Tele2, §119 s. CEDH, 4 décembre 2015, Zakharov c. Russie, §147; CEDH, Szabo and Vissy v. Hungary, 12 janvier 2016, §23.

1650 Voy. article 52 §2 de la Charte : « Les droits reconnus par la présente Charte qui trouvent leur fondement dans les traités communautaires ou dans le traité sur l'Union européenne s'exercent dans les conditions et limites définies par ceux-ci. »

1651 Art. 53 de la Charte : « Aucune disposition de la présente Charte ne doit être interprétée comme limitant ou portant atteinte aux droits de l'homme et libertés fondamentales reconnus, dans leur champ d'application respectif, par le droit de l'Union, le droit international et les conventions internationales auxquelles sont parties l'Union, la Communauté ou tous les États membres, et notamment la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales, ainsi que par les constitutions des États membres. ». Selon A. PÊCHEUL, l'article 53 « institue sans doute une clause de sauvegarde puisqu'il stipule qu'en aucun cas la Charte ne peut être interprétée comme diminuant le contenu actuel de la Convention européenne » Voy. PÊCHEUL (A.), *La Charte des droits fondamentaux de l'Union européenne*, précité, spéc. p. 699.

1652 Voy. la thèse d'A. REMEDEM, *La protection des droits fondamentaux par la Cour de justice de l'Union européenne*, Université d'Auvergne - Clermont-Ferrand I, 2013, Francais.

1653 J. ANDRIANTSIMBAZOVINA, « L'enrichissement mutuel des droits fondamentaux en Europe », *R.F.D.A.*, 2002, pp. 124 et s. Cet enrichissement des droits fondamentaux se voit également favorisé par la multiplication des contentieux et l'invocation croissante de normes externes par les requérants.

1654 CEDH., 30 juin 2005, Bosphorus Airways c/ Irlande », CEDH 2005-VI ; J. ANDRIANTSIMBAZOVINA, « La Cour de Strasbourg, gardienne des droits de l'homme dans l'Union européenne ? Remarques autour de l'arrêt de Grande chambre de la Cour européenne des droits de l'homme, du 30 juin 2005, Bosphorus », *R.F.D.A.*, 2006 p. 560; F. BENOIT ROHMER, « Note A propos de l'arrêt Bosphorus Air Lines : L'adhésion contrainte de l'Union à la Convention », *R.T.D.H.*, 2005, pp. 827 - 584 ; V. CONSTANTINESCO, *C'est comme si c'était fait ?, C.D.E.*, n°2006-3/4, pp.363 - 378 ; S. DOUGLAS-SCOTT, *Note sous C.E.D.H., 30 juin 2005, Bosphorus Hava Yolları Turizm ve Ticaret Anonim Ş irketi (Bosphorus Airways) c/ Irlande*, Common Market Law review, 2006, p. 243 ; J.-P. JACQUÉ, « L'arrêt Bosphorus, une jurisprudence « Solange II » de la Cour européenne des droits de l'homme ? », *R.T.D.E.*, 2005, n°3, pp. 749 - 767 ; F. KAUFF-GAZIN, « L'arrêt Bosphorus : quand le juge de Strasbourg décerne au système communautaire un label de protection satisfaisante des droits fondamentaux », L.P.A., 24 novembre 2005, n°234, pp. 9 - 21.

1655 H. LABAYLE, « Architecte ou spectatrice ? La Cour de justice de l'Union dans l'Espace de liberté, sécurité et justice », *R.T.D.E.*, 2006, p. 1 et s .

droits fondamentaux et objectifs économiques et politiques de l'Union européenne[1656]. De plus, il existe une « hiérarchie variable, des sources des droits fondamentaux dans l'Union européenne » [1657] ce qui laisse persister une certaine disharmonie [1658] . Le droit de l'Union européenne ne s'immisce pas dans la mise en œuvre du droit de la Convention et, parallèlement, le droit conventionnel intervient avec prudence dans l'interprétation de la norme de l'Union européenne. En conclusion, alors que l'objectif de la Cour européenne des droits de l'homme est de garantir les droits fondamentaux tels qu'issus de la Convention, la Cour de justice n'est pas uniquement gardienne des droits fondamentaux. Néanmoins, on assiste à la constitution d'un socle commun en matière de protection des Droits de l'homme entre l'Union européenne et la Convention européenne des droits de l'homme. Le respect du droit fondamental à la protection des données personnelles ne peut donc s'établir que par des conceptions cohérentes des droits mis en œuvre par les deux ordres juridiques et par la suprématie de la norme la plus favorable en la matière. Cette complémentarité harmonise la protection des droits fondamentaux puisque dans un même domaine normatif coexistent différentes compétences aux origines diverses[1659]. Si la Cour de justice affirme son standard de protection, néanmoins, il reviendra à la Cour européenne des droits de l'homme d'unifier la protection et de fixer un standard largement commun aux juges nationaux et à la Cour de justice. Dès lors, peu importerait que le partage des responsabilités soit approximatif puisqu'en définitive la protection offerte serait sensiblement la même. Néanmoins, si le pouvoir du dernier mot reviendra certainement à la CourEDH, il ne faut pas négliger pour autant celui du premier mot qu'offre à la Cour de justice l'avantage de la procédure préjudicielle.

1656 Voy. par ex. CJUE Oméga aff. C-36/02, du 14 octobre 2004. Ici la Cour de justice a démontré la nécessité de concilier les droits fondamentaux avec les objectifs de l'Union européenne, elle n'a pas expressément exprimé l'idée selon laquelle le respect de la dignité de la personne humaine devait prévaloir sur la liberté de circulation. Voy. en ce sens : C. PRIETO, « La Liberté d'établissement et de prestation de services », R.*T.D.E.*, 2005, p. 867.

1657 J. GERKRATH, « Les principes généraux du droit ont-ils encore un avenir en tant qu'instruments de protection des droits fondamentaux dans l'Union européenne? », *R.A.E. – L.E.A.*, 2006/1, pp. 31-43, spec. p. 32. Pour l'auteur, les principes généraux du droit communautaire, la Convention européenne des droits de l'homme et la Charte des droits fondamentaux se voient attribués une valeur juridique variable.

1658 Voy. J. ANDRIANTSIMBAZOVINA, « Harmonie ou disharmonie de la protection des droits de l'homme en Europe : quelques considérations sur la jurisprudence de la Cour européenne des droits de l'homme depuis 2005 », *C.D.E.*, 2006/5-6, pp. 733 à 756 qui démontre que la pluralité peut ne pas être un préalable inconditionnel à une volonté d'homogénéité.

1659 J. ANDRIANTSIMBAZOVINA, « Harmonie ou disharmonie de la protection des droits de l'homme en Europe : quelques considérations sur la jurisprudence de la Cour européenne des droits de l'homme depuis 200 »5, *C.D.E.*, 2006/5-6, p. 751.préc.

§2. Des arrêts historiques confirmant l'autonomisation de la Cour de justice

193 Le rôle constitutionnel de la Cour de justice. S'il est vrai que la Cour de justice s'est appuyée pendant longtemps sur la Conv.EDH et sur les principes généraux de droit qu'elle a elle-même élaborés, la promotion des Droits de l'homme au rang de principes constitutionnels a entrainé une mutation de l'ordre juridique communautaire. C'est seulement avec la constitutionnalisation de la Charte des droits fondamentaux (son inscription dans le droit primaire) que le raisonnement de la Cour de justice se borne à des références à la ConventionEDH et à la jurisprudence de la CourEDH. De récents arrêts en matière de protection des données personnelles sont la parfaite illustration du passage d'une conception fonctionnelle à une conception constitutionnelle des droits fondamentaux[1660]. Ainsi, à partir de l'arrêt *Digital Rights Ireland* le raisonnement de la Cour de justice utilise la Charte des droits fondamentaux comme « boite à outils » pour mener à bien son contrôle. La Charte présente l'avantage de consacrer un droit spécifique à la protection des données personnelles alors que l'article 8 de la CEDH se réfère au droit au respect de la vie privée. La rétention et l'accès des autorités publiques aux données est l'un des aspects les plus controversés de la protection multi niveaux des droits fondamentaux, qui est soumise à une pondération avec les objectifs de sécurité dans le domaine de la prévention et de la lutte contre le terrorisme. La question de la conservation des données apparaît particulièrement emblématique en raison de la surveillance de masse dont elle peut faire l'objet. Ainsi, les opérateurs privés, souvent situés en dehors de l'Union, entrent en contact avec une énorme quantité de données personnelles qui peuvent concerner le contenu ou les métadonnées des communications électroniques. Dans ce domaine, la Cour de justice montre qu'elle souhaite consolider sa fonction de juge constitutionnel en tant que garant des droits fondamentaux. Pour ce faire, elle s'est fondée exclusivement sur la Charte en tant que norme de référence. Dans l'arrêt *Google Spain* la progressive autonomisation semble aboutie. Ici, le juge base son raisonnement sur la Charte et sur sa jurisprudence et exporte son modèle de protection vers le fournisseur de services Internet situés aux États-Unis (A). Ainsi on assiste à une amélioration du parcours de constitutionnalisation de la Cour de justice qui s'est formalisé et cristallisé dans le nouveau règlement sur la protection des données personnelles (B).

A. La Charte comme norme de référence

194 Des arrêts politiques. Depuis l'entrée en vigueur du traité de Lisbonne, la protection des données a été érigée en droit fondamental dans l'Union européenne et est désormais inscrite dans la Charte des droits fondamentaux de l'Union européenne, parallèlement au droit à la vie

1660 F. SUDRE et R. TINIERE, *Droit communautaire des droits fondamentaux*, éd Nemesis, Bruxelles, 2012, p. 17.

privée. Ainsi l'intégration de la Charte[1661] dans le droit primaire permet à la Cour de justice de s'affranchir de la jurisprudence de la CourEDH. Il importe d'observer que la Charte des droits fondamentaux n'a pas immédiatement fait partie de ce cadre de référence et que sa prise en considération par le juge communautaire est le résultat d'un lent processus. Ainsi, dans un premier temps, l'avocat général Tizzano estimait que la Charte était un instrument de référence utile puisqu'elle énonçait des droits qui étaient reconnus par ailleurs[1662].Cependant, dans une autre affaire, la Cour de justice insiste pour ne pas sous-estimer l'importance de la contribution de la Cour de Strasbourg, soulignant que, « l'examen de la validité des dispositions législatives ne doit être effectué qu'à la seule lumière de la Charte » [1663] . La Charte devient alors progressivement la norme de référence du contrôle de légalité par la Cour de justice et lui fournit la méthode pour procéder à ce contrôle. La Cour de justice, lorsqu'elle est appelée à évaluer la légitimité d'un acte de l'UE, se réfère aux articles 7 et 8 de la Charte. De même, lorsqu'elle doit évaluer la justification de l'ingérence dans les droits garantis par les articles 7 et 8 de la Charte, elle utilise comme grille d'analyse l'article 52 §1 de la Charte et non le paragraphe 2 de l'article 8 de la CEDH. Le juge vérifie alors si l'ingérence est prévue par la loi, si elle respecte le contenu essentiel du droit garanti, si la limitation est nécessaire et répond à des objectifs d'intérêt général reconnus par l'Union ou à un besoin de protection des droits et libertés d'autrui et si elle respecte le principe de proportionnalité. Dans l'affaire *Digital Rights*[1664] la Cour se réfère aux seuls articles de la Charte (articles 7 et 8[1665]) qui devient une source propre ; elle ignore l'article 8 CEDH et sa jurisprudence qui l'ont pourtant longuement inspirée. L'adoption de la directive 2006/24 relative à la rétention des données est apparue nécessaire au législateur européen dans le contexte de l'après 11 septembre 2001 et après les attentats terroristes de Madrid et de Londres. Elle a d'ailleurs été définie comme « l'une des

1661 À la différence de la Constitution, le traité de Lisbonne n'incorpore pas la Charte des droits fondamentaux, mais donne à celle-ci la même valeur que les traités.

1662 Il en concluait qu'il « est impossible d'ignorer les énonciations pertinentes de la charte ni surtout son évidente vocation à servir, lorsque les dispositions le permettent, de paramètre de référence substantiel … », Conclusions du 8 février 2001, BECTU, affaire C-173/99, rec. I-4851.

1663 CJUE, C 199/11, *Otis and Others*, par. 47, case C 398/13 P, *Inuit Tapiriit Kanatami*, par. 46 and case C-601/15 PPU, par. 46.

1664 Voy. L. BOLOGNINI, « Una sentenza politica che non stupisce », in *Formiche*, novembre 2015, p.50. Il est vrai que le contexte, tant politique que juridique, y était favorable. Ainsi, d'abord, les révélations d'E. Snowden ont sans doute joué un grand rôle, apprenant que, par le biais du système « Prism », la NSA (National Security Agency) et le FBI (Federal Bureau of Investigation) américains avaient directement accès aux données de communication de millions de citoyens, aussi bien américains qu'européens. Cet espionnage à grande échelle, qui plus est par un allié de l'Europe, n'a pas manqué de sensibiliser tout un chacun à la question de la protection de ses données à caractère personnel. Ensuite, une Charte des droits fondamentaux de l'Union, élevée au rang de droit primaire grâce au traité de Lisbonne, s'est révélée l'instrument idéal pour la Cour afin de jauger une directive limitant manifestement les droits garantis par celle-ci. La Cour axe l'ensemble de son raisonnement sur la Charte et sur elle seule, celle-ci lui fournissant à la fois sa « norme de référence » et sa grille d'analyse, donnant ainsi une autonomie inédite au juge de Luxembourg.

1665 La décision se caractérise d'une part par la distinction entre les articles 7 et 8 de la Charte ; d'autre part, dans l'application des limites qui relèvent de l'article 52§1 de la Charte, le juge n'avait jamais distingué l'application du principe de proportionnalité de celui de la violation du contenu essentiel des droits.

législations clés de l'Union en matière de lutte anti-terroriste »[1666]. La directive légitimait la rétention des données de connexion par les opérateurs de télécommunication ou les fournisseurs d'accès à Internet, permettant la collecte de métadonnées dans l'éventualité d'enquêtes à venir concernant la commission d'infractions graves. La Cour de justice a souligné le caractère sensible de ces données : « Ces données, prises dans leur ensemble, sont susceptibles de permettre de tirer des conclusions très précises concernant la vie privée des personnes dont les données ont été conservées, telles que les habitudes de la vie quotidienne, les lieux de séjour permanents ou temporaires, les déplacements journaliers ou autres, les activités exercées, les relations sociales de ces personnes et les milieux sociaux fréquentés par celles-ci[1667]. Ainsi la Cour de justice a considéré que l'ingérence que comporte la directive 2006/24 dans les droits fondamentaux consacrés aux articles 7 et 8 de la Charte s'avère « d'une vaste ampleur et qu'elle doit être considérée comme particulièrement grave »[1668]. Toutefois, les droits garantis par la Charte ne sont pas inconditionnels et son article 52§1 encadre les limitations possibles. Ainsi, la Cour de justice, en se référant à la Charte, estime que la législation de l'Union doit non seulement prévoir des règles claires et précises, mais également des garanties suffisantes contre le risque d'abus ainsi que contre tout accès et tout utilisation illicite de ces données. L'ingérence prévue par la directive 2006/24 est de vaste ampleur et elle n'est pas précisément encadrée[1669]. Le législateur de l'UE ne peut pas simplement se remettre aux États pour la définition des garanties qui doivent encadrer les limitations des droits fondamentaux. Ce raisonnement avait déjà été suivi par l'Avocat général qui avait souligné le rôle directeur que doit jouer « le législateur de l'Union dans la définition de ces garanties »[1670]. Dans l'affaire *Schrems,* la Cour affirme qu'une ingérence dans les droits fondamentaux garantis par les articles 7 et 8 de la Charte doit « prévoir des règles claires et précises régissant la portée et l'application d'une mesure et imposant un minimum d'exigences » notamment lorsqu'il existe un « risque important d'accès illicite à ces données »[1671] . Surtout, raisonnant par analogie avec l'arrêt *Digital Rights,* la Cour rappelle que la simple existence de législations autorisant la mise en œuvre de mesures de surveillance, sans qu'aucune « différenciation, limitation ou exception » ne soit opérée en fonction de l'objectif poursuivi et sans qu'aucun critère objectif permette de délimiter l'accès des autorités publiques aux données et leur utilisation ultérieure, constitue une violation grave à la protection des données personnelles[1672]. Enfonçant le clou, la Cour estime ainsi qu'une telle réglementation permettant « d'accéder de manière généralisée au contenu de communications électroniques » porte nécessairement atteinte au contenu essentiel de ces droits fondamentaux, tel que garantis par les articles 7 et 8 de la Charte[1673]. La prohibition de la

1666 V. N. VANDYSTADT, « Cour de justice : une directive antiterroriste sur la sellette », *Europolitics*, mardi 8 avril 2014, n°4846, p. 8.

1667 Voy. § 27 de la décision.

1668 Voy. §37 de la décision.

1669 Voy. §65 de la décision.

1670 Voy. §117 de ses conclusions.

1671 CJUE, aff. Schrems, §91.

1672 CJUE, aff. Schrems, §93.

1673 CJUE, Arrêt Schrems, §94.

surveillance de masse, fondée depuis l'arrêt *Digital Rights* sur le droit à la protection des données personnelles et le droit à la protection de la vie privée, est donc désormais ancrée dans les exigences conçues par la Cour comme « inhérentes à l'existence d'un État de droit ». Le processus d'autonomisation semble aboutir dans l'affaire *Google Spain* puisque la Cour de justice base son raisonnement sur la Charte et sur sa propre jurisprudence. De plus, l'interprétation de la Cour est audacieuse et consacre un droit à l'oubli numérique, même à l'encontre des conclusions de l'avocat général Niilo Jaaskinen. En effet, la possibilité d'obtenir l'effacement et la rectification des données personnelles indûment traitées figure explicitement dans le libellé de l'article 8 de la Charte et constitue désormais une exigence conditionnant le respect du contenu même du droit fondamental à la vie privée. La Cour a estimé qu'une personne peut demander l'effacement de données publiques devenues non pertinentes non pas uniquement au regard des articles 12 et 14 de la directive de 1995, mais plus largement et « eu égard à ses droits fondamentaux » au titre des dispositions de la Charte. La Cour de justice dans les affaires *Digital Ireland*[1674], *Google Spain*[1675] et *Schrems*, a joué un rôle fondamental dans l'élargissement de la protection offerte aux données personnelles. La Cour axe l'ensemble de son raisonnement sur la Charte, celle-ci lui fournissant à la fois sa norme de référence et sa grille d'analyse. La nouvelle architecture devra ainsi se confronter avec la CEDH lors de l'adhésion de l'UE prévue par l'article 6§2 TUE[1676] ; la Cour européenne des droits de l'homme sera incontestablement le chef d'orchestre et aura la charge de « garantir l'harmonie entre la Convention et la Charte, en contrôlant l'interprétation de la Convention faite par le juge communautaire à l'occasion de l'application de la Charte »[1677].

B. La cristallisation de la jurisprudence de la Cour de justice

195 Le partage de responsabilité entre le juge et le législateur de l'Union. La jurisprudence de la Cour de justice dans l'affaire *Schrems* est désormais codifiée dans la RGPD. En effet, selon les dispositions du RGPD « l'Union ou un État membre peut restreindre, par des mesures législatives, la portée des obligations et des droits (...), si cette limitation respecte l'essence des droits et libertés fondamentales et constitue une mesure nécessaire et proportionnée dans une société démocratique pour sauvegarder les objectifs d'intérêt général de l'Union ou d'un État membre »[1678]. Les principales indications données par la Cour de justice aux législateurs

1674 CJUE, Digital Rights Ireland Ltd c. Minister for Communications, aff. Jointes C-293/12 et C-594/12, 8 avril 2014. Voy. T. KONSTANDINIDES, « Destroying Democracy on the Ground of Defending It ? The Data Retention Directive, the Surveillance State and Our Constitutional Ecosystem », in *Eur. L. Rev*., 2011, 722.

1675 CJUE, 13 maggio 2014, *Google Spain* SL e Google Inc. c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, causa C-131/12.

1676 Voy. sur l'adhésion de l'UE à la CEDH, l'avis négatif de la CJUE 2/13 du 18 décembre 2014, www.curia.europa.eu.

1677 F. SUDRE, *L'adhésion de l'Union Européenne à la Convention européenne des droits de l'homme*, Annuaire de droit européen, 2006, p. 76.

nationaux et à ceux de l'Union concernent l'équilibre entre la poursuite du but légitime de la sécurité dans la mesure du strict nécessaire et en respectant le principe de proportionnalité, de l'effectivité des recours, du rôle des autorités indépendantes et, dans la mesure du possible, dans le cadre pénal, de l'existence de l'information et du consentement des personnes concernées. De plus, l'RGPD a calqué la jurisprudence *Google Spain* et a codifié le modèle d'application territorial de la protection des données personnelles. Ainsi, le droit de l'Union s'applique aux traitements des données à caractère personnel effectués dans le cadre des activités d'un établissement, d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. De plus le règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées, qui se trouvent sur le territoire de l'Union, par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes, ou au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union[1679]. Par rapport au texte de la directive 95/46, la référence au « territoire de l'État membre » a été remplacée par l'exigence que ce traitement soit effectué « dans l'Union ». Le législateur a décidé d'exclure cette référence, considérant que les dispositions du règlement sont d'application uniforme sur tout le territoire de l'Union. Sur le plan des rapports externes à l'Union européenne, les indications de la Cour de justice ont déjà conduit à la conclusion de nouveaux accords internationaux plus respectueux de cet équilibre[1680], tandis qu'au niveau interne, le remplacement de la directive sur la conservation des données (invalidée dans l'affaire *Digital Rights Ireland*) rencontre une résistance de la part du législateur européen dans la révision des communications électroniques [1681]. De plus, le droit à l'effacement ou à l'oubli consacré dans l'arrêt *Google Spain* est désormais codifié à l'article 17 du RGPD. Dans l'affaire *Tele2*, la Cour donne des indications précises aux législateurs nationaux afin d'éliminer l'incompatibilité constatée avec la Charte. Selon la Cour de justice, la législation nationale peut permettre, à titre préventif, la rétention ciblée de données à des fins de lutte contre les infractions graves, mais à condition que cette conservation soit limitée au strict nécessaire en ce qui concerne les catégories de données, les moyens de communication concernés, les personnes impliquées ainsi que la durée prévue. Enfin, la Cour a souligné que la législation nationale doit prévoir la conservation des données en question sur le territoire de l'Union et leur destruction irréversible à la fin de la période de stockage. Ces indications semblent particulièrement contraignantes, ce qui explique les difficultés rencontrées par le législateur européen dans la mise en œuvre de la décision en question, dans l'élaboration d'une nouvelle directive sur la conservation des données et dans la proposition de réforme de la directive *e-privacy*. Plusieurs autres actes législatifs nationaux et de l'Union présentant des

1678 Selon l'RGPD, les limitations possibles portent sur : la sécurité publique « et » la prévention, la recherche, la détection et la poursuite d'infractions pénales ou l'exécution de sanctions pénales, y compris la prévention des menaces à la sécurité publique (Art. 23, lettres c et d).

1679 Voy. article 3§2 du RGPD.

1680 Voy. l'accord *Privacy Shield* qui a remplacé l'accord *Safe Harbor* suite à l'arret *Schrems* de la Cour de justice.

1681 Council of European Union, doc. 10098/17 of 6 November 2017, Eurojust Report, Data Retention regimes in Europe in light of the CJEU ruling of 21 December 2016 in Joined Cases C-203/15 and C-698/15.

« défauts de fabrication » très similaires pourraient être soumis au jugement de la Cour de justice prochainement. Entre-temps, de tels actes doivent continuer à être interprétés par les juridictions nationales conformément aux indications en question[1682]. Ainsi la Cour de justice confirme ici son rôle normatif, puisque « c'est principalement la Cour de justice qui détient les moyens juridiques permettant de définir puis de renforcer le système juridique de la Communauté européenne. La mission du juge n'est donc plus comprise uniquement en rapport avec la garantie des libertés offertes par un système juridique donné, c'est-à-dire le respect des droits et obligations qui en découlent. La Cour de Luxembourg, pour des raisons spécifiques à l'ordre d'intégration, sera dans le même temps amenée à définir ces droits et ces obligations avant qu'elle n'ait à assurer leur respect, en d'autres termes, le recours à des normes jurisprudentielles est justifié par les prémisses initiales contenues dans les traités, alors même que ce juge ne disposait pas toujours des instruments susceptibles de poursuivre la réalisation des objectifs fixés ou rendait ces derniers dépendants d'appréciations distinctes voire divergentes »[1683]. Ainsi, les décisions juridictionnelles ne sont pas purement déclaratives mais participent à la création du droit. Comme le souligne Hans KELSEN, l'office du juge ordinaire ne se limite pas simplement à dire le droit selon la conception de Montesquieu. Au contraire, le juge détient un pouvoir normatif sur les normes qu'il a à appliquer, et la loi « *jusqu'à Intervention du juge n'a de sens vrai ni de sens faux. C'est l'interprétation authentique qui lui donne un sens et lui confère par-là la signification objective d'une norm*e »[1684] .Une Cour constitutionnelle, en interprétant la Constitution, en choisissant de donner un sens à une disposition plutôt qu'à une autre, participe à l'élaboration de normes constitutionnelles et peut pallier les insuffisances normatives matérielles des normes constitutionnelles. A l'instar d'une Cour constitutionnelle, la Cour de justice dispose d'un pouvoir normatif car elle a le monopole de l'interprétation authentique du droit de l'Union européenne.

1682 Voy. G. CAGGIANO, L »a Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali », Studi sull'integrazione europea, 2018, fasc.1., p. 3 et ss.

1683 C. MAUBERNARD, *Les normes juridiques de la jurisprudence de la Cour de justice des Communautés européennes, contribution à l'étude du pouvoir judiciaire communautaire*, Thèse université de Montpellier I, 2001, p. 5.

1684 M. TROPER, « Le problème de l'interprétation et la théorie de la supra légalité constitutionnelle », in Recueil d'études à la mémoire de Charles Eisenmann, éd. Cujas, 1975, p.149.

CONCLUSION DU CHAPITRE II

La construction du droit fondamental à la protection des données personnelles est la combinaison de deux facteurs : d'un côté, l'entrée en vigueur du traité de Lisbonne reconnaissant la force contraignante de la Charte des droits fondamentaux de l'Union européenne et de l'autre, les développements de la jurisprudence de la Cour de justice. Le présent chapitre a analysé le rôle de la Cour de justice comme gardienne du droit fondamental à la protection des données personnelles, et son émancipation vis-à-vis de la CourEDH.

La mission de sauvegarde et d'interprétation de la Cour de justice de l'Union, si elle s'apparente à de nombreux égards à celle exercée par un juge constitutionnel, ne saurait lui être pleinement confondue. En effet, s'exerçant sur des objets distincts du constitutionnalisme classique et outrepassant parfois les prérogatives d'une Cour constitutionnelle nationale[1685], l'office du juge de l'Union sort des sentiers prédéterminés. La comparaison mérite d'être analysée en raison de l'exercice de deux autres fonctions emblématiques, très proches de celles exercées par une Cour constitutionnelle nationale, à savoir le monopole dans l'interprétation des traités en tant que norme suprême et le contrôle de validité des actes de droit dérivé avec le droit primaire de l'Union européenne. Le droit à la protection des données personnelles a connu des développements qui lui ont garanti un « fabuleux destin »[1686]. La Cour de justice a su intégrer les méthodes et les outils du raisonnement de la CourEDH pour ensuite les importer dans l'ordre juridique de l'Union. Avec l'inscription de la Charte dans le droit primaire, établissant un droit spécifique à la protection des données, la Cour de justice s'est progressivement émancipée à l'égard de la jurisprudence de la CourEDH. Elle joue ainsi un rôle de juge constitutionnel en tant que gardienne des droits fondamentaux, tout en participant également à l'élaboration de normes.

La gouvernance de la Cour de justice en matière de protection des données personnelles est réaffirmée dans des arrêts historiques marquant l'abandon de toute référence à la CEDH et aux principes généraux de droit en faveur d'une grille d'analyse constituée uniquement par la Charte des droits fondamentaux. De plus, on assiste à une amélioration du parcours constitutionnel de la Cour de justice qui s'est formalisé dans le nouveau Règlement sur la protection des données personnelles intégrant la jurisprudence de la Cour de justice en matière de protection des données personnelles.

1685 Comme relevé par H. GAUDIN, le rôle d'un juge constitutionnel n'est, en effet, pas de se substituer au pouvoir constituant, il est simplement de lui servir d'aiguillage. Ainsi, la Cour de justice outrepasserait l'office d'un juge constitutionnel national puisque le pouvoir constituant ne pourrait contredire une de ses jurisprudences», Voy. H. GAUDIN, *La Cour de justice, juridiction constitutionnelle ?* p.216.

1686 J. ZILLER, « Le fabuleux destin des Explications relatives à la charte des droits fondamentaux de l'Union européenne », *in Chemins d'Europe-Mélanges, Jean-Paul Jaqué, Paris*, Dalloz 2010.

Dans l'analyse des limites des droits garantis, la Cour de justice fonde son raisonnement sur l'article 52§1 de la Charte et non plus l'article 8 §2 de la CEDH. La Charte devient alors la seule grille d'analyse de la CJ, et la protection des données personnelles a, avant tout, obtenu une valeur constitutionnelle[1687]. De plus, le législateur dispose désormais d'une voie tracée par la Charte et par le juge. On est passé de l'affirmation simplement législative et jurisprudentielle, à la constitutionnalisation[1688] de ce droit devenu fondamental. Le rôle central dans la défense des droits fondamentaux est désormais joué par la Cour de justice[1689]. Le présent chapitre a démontré l'impact de l'inscription du droit à la protection des données personnelles sur l'ordre juridique de l'Union européenne[1690] dans la Charte des droits fondamentaux.

La constitutionnalisation de la Charte, c'est-à-dire la consécration de la Charte des droits fondamentaux dans le droit primaire, a permis à l'article 8, garantissant la protection des données personnelles, de doter l'Union européenne d'un droit fondamental spécifique distinct du droit au respect de la vie privée et familiale[1691]. Ainsi la proclamation puis, seulement en décembre 2009, l'entrée en vigueur de la Charte, et en particulier la portée de ses articles 7 et 8, ont déterminé l'incompatibilité d'actes juridiques de l'UE, initialement compatibles avec le droit de l'Union, en raison de leur « relecture » à la lumière du nouveau paramètre. Dans le domaine de la protection des données personnelles, le rôle de la Cour de justice de l'Union européenne comme « gardienne constitutionnelle » semble désormais central et stratégique, non seulement au niveau européen, mais aussi mondial. En effet, non seulement la CJUE a joué le rôle de recours suprême au sein de l'Union pour sauvegarder l'intégration supranationale, mais elle a également joué un rôle important dans la recherche de l'équilibre entre le respect des droits fondamentaux et l'intérêt général de la sécurité. Cela à travers l'évaluation de la nécessité et de la proportionnalité des mesures prises aux niveaux européen et national. La reconnaissance de la Charte des droits fondamentaux en tant que source du droit primaire a contribué de manière décisive aux derniers développements de sa jurisprudence en la matière.

1687 Le droit à la protection des données à caractère personnel, bénéficie d'un ancrage « constitutionnel », grâce au traité de Lisbonne. L'affirmation symbolique et juridique de ses valeurs par l'Union européenne donne en effet, par la mê me, un nouvel élan à la Cour de justice, tout en facilitant son office. L'idée qui émerge est celle d'une Charte des droits fondamentaux devenue norme de référence du contrô le opéré par la Cour de justice, permettant à celle-ci de s'affirmer en tant que juge « constitutionnel », garant des droits fondamentaux. La Cour axe l'ensemble de son raisonnement sur la Charte et sur elle seule, celle-ci lui fournissant à la fois sa « norme de référence » et sa grille d'analyse, donnant ainsi une autonomie inédite au juge de Luxembourg.

1688 J.M. SAUVÉ, *La protection des droits fondamentaux au niveau de l'Union européenne et des États membres*, propos introductifs au XXVe Congrès de la Fédération internationale de droit européen (FIDE), Tallin, 30 mai-2 juin 2012.

1689 G. GONZALES FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Springer International Publishing, 2014, p 142 ; S. CARRERA, M. De SOMER, B. PETKOVA, *The Court of Justice of the European Union as a Fundamental Rights Tribunal Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom*, Security and Justice, paper 49, agosto 2012, p 73. Voy. également H. LABAYLE, « La Cour de justice et la protection des données : quand le juge européen des droits fondamentaux prend ses responsabilités », disponible à l'adresse : www.gdr-elsj.eu del 9 aprile 2014. J.P. JAQUE, « Protection des données personnelles, Internet et conflits entre droits fondamentaux devant la Cour de justice », in *Rev. Trim. dr. europ*., 2014, p. 283 ss.

1690 Charte des Droits fondamentaux, article 51§1 « Les dispositions de la présente Charte s'adressent aux institutions et organes de l'Union dans le respect du principe de subsidiarité, ainsi qu'aux États membres uniquement lorsqu'ils mettent en œuvre le droit de l'Union. En conséquence, ils respectent les droits, observent les principes et en promeuvent l'application, conformément à leurs compétences respectives ».

1691 Voy. l'article 7 de la Charte.

Il apparaît que le défi que représente la délimitation du champ de la protection des données personnelles naît d'un processus constant d'extension de l'identité et de l'intégration de l'union européenne.

CONCLUSION DU TITRE I

Alors que Montesquieu considérait que les juges ne sont que « la bouche qui prononce les paroles de la loi, des êtres inanimés qui n'en peuvent modérer la force, ni la rigueur »[1692], il a été souligné comment les juges de Luxembourg et de Strasbourg ont su aller au-delà des textes pour faire évoluer le droit. En particulier, l'ouverture du droit de l'Union européenne aux droits fondamentaux est le fruit de l'œuvre de son juge. Afin d'établir une protection harmonieuse et cohérente du droit fondamental à la protection des données, le dialogue des juges constitue un élément essentiel. Il en résulte une pluralité d'espaces juridiques variables dans leurs circonscriptions territoriales, et également distincts quant à leurs objectifs et au caractère impératif des régulations qui en émanent. L'Europe prend de plus en plus la dimension d'un réseau au sein duquel s'élabore une inter normativité visant à assurer un dialogue entre différents ordres juridiques capables de générer des effets non seulement sur le territoire européen mais partout où il existe des interconnexions[1693]. Il est possible de remarquer que les droits fondamentaux ont été à l'origine de ce dialogue stratégique de la Cour de justice et de la Cour européenne des droits de l'homme. Les interactions entre les deux ordres juridiques entraînent des répercussions quant à la conception des droits fondamentaux. Ainsi, la future adhésion de l'Union européenne à la Convention européenne des droits de l'homme devrait clarifier les interactions entre les deux ordres juridiques et la protection des droits fondamentaux. L'Union européenne a établi une politique spécifique de protection des droits fondamentaux qui se veut cohérente avec celles mises en œuvre tant par les États que par la Convention européenne des droits de l'homme [1694] . Le droit à la protection des données personnelles n'est pas un droit absolu, il peut se voir limité face à des intérêts généraux ou droits d'autrui. Concernant les limitations au nom de l'intérêt général, les ordres juridiques européens imposent que les restrictions au droit fondamental à la protection des données personnelles soient entourées de garanties tant formelles que matérielles. Les garanties matérielles concernent le contenu des restrictions elles-mêmes et se traduisent dans le principe de proportionnalité tandis quel les garanties formelles concernent la prévisibilité des restrictions. Néanmoins, dans le contrôle sur le respect du droit fondamental à la protection des données, il reste des différences quant au raisonnement des juges de Luxembourg et de Strasbourg. L'étude de l'application des justifications formelles a montré que le contrôle effectué par la CourEDH est plus étendu que celui effectué par la Cour de justice, ce dernier se traduisant souvent par une simple vérification de l'existence d'une base légale et comme le

1692 MONTESQUIEU, *De l'esprit des lois*, Livre XI, Chapitre VI, « De la Constitution d'Angleterre », GF Flammarion, Paris, 1979, p. 301.

1693 K. BENYEKHLEF, *Une possible histoire de la norme*, Montreal, Éditions Thémis, 2008, p. 728.

1694 Cette coherence est garantie grace au recours aux articles 52 §3 et 53 de la Charte. Voy. aspect A. PÊCHEUL, « La Charte des droits fondamentaux de l'Union européenne », *R.F.D.A.*, 2001, p. 688 et s.

démontre la jurisprudence récente, parfois le juge ne se penche même pas sur la question[1695]. Ainsi, l'importance du contrôle formel dans l'ordre juridique de l'Union européenne semble moindre. Diversement, pour la CourEDH, la condition de l'existence d'une base légale encadrant l'ingérence a souvent constitué un moyen suffisant pour conclure à la violation de la CEDH sans avoir besoin de se prononcer sur le fond de l'affaire. Elle a ainsi développé le principe de « qualité de la loi » qui a été repris par la jurisprudence de la Cour de justice[1696]. Concernant le contrôle matériel, l'étude de l'application du principe de proportionnalité montre plusieurs degrés de contrôle. La Cour européenne des droits de l'homme exerce un contrôle qui va de l'absence de marge nationale d'appréciation à la vérification que l'ingérence de l'État n'est pas déraisonnable alors que le contrôle opéré par la Cour de justice comporte plusieurs degrés et exige que les mesures restrictives afin de réaliser les objectifs légitimes prévus par la réglementation considérée, « ne dépassent pas les limites de ce qui est approprié et nécessaire à la réalisation de ces objectifs »[1697]. De plus, « l'étendue du pouvoir d'appréciation »[1698] du législateur de l'Union peut être limitée, en fonction de la nature du droit garanti, ainsi que de la nature, la gravité et la finalité de l'ingérence. Cela souligne la capacité du juge de Luxembourg à graduer et renforcer la protection face à l'augmentation et à l'aggravation des atteintes. L'analyse des affaires dans lesquels le triple test de proportionnalité est appliqué, a montré que ledit contrôle est pour la plupart limité. Seuls des motifs liés à la nature particulièrement sensible des données ou aux atteintes particulièrement graves peuvent justifier un contrôle de proportionnalité approfondi *stricto sensu*. Par ailleurs, le droit à la protection des données personnelles peut faire l'objet de mesures de limitation non seulement provenant de l'État mais également des restrictions provenant de la mise en balance avec les droits et intérêts d'autrui. Le droit à la protection des données n'est ni absolu ni intangible et doit être mis en balance avec d'autres droits, dont le droit à la protection de la propriété intellectuelle, la liberté d'entreprise des fournisseurs de services de télécommunication électronique et à la liberté d'expression.

1695 Voy. Les Conclusions de l'Avocat général P. CRUZ VILLALON, 12 décembre 2013, affaires Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C 293/12 et C 594/12 dans lesquelles il se penche sur une analyse détaillée de l'existence de la base légale de la directive 24/2006. Analyse laissée de coté par la Cour de justice dans ses motivations.

1696 Voy. Affaire CJCE, 20 mai 2003, Rechnungshof c. Österreichischer Rundfunk et autres, aff. C-465/00, C-138/01, C-139/01, §77-79.

1697 Voy. §46 de la décision Digital Rights.

1698 Voy. §47 de la décision Digital Rights.

TITRE II. L'ADJONCTION D'UNE PROTECTION NON- JURIDICTIONNELLE

196 Des autorités de contrôle indépendantes inscrites dans le droit primaire de l'Union. Il convient de s'intéresser aux acteurs non juridictionnels qui contribuent à l'élaboration des normes européennes et qui participent à la mise en œuvre du droit à la protection des données personnelles. En effet, le droit fondamental à la protection des données personnelles légitime l'intervention dans le processus normatif d'autres acteurs que le législateur et le juge. L'intervention de ces autres acteurs est alors susceptible de renforcer l'efficacité de la protection [1699] . L'architecture de la protection des droits fondamentaux s'est développée progressivement dans l'Union européenne et elle continue d'évoluer. Ainsi, la protection des droits fondamentaux se voit complétée par diverses institutions quasi juridictionnelles qui méritent d'être étudiées puisqu'elles témoignent de la volonté de l'Union européenne d'établir une politique générale en faveur de ces droits[1700] et par des acteurs qui relèvent de la société civile.

Depuis l'entrée en vigueur du Traité de Lisbonne, le droit à la protection des données personnelles a été élevé au rang de droit primaire[1701]. Par ailleurs, en vertu de l'article 8 §3 de la Charte[1702] : « le respect des règles est soumis au contrôle d'une autorité indépendante » tout comme et en vertu de l'article 16 §2 TFUE : « le respect des règles est soumis au contrôle d'une autorité indépendante ». Grace à l'article 8 de la Charte et à l'article 16 TFUE, les autorités de contrôle nationales ont une valeur para-constitutionnelle, elles sont inscrites dans le droit primaire de l'Union. Ainsi, les autorités de protection des données à caractère personnel des États membres s'inscrivent dans une coopération et une synergie avec d'autres gardiens des droits fondamentaux au sein de l'Union européenne. Au niveau européen, l'article 41[1703] du règlement n° 45/2001 institue le Contrôleur européen de la protection des données (CEDP) qui veille sur le traitement de données personnelles par les institutions, organes et organismes de l'Union. L'étude de ces acteurs quasi juridictionnels montre l'architecture émergente des droits

1699 Voy. Thèse Deabaets.

1700 P. ALSTON, J.-H.H. WEILER, « Vers une politique des droits de l'homme authentique et cohérente pour l'Union européenne », in P. ALSTON (sous la dir.), *L'Union européenne et les droits de l'homme*, Bruxelles, Bruylant, 2001, pp. 7 et s.

1701 Conformément à l'article 6 du Traité sur l'Union européenne (TUE), la Charte des droits fondamentaux de l'UE a « la même valeur juridique que les traités ».

1702 Selon l'article 8 de la Charte des droits fondamentaux de l'UE1702 : « 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Ces données doivent être traitées loyalement, à des fins déterminées et sur l a base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. Le respect de ces règles est soumis au contrôle d'une autorité indépendante ». Pour un commentaire sur l'article 8 de la Charte, voy. : « Commentary of the Charter of Fundamental Rights of the EU », Réseau UE d'experts indépendants en matière de droits fondamentaux, juin 2006, p. 90, disponible à l'adresse : http://ec.europa.eu/justice_home/doc_centre/rights/charter/docs/network_ commentary_fi nal %20_180706.pdf.

1703 En particulier, l'article dispose que le CEDP a pour fonction de « conseiller l'ensemble des institutions et organes communautaires, soit de sa propre initiative, soit en réponse à une consultation pour toutes les questions concernant le traitement de données à caractère personnel, en particulier avant l'élaboration par ces institutions et organes de règles internes relatives à la protection des libertés et droits fondamentaux des personnes à l'égard du traitement des données à caractère personnel ».

fondamentaux au sein de l'Union européenne [1704] . Parmi les acteurs qui contribuent à l'élaboration des normes en matière de données personnelles, on retrouve notamment les autorités administratives de contrôle établies dans chaque État membre et la société civile (Chapitre I), mais aussi au niveau européen le groupe de travail de l'art. 29 (le G29) qui a contribué à l'élaboration d'un droit souple avec l'adoption des avis, recommandations et autres documents, auquel se substitue le Comité européen pour la protection des données personnelles et, depuis 2001, le Contrôleur européen de la protection des données (CEDP) qui veille sur le traitement de données personnelles par les institutions, organes et organismes de l'Union (Chapitre II).

1704 Agence des droits fondamentaux de l'union européenne, « La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données. Renforcement de l'architecture des droits fondamentaux au sein de l'UE II », Luxembourg, Office des publications de l'Union européenne, 2012, 50 p.

CHAPITRE I. LA PROTECTION NON-JURIDICTIONNELLE AU SEIN DES ÉTATS MEMBRES

197 La différence avec d'autres acteurs intervenants dans la protection des droits fondamentaux. Le droit fondamental à la protection des données personnelles légitime l'intervention d'autres acteurs tels que le législateur et le juge. Ces acteurs participent à l'élaboration et à la mise en œuvre des normes juridiques relatives à l'utilisation des données personnelles. Toutefois la mise en œuvre de ce droit et son effectivité ont légitimé la création d'autorités de contrôle nationales[1705]. Afin de comprendre le rôle des autorités de contrôle indépendantes au sein des États membres, il convient de citer une autre autorité chargée d'assurer la bonne application des droits au niveau européen. Il s'agit de l'Agence des droits fondamentaux créée par règlement 168/2007 du Conseil du 15 février 2007[1706]. Elle réalise des études et elle met au point des informations quant à la situation au regard du respect effectif des droits fondamentaux. Elle interagit de manière non formalisée, avec des instances décisionnelles, en fournissant des avis aux institutions de l'Union et aux États membres lorsqu'ils mettent en œuvre le droit de l'UE[1707]. Enfin, l'Agence interagit avec les titulaires des droits fondamentaux en assurant la communication et la promotion des droits auprès de la société civile. L'Agence relève du type « agence d'information » [1708] , elle n'est donc pas compétente pour adopter des actes juridiques contraignants à la différence des agences de régulation et en particulier des autorités de contrôle en matière de protection des données à caractère personnel. Elle est, selon la doctrine, le reflet d'une volonté d'approfondir la valorisation des droits fondamentaux au sein de l'Union européenne[1709]. À la différence de l'Agence des droits fondamentaux, les autorités de contrôle en matière de protection des données à caractère personnel sont ancrées au niveau du droit primaire de l'UE[1710]. Les autorités de contrôle en matière de protection des données personnelles constituent les seules autorités

1705 A. BALTHASAR, Complete Independence of National Data Protection Supervisory Authorities – Second Try: Comments on the Judgment of the CJEU of 16 October 2012, C-614/10 (European Commission v. Austria), with Due Regard to its Previous Judgment of 9 March 2010, C-518/07 (European Commission v. Germany) in *Utrecht Law Review*, 2013, p. 26 ss.; S. PEERS, The CJEU confirms the independence of data protection authorities in EU Law Analysis, 9 April 2014, disponibile *online*; O. LYNSKEY, *The Europeanisation of data protection law*, in *Cambridge Yearbook of European Legal Studies*, 2016, p. 1 ss.; S. DE SOMER, *Autonomous Public Bodies and the Law, A European Perspective*, Cheltenham, 2017.

1706 Aux termes de l'article 3 du règlement 168/2007, l'Agence exécute ses tâches dans le cadre des compétences de l'UE et n'examine les questions relatives aux droits fondamentaux dans les États membres que lorsqu'ils « mettent en œuvre le droit de l'UE ».

1707 Voy. Par ex. le rapport du 214 de l'Agence dans le domaine de la protection des données personnelles consacré aux voies de recours en matière de protection des données personnelles dans les États membres.

1708 Par opposition aux « agences de régulation » qui sont investies du pouvoir d'adopter des actes juridiquement contraignants à l'égard de personnes physiques ou morales dans le domaine spécifique.

1709 A. ILIOPOULOU, « Assurer le respect et la promotion des droits fondamentaux : un nouveau défi pour l'Union européenne », *CDE* 3-4/2007, p. 458 et s.

1710 Depuis l'entrée en vigueur du Traité de Lisbonne, le droit à la protection des données personnelles est élevé de ce qui était du droit dérivé préexistant au rang du droit primaire. En vertu de l'article 8 §3 de la Charte « le respect des règles est soumis au contrôle d'une autorité indépendante » et l'article 16 §2 TFUE dispose que « le respect des règles (fixées par le législateur) est soumis au contrôle d'une autorité indépendante.

citées dans la Charte des droits fondamentaux, elles ont donc un rang para-constitutionnel. Le droit de l'Union garantit donc l'existence de « nouveaux acteurs » ayant pour mission de renforcer les droits fondamentaux. Le présent chapitre analyse les problèmes et les pratiques encourageantes relatives aux systèmes de protection des données de l'Union[1711] et au rôle crucial des acteurs institutionnels et non institutionnels dans la mise en œuvre du droit à la protection des données personnelles. L'étude englobe une évaluation de leur efficacité, de leur fonctionnement et de leur indépendance. En effet, la protection des données à caractère personnel n'exige pas simplement que les institutions de l'UE ou les organes des États membres s'abstiennent de toute interférence illégale dans les données personnelles. Il existe également une obligation positive de garantir la protection des données à caractère personnel. L'UE et ses États membres doivent prévoir une ou plusieurs autorités indépendantes chargées de surveiller l'application des dispositions relatives aux données à caractère personnel. Ces autres acteurs qui participent à l'élaboration et à la mise en œuvre de normes concernant la protection des données personnelles sont de deux types. Il s'agit non seulement d'acteurs institutionnels (section I) mais aussi d'acteurs non-institutionnels (section II).

1711 Sur la consécration des autorités de contrôle par le droit primaire : L. COUDRAY, *La protection des données personnelles dans l'Union européenne*, Sarrebruck, 210, p. 316.

Section I. Le rôle des autorités nationales de protection des données personnelles

198 L'origine des autorités de contrôle. Les autorités de protection des données sont un élément crucial de l'architecture du droit fondamental à la protection des données personnelles car elles contribuent à stimuler le développement des systèmes de protection cohérents et effectifs dans les États membres. Les autorités de contrôle se rattachent à la catégorie des autorités administratives indépendantes. Historiquement, les autorités administratives indépendantes sont nées en Amérique du nord à la fin du XIXe siècle, bien que les pays scandinaves fassent valoir que dès le début de ce XIXe siècle des organismes semblables à ce que nous appelons des autorités administratives indépendantes avait été créés. Dans la plupart des pays européens, les autorités administratives indépendantes apparaissent au cours de deux vagues successives, l'une dans les années 1970, l'autre dans les années 1990, la seconde vague concernant en particulier les pays d'Europe centrale et orientale[1712]. Il existe une multitude d'autorités administratives indépendantes, tant au niveau économique qu'au niveau de la protection des droits et des libertés. Leurs domaines d'activité sont aussi divers que leurs règles de composition et de fonctionnement, ou que leurs pouvoirs. Cette diversité résulte de l'adaptabilité des autorités administratives indépendantes à leurs missions. Leur essor répond à une volonté de distinguer, à côté des administrations traditionnelles, des organes dotés, pour l'accomplissement de leur mission, de garanties d'indépendance particulières par rapport au pouvoir exécutif. Les autorités administratives indépendantes ont en commun « d'agir au nom de l'État sans être subordonnées au gouvernement et de bénéficier, pour le bon exercice de leurs missions, de garanties qui leur permettent d'agir en pleine autonomie, sans que leur action puisse être orientée ou censurée, si ce n'est par le juge »[1713]. La spontanéité qui caractérise leur institution est l'une des principales raisons de l'hétérogénéité des pouvoirs et des disciplines qui distinguent ces matières institutionnelles. Malgré leur hétérogénéité [1714] , elles ont en commun l'indépendance qui leur est accordée afin de mettre en œuvre leur tâche. Il s'agit d'autorités administratives qui ont été créées pour éviter une intervention directe de l'État dans des secteurs sensibles[1715].

1712 Voy. L'étude dirigée pour l'Office du Senat par J.-M. PONTIER.

1713 Voy. Rapport public 2001 du Conseil d'État disponible sur : http://www.conseil-etat.fr/Decisions-Avis-Publications/Etudes-Publications/Rapports-Etudes/Les-autorites-administratives-independantes-Rapport-public-2001

1714 P. GELARD, Les *autorités administratives indépendantes : évaluation d'un objet juridique non identifié.* Tome 1, Rapport, disponible à l'adresse : https://www.senat.fr/rap/r05-404-1/r05-404-1.html

1715 N. DECOOPMAN, « À propos des autorités administratives indépendantes et de la déréglementation », in J. CLAM, G. MARTIN, *Les transformations de la régulation juridique, LGDJ*, coll. Droit et Société, n° 5, Paris, 1998, pp. 249 et s., sp. p. 249 : « L'intervention des autorités administratives indépendantes – créées pour éviter une intervention directe de l'État dans des secteurs sensibles (informatique, communication, bourse…) et rendus complexes par l'évolution technologique et la mondialisation des échanges – peut s'analyser comme une forme de déréglementation si on entend par là dans un sens large un allégement des contraintes étatiques, un désengagement de l'État central au profit de modes d'intervention plus souples, plus indirects ». La création des AAI motivée par la volonté de leur confier le règlement de questions dont le Gouvernement ne voulait pas assumer la responsabilité politique ne paraît concerner qu'une faible minorité d'entre elles. Les autorités administratives indépendantes apparaissent plutôt comme une nouvelle façon de gouverner, favorisant la transparence, la consultation et la négociation.

L’institution de telles autorités s’explique à la fois par la méfiance vis-à-vis de l’État traditionnel, contesté dans sa toute puissance et mis en cause quant à son impartialité et son efficacité, et par l’aspiration à de nouveaux modes de régulation sociale, faisant une plus large place à la médiation ou aux compromis négociés. La présente section offre une analyse du rôle crucial des autorités de contrôle en ce qui concerne le droit fondamental à la protection des données à caractère personnel. Cette analyse englobe une évaluation de leur fonctionnement, de leur indépendance et de leur efficacité. De plus l’action des autorités de contrôle demeure essentielle dans un contexte où les avancées technologiques récentes et en cours posent de nouveaux défis que le législateur arrive à encadrer avec du retard. La question quant à leur efficacité est de savoir si les autorités nationales de protection des données sont en mesure de jouer leur rôle face aux nouveaux défis technologiques. Nous verrons que leur capacité à relever ce défi dépend de trois facteurs : l’existence de règles qui octroient l’indépendance nécessaire à l’égard des pouvoirs publics ainsi que des acteurs privés du monde informatique (§1), la possibilité concrète de jouer un rôle clé vis-à-vis des pouvoirs publics et au sein des institutions européennes et l’existence des moyens et des pouvoirs nécessaires à l’accomplissement de leur tâche (§2).

§1. La nature juridique des autorités de contrôle

199 Des autorités administratives indépendantes. La création des autorités administratives indépendantes exprime une nouvelle façon de gouverner, favorisant la transparence, la consultation et la négociation, dans des domaines dont l'État ne veut pas assumer la responsabilité politique par exemple à cause de la technicité d'un secteur ou d'une obligation communautaire. Ainsi l'article 28 de la directive 95/46/CE disposait que chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la directive[1716]. Le nouveau règlement général 679/16 reprend cette formulation à l'article 51. Plusieurs États membres comme l'Autriche et les Pays-Bas ont désigné une autorité de protection des données disposant d'une compétence générale et plusieurs autres organes de contrôle spécifiques par secteur (par exemple, santé, poste ou télécommunications, etc.). D'autres États membres, caractérisés par une organisation fédérale ou dans lesquels des pouvoirs importants sont détenus au niveau régional, tels que l'Allemagne ou l'Espagne, se sont, quant à eux, dotés d'une entité de contrôle nationale et de plusieurs sous-agences infra-étatiques assurant les mêmes fonctions au niveau régional ou fédéral. Par ailleurs, alors que dans beaucoup de pays tels que la Roumanie, avant la mise en place des autorités de protection des données, les médiateurs étaient chargés de surveiller le respect des droits à la vie privée, dans certains États membres comme en Finlande, le médiateur conserve encore une fonction relative à la protection des données à caractère personnel.

La création des autorités de contrôle indépendantes souligne que la protection des données à caractère personnel représente un domaine politique stratégique de plus en plus important dans

---

1716 Voy. l'article 28 de la directive 95/46 : 1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la présente directive. Ces autorités exercent en toute indépendance les missions dont elles sont investies. 2. Chaque État membre prévoit que les autorités de contrôle sont consultées lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. 3. Chaque autorité de contrôle dispose notamment : de pouvoirs d'investigation, tels que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de sa mission de contrôle; de pouvoirs effectifs d'intervention, tels que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements, conformément à l'article 20, et d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement ou celui de saisir les parlements nationaux ou d'autres institutions politiques; du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la présente directive ou du pouvoir de porter ces violations à la connaissance de l'autorité judiciaire. Les décisions de l'autorité de contrôle faisant grief peuvent faire l'objet d'un recours juridictionnel. 4. Chaque autorité de contrôle peut être saisie par toute personne, ou par une association la représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel. La personne concernée est informée des suites données à sa demande. Chaque autorité de contrôle peut, en particulier, être saisie par toute personne d'une demande de vérification de la licéité d'un traitement lorsque les dispositions nationales prises en vertu de l'article 13 de la présente directive sont d'application. La personne est à tout le moins informée de ce qu'une vérification a eu lieu. 5. Chaque autorité de contrôle établit à intervalles réguliers un rapport sur son activité. Ce rapport est publié. 6. Indépendamment du droit national applicable au traitement en cause, chaque autorité de contrôle a compétence pour exercer, sur le territoire de l'État membre dont elle relève, les pouvoirs dont elle est investie conformément au paragraphe 3. Chaque autorité peut être appelée à exercer ses pouvoirs sur demande d'une autorité d'un autre État membre. Les autorités de contrôle coopèrent entre elles dans la mesure nécessaire à l'accomplissement de leurs missions, notamment en échangeant toute information utile. 7. Les États membres prévoient que les membres et agents des autorités de contrôle sont soumis, y compris après cessation de leurs activités, à l'obligation du secret professionnel à l'égard des informations confidentielles auxquelles ils ont accès.

l'Union, qui a joué un rôle clé pour la mise en place d'une législation cohérente dans les États membres[1717]. La nature juridique des autorités de contrôle a des conséquences sur leur statut ainsi que sur leurs missions. Toutefois des améliorations sont également nécessaires concernant l'indépendance, l'efficacité, les ressources et les pouvoirs des autorités de protection des données. Ainsi, tous les États membres de l'UE, en application des dispositions de l'article 28, paragraphe 1 de la directive 95/46 et maintenant de l'article 52 du règlement 679/16 relatifs à la protection des données, ont accordé à une autorité de contrôle nationale le mandat de surveiller l'application et de garantir le respect, sur leur territoire, de la législation relative à la protection des données. La directive 95/46/CE et maintenant le RGPD requiert que les autorités de protection des données « exercent en toute indépendance les missions dont elles sont investies » (A). Cependant, la nature de cette « indépendance » n'est pas précisée (B).

A. L'indépendance des autorités nationales de protection

200 Le principe d'indépendance dégagé par la Cour de justice. Les autorités de protection des données personnelles relèvent de la catégorie juridique des autorités administratives indépendantes. Les autorités administratives indépendantes sont « les organismes publics dépourvus de la personnalité morale qui sont conçus comme n'étant ni subordonnés au pouvoir exécutif, ni des prolongements du pouvoir législatif ou judiciaire et qui sont dotés de pouvoirs leur permettant d'exercer de façon autonome une mission de régulation sectorielle »[1718]. La directive 95/46/CE relative à la protection des données disposait que les autorités de protection des données « exercent en toute indépendance les missions dont elles sont investies »[1719] . Cependant, la nature de cette « indépendance » n'a pas été encadrée par la directive et c'est grâce à la jurisprudence de la Cour de justice que le principe d'indépendance des autorités de contrôle a été précisé. Le nouveau règlement ajoute que chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du règlement, afin de protéger les libertés et les droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel au sein de l'Union, et que chaque autorité de contrôle demeure libre de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicite ni n'accepte d'instructions de quiconque.

Ainsi l'indépendance des Autorités administrative tient en premier lieu à l'impartialité de leurs membres (1). Cette indépendance s'exprime à travers la collégialité, l'irrévocabilité et la durée des mandats[1720] (2).

1717 A. VITALIS, « L'apport à la démocratie des autorités de régulation indépendantes », préc., sp. p. 187

1718 C. TEITGEN-COLLY, « Les autorités administratives indépendantes : histoire d'une institution », in Cl. A. COLLIARD et G. TIMSIT, *Les autorités administratives indépendantes*, PUF, coll. Les voies du droit, 1988, p. 21 et s.

1719 Voy. Article 28, paragraphe 1 directive 95/46.

1720 La collégialité apparaît comme une garantie essentielle de l'indépendance : l'irrévocabilité des mandats des membres constitue une garantie d'indépendance essentielle, toutefois la règle n'est applicable qu'à condition de prévoir une durée de

1) L'impartialité comme expression d'indépendance

201 Le non-respect du principe d'impartialité par l'Allemagne. L'affaire *Commission c. Allemagne* est la première décision de la Cour de justice concernant l'indépendance des autorités de contrôle nationales[1721]. S'agissant d'un recours en manquement, la Commission a, le 5 juillet 2005, adressé une lettre de mise en demeure à la République fédérale d'Allemagne estimant qu'il est incompatible avec l'article 28, paragraphe 1, second alinéa, de la directive 95/46 de soumettre l'autorité chargée de veiller au respect des dispositions sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel par le secteur non public à une tutelle de l'État, comme c'est le cas dans tous les Länder allemands. Cette dernière a répondu par une lettre datée du 12 septembre 2005, en affirmant que le système allemand de contrôle en la matière répondait aux exigences de ladite directive. La Commission a ensuite adressé, le 12 décembre 2006, un avis motivé à la République fédérale d'Allemagne, réitérant le grief précédemment formulé. Dans sa réponse du 14 février 2007, celle-ci a réaffirmé son point de vue initial. L'argument de la République fédérale d'Allemagne portait sur une interprétation plus étroite des termes « en toute indépendance ». Ainsi, elle estimait que l'article 28, paragraphe 1, second alinéa, de la directive 95/46 exigeait une indépendance fonctionnelle des autorités de contrôle, en ce sens que ces autorités doivent être indépendantes du secteur non public soumis à leur contrôle et qu'elles ne doivent pas être exposées à des influences extérieures. Or, selon elle, la tutelle de l'État exercée dans les Länder allemands constitue non pas une telle influence extérieure, mais un mécanisme de surveillance interne à l'administration, mis en œuvre par des autorités relevant du même appareil administratif que les autorités de contrôle et tenues, tout comme ces dernières, de remplir les objectifs de la directive 95/46. De plus, selon elle, la tutelle de l'État ne vise qu'à garantir une action des autorités de contrôle qui soit conforme aux dispositions nationales et communautaires applicables, et qu'elle n'a donc pas pour objectif de contraindre lesdites autorités à éventuellement poursuivre des objectifs politiques contraires à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et aux droits fondamentaux. Toutefois, la Cour de justice souligne qu'il ne saurait être exclu que les autorités de tutelle, qui font partie de l'administration générale et sont donc soumises au gouvernement de leur Land respectif, ne soient pas en mesure d'agir de manière objective lorsqu'elles interprètent et appliquent les dispositions relatives au traitement des données à caractère personnel.

Selon la Cour de justice, les autorités de contrôle doivent être indépendantes et dotées de pouvoirs pour veiller à l'application des lois nationales, issues de la transposition de la directive (art. 28§1 de la directive 95/46). Elle précise que l'article 28 §1 de la directive 95/46 prévoit une indépendance qui n'est pas simplement fonctionnelle. La CJ, contre l'avis de l'Avocat

mandat suffisamment longue et un renouvellement du collège par moitié ou par tiers, afin de préserver la mémoire de l'autorité requise pour la sécurité juridique. Le caractère non renouvelable des mandats constitue également un facteur d'indépendance, en réduisant le risque de pression par l'autorité de nomination.

1721 CJUE, Gr. Ch. *Commission c. Allemagne*, C- 518/07, 9 mars 2010.

général qui estimait que la Commission n'avait pas prouvé que la tutelle empêchait l'indépendance[1722], a donné raison à la commission européenne et condamné l'Allemagne pour avoir manqué à cette obligation d'indépendance en imposant un contrôle au sein des Länder allemands. La Cour a conclu que le risque que les autorités de tutelle puissent exercer une influence politique sur les décisions des autorités de contrôle suffisait pour entraver l'exercice indépendant des missions de celles-ci. D'une part, comme l'a relevé la Commission, il pourrait y avoir une « obéissance anticipée » de ces autorités eu égard à la pratique décisionnelle de l'autorité de tutelle. D'autre part, le rôle de gardiennes du droit à la vie privée qu'assument lesdites autorités exige que leurs décisions, et donc elles-mêmes, soient au-dessus de tout soupçon de partialité[1723]. Il faut considérer que l'institution, dans les États membres, d'autorités de contrôle exerçant en toute indépendance leurs fonctions est un élément essentiel de la protection des personnes à l'égard du traitement des données à caractère personnel. Cette indépendance est nécessaire pour créer, dans tous les États membres, un niveau également élevé de protection des personnes physiques à l'égard du traitement des données à caractère personnel et contribue de cette façon à la libre circulation des données, qui est nécessaire à l'établissement et au fonctionnement du marché intérieur[1724]. La Cour n'a pas suivi les conclusions de l'Avocat général selon lequel, le recours devait être rejeté car la Commission n'avait pas prouvé en quoi la tutelle exercée sur les autorités de contrôle en matière de protection des données à caractère personnel empêchait ces autorités de contrôle d'exercer leurs missions en toute indépendance.

202 Le non-respect du principe d'impartialité par l'Autriche. Dans l'affaire *Commission c. Autriche*[1725], la Cour de justice a aussi statué dans le même sens, elle a dû se prononcer à nouveau sur l'indépendance des autorités de contrôle et a condamné l'Autriche. Dans sa requête, la Commission européenne demandait à la Cour de constater que, en ne prenant pas toutes les dispositions nécessaires pour que la législation en vigueur en Autriche satisfasse au critère d'indépendance concernant la *Datenschutzkommission* (commission de protection des données, la « DSK »), instituée en tant qu'autorité de contrôle de la protection des données à caractère personnel, l'Autriche avait violé le droit de l'UE. Ainsi la République d'Autriche avait manqué aux obligations qui lui incombent en vertu de l'article 28, paragraphe 1, second alinéa, de la directive 95/46/CE puisque selon la réglementation en vigueur, le membre administrateur de la DSK doit toujours être un fonctionnaire de la chancellerie fédérale. L'Autriche avaient souligné que l'art 28§1 de la directive 95/46 se réfère à une indépendance fonctionnelle. Ainsi, la DSK disposerait d'une telle indépendance dès lors que ses membres seraient indépendants et ne seraient liés par aucune instruction dans l'exercice de leur fonction.

1722 Voy. Conclusion de l'Avocat général M. JÁN MAZÁK présentées le 12 novembre 2009 Affaire C 518/07, point 13-16 : « À cet égard, il y a lieu de noter que l'article 28, paragraphe 1, de la directive 95/46 n'impose pas aux États membres de constituer des autorités qui seraient séparées du système administratif hiérarchiquement organisé. Il convient toutefois d'ajouter que rien ne les en empêche. Étant donné que l'article 28, paragraphe 1, de la directive 95/46 demande aux États membres de garantir l'exercice des missions des autorités de contrôle en toute indépendance, et non de garantir l'indépendance de telles autorités, il leur laisse une marge d'appréciation pour décider de la manière dont ils satisfont à cette demande. Il convient aussi de ne pas perdre de vue que le terme « indépendance » est un terme relatif, dès lors qu'il convient de préciser à l'égard de qui ou de quoi et à quel niveau cette indépendance doit exister ».

1723 Voy. §36 de la décision.

1724 Voy. considérant 62 de la directive 95/46/CE.

1725 CJUE, Gr. Ch. Commission c. Autriche, C 614/10,16 octobre 2012.

Elle soulignait que le membre administrateur ne serait pas nécessairement un fonctionnaire de la chancellerie fédérale, même s'il n'est pas contesté que ledit poste a toujours été occupé par un tel fonctionnaire. Par ailleurs, la DSK pourrait elle même décider de nommer librement son membre administrateur en modifiant de manière autonome son règlement intérieur. Le fait que le membre administrateur, à l'instar de tout autre fonctionnaire, dépendrait, pour son avancement, de la décision de son supérieur hiérarchique et, en dernier ressort, d'un ministre, n'affecterait pas son indépendance. Au contraire, selon l'argumentation de la Commission, toutes les affaires de la DSK seraient ainsi de facto gérées par un fonctionnaire fédéral. Selon la Commission, un tel système réaliserait une simple autonomie fonctionnelle de l'autorité de contrôle. La Cour de justice estime qu'une telle indépendance fonctionnelle ne suffit pas, à elle seule, à préserver ladite autorité de contrôle de toute influence extérieure. La Cour dans son argumentation rappelle son arrêt Commission c. Allemagne, précité[1726], en soulignant que le terme « en toute indépendance » prévu au titre de l'article 28, paragraphe 1, de la directive 95/46, vise à exclure non seulement l'influence directe, sous forme d'instructions, mais également, toute forme d'influence indirecte susceptible d'orienter les décisions de l'autorité de contrôle. La Cour de justice a conclu que l'autorité de protection des données autrichienne n'exerçait pas sa mission en toute indépendance car le membre administrateur était un fonctionnaire fédéral assujetti à une tutelle de service, le bureau de la Commission était intégré aux services de la chancellerie fédérale, et le chancelier fédéral disposait d'un droit inconditionnel à l'information sur tous les aspects de la gestion de la Commission. À l'occasion des arrêts précités concernant l'Allemagne et l'Autriche, la Cour de justice consacre l'existence des autorités publiques situées en dehors de l'administration centrale.

1726 Voy. CJUE, Commission/Allemagne, précité, points 19, 25, 30 et 50

2) L'étendue du mandat comme expression d'indépendance

203 L'affirmation du principe d'irrévocabilité des membres. La Cour de justice a plus récemment eu l'occasion de rendre une décision concernant l'exigence relative au mandat des membres de l'autorité de contrôle. Ainsi dans l'affaire *Commission c. Hongrie*[1727], la Cour de justice a condamné la Hongrie pour violation du droit de l'Union. L'affaire concernait l'irrévocabilité du mandat du commissaire à la protection des données comme expression d'indépendance. La Commission avait introduit un recours en manquement devant la Cour de justice à l'encontre de la Hongrie. Le Contrôleur européen de la protection des données était intervenu dans la procédure en soutien de la Commission. Dans son arrêt, la Cour rappelle que les autorités de contrôle, créées conformément à la directive, doivent pouvoir exercer leurs missions sans aucune influence extérieure. Cette exigence implique, d'une part, qu'elles ne soient liées par aucune instruction dans l'exercice de leurs fonctions et, d'autre part, que leurs décisions soient prises sans aucune influence politique, le risque d'une telle influence devant lui-même être écarté. Or, permettre à un État membre de mettre fin au mandat d'une autorité de contrôle avant son expiration, sans respecter les règles et les garanties préétablies à cette fin par la législation applicable, pourrait conduire celle-ci à obéir à la volonté du pouvoir politique. Par conséquent, l'indépendance de l'autorité de contrôle inclut nécessairement l'obligation de respecter la durée du mandat confié à cette autorité et de n'y mettre fin qu'en respectant la législation applicable. Ainsi, en mettant fin de manière anticipée au mandat du commissaire chargé de la protection des données, la Hongrie a violé le droit de l'Union. L'indépendance des autorités responsables de la protection des données à caractère personnel impose aux États membres de respecter la durée du mandat confié à ces autorités.

204 La compétence de chaque autorité de vérifier si un transfert de données de son État membre vers un pays tiers répond aux exigences du droit dérivé de l'Union. Concernant l'étendue des pouvoirs des autorités de contrôle, la Cour de justice, dans l'affaire *Schrems*[1728], a souligné que la décision de la Commission constatant le caractère adéquat de la protection des données à caractère personnel aux États-Unis[1729] n'empêchait pas les autorités nationales de suspendre le transfert des données des abonnés européens de Facebook vers des serveurs situés aux États-Unis[1730]. Saisie de l'affaire, la *High Court of Ireland* (Haute Cour de justice

---

1727 CJUE, Commission c. Hongrie, C-288/12, 8 avril 2014.

1728 CJUE, Gr. Ch., C 362/14, Maximillian Schrems c. Data Protection Commissioner, 6 octobre 2015.

1729 En effet, la directive 95/46/CE sur le traitement des données à caractère personnel dispose que le transfert de telles données vers un pays tiers peut avoir lieu si le pays tiers en question assure un niveau de protection adéquat à ces données. Toujours selon la directive, la Commission peut constater qu'un pays tiers assure un niveau de protection adéquat. La Commission avait adopté une décision en ce sens. Voy. Décision 2000/520/CE de la Commission, du 26 juillet 2000, conformément à la directive 95/46/CE du Parlement européen et du Conseil relative à la pertinence de la protection assurée par les principes de la « sphère de sécurité » et par les questions souvent posées y afférentes, publiés par le ministère du commerce des États-Unis d'Amérique (JO 2000, L 215, p. 7).

1730 Le requérant, M. Schrems, avait déposé plainte auprès de l'autorité irlandaise de protection des données, considérant qu'au vu des révélations faites en 2013 par M. Edward Snowden au sujet des activités des services de renseignement des États-

irlandaise) à travers le renvoi préjudiciel en appréciation de validité souhaitait savoir si la décision d' « adéquation » de la Commission avait pour effet d'empêcher une autorité nationale de contrôle d'enquêter sur une plainte alléguant qu'un pays tiers n'assurait pas un niveau de protection adéquat et, le cas échéant, de suspendre le transfert de données contesté. La Cour, dans son raisonnement, a souligné le fondement « constitutionnel » des pouvoirs dont disposent les autorités nationales. Elle rappelle que l'institution d'autorités indépendantes dans les États membres résulte d'une double exigence issue de l'article 8, paragraphe 3, de la Charte et de l'article 16, paragraphe 2, TFUE et constitue à ce titre un élément essentiel du respect de la protection des personnes à l'égard du traitement des données à caractère personnel[1731]. Elle a estimé que la délicate conciliation entre le respect du droit fondamental à la vie privée et les intérêts économiques liés à la libre circulation des données à caractère personnel que doivent opérer ces instances, implique que celles-ci puissent disposer d'un large éventail de pouvoirs dont, notamment, des pouvoirs d'investigation, et des pouvoirs effectifs de sanction et d'intervention[1732] tels que celui d'interdire temporairement ou définitivement un traitement de données ou encore et surtout celui d'ester en justice[1733]. La Cour de justice en suivant les conclusions de l'Avocat général a souligné que, si les autorités nationales de contrôle étaient liées de manière absolue par les décisions adoptées par la Commission, cela limiterait inévitablement la totale indépendance dont elles bénéficient en vertu de la directive. Si une autorité nationale de contrôle estime qu'un transfert de données porte atteinte à la protection des citoyens de l'Union quant au traitement de leurs données, elle a le pouvoir de suspendre ce transfert. Autrement dit, la Commission ne dispose pas de la compétence de restreindre les pouvoirs des autorités nationales de contrôle. En effet, ces transferts doivent répondre au même niveau d'exigence de respect des droits fondamentaux que les traitements réalisés sur le territoire des États membres d'une part, et que les autorités nationales doivent être investies des pouvoirs permettant de contrôler le respect de ces mêmes droits d'autre part[1734]. En conséquence, chacune de ces autorités doit être investie « de la compétence de vérifier si un transfert de données à caractère personnel depuis l'État membre dont elle relève vers un pays tiers respecte les exigences posées par la directive 95/46 »[1735]. Il est surtout remarquable que la Cour de justice citant l'arrêt *Kadi*[1736], ancre l'accès effectif à un contrôle indépendant dans

Unis (en particulier la National Security Agency ou « NSA »), le droit et les pratiques des É tats-Unis n'offraient aucune protection réelle contre la surveillance, par l'État américain, des données transférées vers ce pays. En effet, les données fournies par M. Schrems à Facebook sont transférées, en tout ou partie, à partir de la filiale irlandaise de Facebook sur des serveurs situés sur le territoire des États-Unis, où elles sont conservées. L'autorité irlandaise avait rejeté la plainte, au motif notamment que, dans une décision du 26 juillet 20002, la Commission a estimé que, dans le cadre du régime dit de la « sphère de sécurité », les États-Unis assurent un niveau adéquat de protection aux données à caractère personnel transférées.

1731 Voy. Décision *Schrems* §41.

1732 CJUE, 9 mars 2010, Commission/Allemagne, Aff. C 518/07 §24, ; CJUE, 8 avril 2014 Commission/Hongrie C 288/12, §51.

1733 Voy. § 48 de la décision.

1734 Dans le RGPD voy. Article 45 (tranbsfert sur la base d'une décision d'adéquation); article 46 (autres garanties appropriées, y compris des règles d'entreprise contraignantes); art. 49 (dérogations dans des situations spécifiques).

1735 Voy. §49 de la décision.

1736 Voy. §60 de la décision.

l'exigence d'accès à un recours effectif. A cet égard, et comme le rappelait l'avocat général Yves Bot[1737], doivent être examinés de manière approfondie « le contenu des règles applicables et les moyens d'assurer le respect de ces règles ». Il doit donc exister dans le droit étranger en question un dispositif de contrôle externe sous la forme d'une autorité indépendante qui « constitue un élément nécessaire de tout système visant à assurer le respect des règles relatives à la protection des données à caractère personnel ». Le nouveau règlement 679/2016 a su intégrer la jurisprudence de la Cour de justice, en prévoyant dans son article 52.2 que les autorités de contrôle demeurent libres de toute influence extérieure, qu'elle soit directe ou indirecte, et ne sollicitent ni n'acceptent d'instructions de quiconque. Si la jurisprudence est intervenue pour préciser le contenu de l'indépendance et de l'étendue des pouvoirs des autorités de contrôle, dans la pratique on constate des lacunes et des limites qui perdurent.

B. Une indépendance limitée

205 Quid des ressources nécessaires. Afin de garantir l'autonomie et l'indépendance des autorités de contrôle, les moyens financiers constituent un point important. Concernant l'indépendance budgétaire, elle regroupe l'indépendance financière, qui vise les ressources de l'autorité, l'indépendance d'exécution budgétaire, qui permet à l'autorité de décider de l'utilisation de son budget et l'autonomie de gestion budgétaire, qui désigne la capacité de l'autorité à effectuer ses dépenses. Il a été souligné que l'absence de ressources financières suffisantes suscitait de graves difficultés au niveau du fonctionnement de plusieurs autorités de protection des données[1738]. Dans la plupart des États membres, les autorités de protection des données reçoivent les ressources nécessaires à leur fonctionnement du budget de l'État[1739] et souvent à partir du budget alloué au ministère de la Justice. Dans certains États membres, les autorités de contrôle peuvent accroître de façon importante leurs ressources financières grâce aux recettes obtenues des notifications des sous-traitants chargés du traitement des données et/ou des sanctions pécuniaires imposées en cas d'infraction à la législation relative à la protection des données[1740]. Au Royaume-Uni, les droits de notification représentent la seule source de revenus de l'autorité de contrôle pour les travaux menés en matière de protection des données. Même si seules des ressources suffisantes peuvent garantir l'indépendance des autorités de contrôle, dans d'autres pays, où l'autorité de protection des données bénéficie actuellement d'un financement relativement adéquat, des coupes budgétaires ont été prévues pour les années à venir [1741] . L'absence de ressources humaines et financières suffisantes

---

1737 Voy. les Conclusions de l'Avocat général Yves Bot dans l'affaire C 362/14, 23 septembre 2015, §52.

1738 Voy. l'étude de l'Agence des droits fondamentaux de l'Union europeenne, « La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données – Renforcement de l'architecture des droits fondamentaux au sein de l'UE II », préc., sp. p. 28.

1739 Par exemple, l'Estonie, la France, l'Italie, les Pays-Bas.

1740 Voy. Par exemple, au Luxembourg et à Malte.

représente un défi majeur pour l'efficacité des systèmes de contrôle nationaux, qui pourrait mettre en danger la protection des droits fondamentaux des personnes concernées. De ce fait, le nouveau règlement 679/16 prévoit à son article 51.4 que chaque État membre veille à ce que chaque autorité de contrôle dispose des ressources humaines, techniques et financières ainsi que des locaux et de l'infrastructure nécessaires à l'exercice effectif de ses missions et de ses pouvoirs. Ainsi, les États membres devraient garantir que les autorités nationales de protection des données disposent de ressources suffisantes pour fonctionner correctement. Sur le plan opérationnel, les pouvoirs limités de plusieurs d'entre elles restent un problème de taille. Dans certains États membres, les autorités de contrôle ne disposent pas de pleins pouvoirs pour instruire, intervenir dans le traitement des opérations, prodiguer des conseils juridiques et ester en justice. Concernant l'indépendance de leur mandat, dans un certain nombre d'États membres, comme en Allemagne et en Slovénie, les délégués des autorités de contrôle en matière de protection des données sont élus par les assemblées législatives, et parfois même (comme en Grèce) dans le cadre de procédures exigeant un consensus entre la majorité et l'opposition: à quelques exceptions près (par exemple, en Hongrie, où la pratique constitutionnelle permet aux partis représentés au parlement de se répartir les postes disponibles selon le choix de candidat du parti) cela garantit un niveau élevé d'indépendance des délégués élus. Toutefois, dans d'autres États membres, au contraire, les délégués à la protection des données sont directement nommés par le gouvernement (par exemple, en Irlande et au Luxembourg) sans intervention de l'opposition parlementaire. Cette situation a suscité d'importantes préoccupations quant à l'indépendance effective des autorités de contrôle en matière de protection des données. Des inquiétudes similaires peuvent naître dans les pays où l'autorité de contrôle est rattachée au ministère de la Justice (par exemple, au Danemark et en Lettonie). De plus, d'autres États membres (tels que la Belgique, la France, l'Espagne, le Portugal) ont prévu une procédure mixte pour la désignation des délégués de l'autorité nationale de contrôle en matière de protection des données, impliquant à la fois le pouvoir exécutif, législatif et judiciaire ainsi que d'autres groupes organisés de la société (par exemple, le conseil suprême des universités en Espagne). Dans de telles situations, toutefois, il est essentiel de garantir que le gouvernement ne contrôle pas directement ou indirectement, la majorité des personnes désignées, dénaturant ainsi la finalité même d'une procédure de nomination pluraliste. Dans d'autres États membres, comme en Italie par exemple, les délégués des autorités de contrôle en matière de protection des données ont un mandat de sept ans non renouvelable. Dans certains pays (comme en Pologne et en Slovaquie), les délégués des autorités de contrôle en matière de protection des données peuvent être démis de leurs fonctions de façon anticipée uniquement en cas de mauvaise conduite spécifique et en suivant la même procédure que celle adoptée pour leur désignation. Ces solutions garantissent une grande indépendance des organes de contrôle, en limitant l'influence et les pressions des pouvoirs politiques. À l'inverse, dans d'autres États membres comme l'Irlande, le gouvernement peut directement destituer de leurs fonctions les commissaires à la protection des données, ce qui suscite des préoccupations quant à l'indépendance réelle de l'organe de contrôle, notamment concernant la surveillance du respect de la législation relative à la protection des données par les autorités gouvernementales. D'autres garanties importantes renforcent l'autonomie et

1741 Voy. Par exemple, au Danemark et en Irlande.

l'indépendance des autorités de contrôle : par exemple au Portugal et en Grèce, l'existence et le mandat de l'autorité indépendante sont explicitement établis dans la Constitution. Dans d'autres États membres, comme en Espagne et à Malte, l'attribution d'une personnalité juridique distincte de l'autorité de contrôle en matière de protection des données et la possibilité d'entamer des poursuites judiciaires devant la Cour constitutionnelle du pays (par exemple, en Slovénie) constituent d'autres garanties importantes d'indépendance institutionnelle. Concernant le mandat, dans un certain nombre d'États membres comme en Italie, les délégués des autorités de contrôle en matière de protection des données ont un mandat de sept ans non renouvelable. Dans certains pays comme en Pologne et en Slovaquie, les délégués des autorités de contrôle en matière de protection des données peuvent être démis de leurs fonctions de façon anticipée uniquement en cas de mauvaise conduite spécifique et en suivant la même procédure que celle adoptée pour leur désignation. Le RGPD renforce les garanties en prévoyant à son article 53.1 que les États membres prévoient que chacun des membres de leurs autorités de contrôle est nommé selon une procédure transparente par leur gouvernement, leur chef d'État et un organisme indépendant, et qu'un membre ne peut être démis de ses fonctions que s'il a commis une faute grave ou s'il ne remplit plus les conditions nécessaires à l'exercice de ses fonctions.

§2. La mise en œuvre du droit à la protection des données personnelles par les autorités de contrôle indépendantes nationales

Les États membres de l'Union ont attribué à leur autorité nationale de contrôle des pouvoirs en conformité avec le RGPD [1742]. Le RGPD prévoit que chaque autorité de contrôle est compétente pour exercer les missions et les pouvoirs dont elle est investie sur le territoire de l'État membre dont elle relève. La caractéristique distinctive des autorités de contrôle consiste dans une sorte de dérogation au principe classique de la séparation des pouvoirs, c'est-à-dire des détenteurs de fonctions qui se chevauchent à l'échelon législatif, exécutif et judiciaire. D'une part, les autorités ont des pouvoirs administratifs à part entière (par exemple, la délivrance d'autorisations, l'imposition de sanctions), dans le passé attribués au type administratif

1742 Voy. l'article 28, paragraphe 2 (pouvoir de conseiller les autorités législatives ou administratives lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel), paragraphe 3 (pouvoirs d'investigation, d'intervention et d'ester en justice) et paragraphe 4 (pouvoir d'être saisie d'une demande). En règle générale, l'analyse des pouvoirs des différentes autorités nationales de protection des données permet de distinguer deux grandes tendances, qui reflètent les approches suivies par les États membres dans la mise en œuvre de la directive relative à la protection des données. Alors que plusieurs pays (par exemple, la Finlande, la Suède, l'Irlande et le Royaume-Uni) ont souligné le rôle préventif et proactif des agences de contrôle, mettant en exergue leur rôle ex-ante pour garantir la protection des données à caractère personnel, d'autres États membres (tels que la Lettonie, la République tchèque et la Grèce) ont donné la priorité aux fonctions d'application et de contrôle a posteriori des autorités de protection des données et leur ont confié une mission réactive afin de veiller au respect de la législation relative à la protection des données. La nature des pouvoirs conférés aux organes de contrôle varie en conséquence, avec une préférence pour les instruments de prévention « souples », dans le premier cas, et pour des mesures « plus strictes », dans le second. Il est important, néanmoins, de ne pas trop insister sur ces différences, et certains pays (tels que le Danemark, les Pays-Bas, la Slovénie et l'Italie) ont adopté une position intermédiaire, en attribuant à leur autorité nationale de protection des données des compétences destinées à aider et à garantir un respect actif de la législation relative à la protection des données, tout en les habilitant dans le même temps à poursuivre et sanctionner les cas d'infraction.

traditionnel, les ministères. D'autre part, elles sont aussi titulaires de fonctions arbitraires et quasi juridictionnelles liées à des situations juridiques bilatérales horizontales entre particuliers, pour lesquelles le rôle des autorités est l'arbitre équidistant concernant les intérêts opposés en jeu. Il ressort en ce sens le rôle neutre ou quasi juridictionnel des autorités dont les pouvoirs, selon certains auteurs[1743], ne présupposent pas une mise en balance réelle d'intérêts publics et privés et seraient donc dépourvus du caractère discrétionnaire propre aux juridictions. Concernant le rôle quasi-contentieux des autorités de contrôle, selon certains auteurs[1744], cette tâche relève de certaines fonctions de l'Autorité et non de l'organe lui-même. L'attribution des fonctions réglementaires est l'aspect le plus important de l'indépendance des autorités administratives indépendantes, cette fonction permet à l'autorité de déterminer ses activités dans des secteurs particuliers[1745] . À côté des pouvoirs d'influence[1746] (A), les autorités de protection des données personnelles disposent aussi de pouvoirs de contrainte qui lient les pouvoirs publics et privés (B).

A. Des pouvoirs consultatifs

206 Un pouvoir d'influence. À l'origine, les compétences des autorités de protection des données personnelles étaient essentiellement consultatives. Leur pouvoir d'influence a été consolidé avec la reconnaissance d'un droit à la protection des données personnelles. C'est au nom de ce droit que leur est justifiée l'attribution d'une fonction consultative à l'égard du pouvoir normatif. C'est donc essentiellement le Groupe G 29 qui a cherché à développer son rôle consultatif en s'appuyant sur la consécration d'un tel droit à l'article 8 de la Charte des droits fondamentaux de l'Union européenne. Sans être une autorité de protection des données personnelles, le Groupe G 29, qui réunit les autorités de protection des données personnelles nationales, a des fonctions similaires et s'est appuyé sur le droit à la protection des données personnelles pour développer « une conception proactive de son rôle de conseil »[1747]. Il a ainsi donné son avis sur des sujets en matière de sécurité et de justice qui n'entraient pas

---

1743 V. CAIANIELLO, « Il difficile equilibrio delle autorità indipendenti », in Il diritto dell'economia, 1998, p. 258 e « Le autorità indipendenti tra potere politico e società civile », in *Rassegna giuridica dell'energia elet.trica*, 1997, p. 37.

1744 TESAURO, « Esiste un ruolo paragiurisdizionale dell'Antitrust nella promozione della concorrenza*? »*, in F. KOSTORIS PADUA SCHIOPPA (a cura di), Le autorità indipendenti e il buon funzionamento dei mercati, Milano 2002, p169 et ss.

1745 G. VESPERINI-MAISL, « Les autorités administratives indépendantes : protection des libertés ou régulation sociale*? »*, in *Les autorités administratives indépendantes*, Colliard – Timsit, p. 87 e ss.;

1746 Concernant la CNIL, N. LENOIR, H. MAISL, *La CNIL et le contrôle de l'administration. Premières orientations (1978-1983)*, préc., sp. p. 646 : « la commission a peut-être d'abord un pouvoir d'influence et de persuasion. Son action d'information et de concertation à travers, par exemple, l'instruction des dossiers, les conseils aux pouvoirs publics, les conférences de presse, la publication des rapport annuels, est sans doute ce qui est le plus délicat à mesurer et en même temps l'essentiel ».

1747 S. NERBONNE, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *Legicom*, 2009, n° 42, pp. 37 et s., sp. p. 41.

matériellement dans le champ de la directive n° 95/46 CE qui a institué cette autorité[1748]. Il a aussi fait part de son avis à d'autres institutions que la Commission européenne telles que le Parlement européen notamment. « La relation entre le G 29 et le Parlement s'est ainsi resserrée au fil du temps, le Parlement reprenant la plupart des avis du groupe de travail dans ses résolutions sur les questions de protection des données »[1749]. Deplus, conformément à l'article 28, paragraphe 2, de la directive relative à la protection des données, les autorités de contrôle sont consultées par les législateurs et administrations nationales lors de l'élaboration des mesures réglementaires ou administratives relatives à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel. Les finalités mêmes de la directive relative à la protection des données impliquent donc de la part des autorités de protection des données le pouvoir général de donner des avis et d'être consultées par des parties privées concernées par le traitement des données et de fournir des recommandations générales par secteur. Enfin, l'article 25 de la directive relative à la protection des données établit des règles spécifiques sur le transfert de données à caractère personnel vers des pays extérieurs à l'UE (à savoir des pays tiers), avec possibilité d'intervention pour les autorités nationales de contrôle. Dans sa mission consultative, l'autorité de contrôle nationale est tout d'abord tenue de conseiller des parties privées sur l'application de la législation relative à la protection des données. Les autorités de protection des données disposent également d'un pouvoir quasi législatif pour élaborer des réglementations générales destinées à des secteurs spécifiques, promouvoir l'élaboration de codes de conduite privés et soumettre des avis et des recommandations à l'attention d'acteurs publics et privés intervenant dans le domaine du traitement des données. La plupart de ces mesures n'ont toutefois aucun caractère juridiquement contraignant. Par ailleurs, beaucoup d'États membres n'accordent à leurs autorités de contrôle qu'une fonction consultative dans le contexte des avis fournis aux pouvoirs législatif et exécutif sur les projets de législation relatifs à la protection des données à caractère personnel. Par conséquent, leurs avis sur les projets de loi et de règlements sont facultatifs[1750] ou ne sont strictement requis légalement que pour l'élaboration de règlements d'exécution. Cela est regrettable étant donné que les conseils donnés durant la rédaction permettent parfois d'éviter les futurs problèmes. L'absence d'avis des autorités de protection des données avant l'adoption d'une législation ou d'une règlementation qui peuvent avoir un effet négatif sur la protection des données à caractère personnel peut indiquer que l'importance des aspects concernant la protection de la vie privée n'a pas été pleinement appréciée lors de choix politiques. La fonction

---

1748 Voy. par ex. G 29, Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, WP 178, 12 novembre 2010 ; G 29, Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives présentée par la Commission le 6 novembre 2007, WP 145, 5 décembre 2007 ; G 29, Avis 3/2005 sur l'application du règlement (CE) no 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, WP 112, 4 septembre 2012

1749 S. NERBONNE, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position « ?, préc., sp. pp. 41-*42.*

1750 Comme en Allemagne, en Autriche, en France, en Grèce, et en Italie, Voy. l'étude de l'Agence des droits fondamentaux de l'Union europeenne, « La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données – Renforcement de l'architecture des droits fondamentaux au sein de l'UE II », préc., sp. p. 26.

consultative des autorités de protection des données personnelles ne s'adresse pas seulement aux pouvoirs publics. Ces autorités qui constituent des « sources officielles d'information »[1751] peuvent également conseiller les juridictions. Ainsi, les autorités de protection des données personnelles peuvent être sollicitées par les juridictions puisqu'elles constituent des « experts gracieux des juridictions » : en effet, « les juridictions ne sont généralement pas spécialisées, ce qui accroît la difficulté de la tâche des magistrats. C'est pourquoi il est essentiel de prévoir que les autorités administratives indépendantes peuvent, sans exception, fournir des avis à des juridictions ou interpréter le silence des textes dans ce sens »[1752]. Leur activité fait l'objet d'un rapport annuel qui peut comprendre une liste des types de violations notifiées et des types de mesures prises conformément. Ce rapport est transmis au parlement national, au gouvernement et à d'autres autorités désignées par le droit de l'État membre. Il est mis à la disposition du public, de la Commission et du Comité. A côté des pouvoirs d'influence, les autorités de protection des données personnelles disposent aussi de pouvoirs de contrainte qui lient les pouvoirs publics.

B. Des pouvoirs de contrainte

207 Un pouvoir quasi juridictionnel. Les pouvoirs des autorités de protection des données ne se limitent pas à un pouvoir d'influence. Celles-ci disposent également d'un pouvoir de contrainte tel que l'on peut parler d'un pouvoir quasi juridictionnel. Ce pouvoir de contrainte consiste d'abord en la faculté d'autoriser ou de refuser certains traitements de données personnelles. Il correspond ensuite à la faculté d'adopter des règlements relatifs à l'utilisation des données personnelles. Ainsi, les autorités de contrôle disposent de pouvoirs d'enquête tels que le pouvoir d'obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel et à toutes les informations nécessaires à l'accomplissement de ses missions ; celui d'obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant, notamment à toute installation et à tout moyen de traitement, conformément au droit de l'Union ou au droit procédural des États membres. Elles disposent également d'un pouvoir coercitif, tel que le pouvoir d'ordonner au responsable du traitement ou au sous-traitant de mettre les opérations de traitement en conformité avec les dispositions du présent règlement, le cas échéant, de manière spécifique et dans un délai déterminé ; celui d'imposer une limitation temporaire ou définitive, y compris une interdiction, du traitement ; d'ordonner la rectification ou l'effacement de données à caractère personnel ou la limitation du traitement ; d'imposer une amende administrative. Ainsi leur pouvoir de contrainte se concrétise, en premier lieu, dans la possibilité de prendre d'office et de manière préventive, des mesures en cas de non-respect des

---

1751 D. MAZEAUD, « L'expertise de droit à travers l'amicus curiae », in M.-A. FRISON -ROCHE, D. MAZEAUD (dir.), *L'expertise*, Dalloz, coll. Thèmes et commentaires, 1997, pp. 109 et s.

1752 M.-A. FRINSON-ROCHE, « Etude dressant un bilan des autorités administratives indépendantes », in P. Gelard, *Les autorités administratives indépendantes : évaluation d'un objet juridique non identifié*, t. 2, préc., pp. 9 et s., sp. p. 113.

dispositions régissant le traitement des données personnelles[1753]. Deuxièmement, leur pouvoir de contrainte consiste dans des mesures visant à protéger le droit fondamental à la protection des données personnelles de manière restitutive dans des cas individuels[1754]. Ainsi les États membres de l'UE ont investi leur autorité nationale d'un contrôle des pouvoirs tels que les pouvoirs d'investigation et d'intervention (1), celui d'ester en justice et le pouvoir d'être saisie d'une demande[1755] (2). De plus, la cohérence de leur pouvoir est garantie par la mise en place d'une autorité chef de file et du mécanisme de cohérence (3).

1) Le pouvoir d'investigation et intervention

208 Un pouvoir quasi normatif et quasi juridictionnel. Les autorités de contrôle nationales disposent d'un pouvoir de contrainte, à travers la reconnaissance d'un pouvoir quasi normatif[1756] et d'un pouvoir quasi juridictionnel. Ce pouvoir de contrainte leur permet de mettre en œuvre elles-mêmes le droit à la protection des données personnelles. Pour garantir la mise en œuvre du droit à la protection des données personnelles, les autorités de contrôle disposent tout d'abord d'un pouvoir d'investigation tel que le pouvoir d'accéder aux données faisant l'objet d'un traitement et de recueillir toutes les informations nécessaires à l'accomplissement de leur mission de contrôle[1757]. Ces pouvoirs peuvent être exercés d'office ou sur demande d'une personne alléguant la violation de ses droits en matière de données à caractère personnel. Selon l'étude de l'Agence des droits fondamentaux, dans la grande majorité des États membres, les autorités de contrôle peuvent, dans l'exercice de leurs fonctions, et en vue d'identifier des violations de la législation en matière de protection des données, entrer (au besoin avec l'aide de la police) dans les locaux et dans tout autre lieu où le traitement de données est réalisé, saisir les matériels nécessaires, enquêter et relever des preuves (même sans le consentement des responsables du traitement des données), sans devoir demander au préalable un mandat judiciaire. Seules les autorités de protection des données personnelles de la France, de Malte, du Royaume-Uni et de la Roumanie ne peuvent pas perquisitionner le responsable d'un traitement de données personnelles sans mandat judiciaire[1758]. Deuxièmement, les autorités nationales de contrôle disposent d'un pouvoir d'intervention tel que, par exemple, celui de rendre des avis préalablement à la mise en œuvre des traitements de données sensibles et

1753 Concernant le CEDP voy. l'art. 46 b) et c) du règlement 45/2001, concernant les autorités de contrôle nationales voy. art. 20§1 et 2 de la directive 95/46.

1754 Conformément à l'article 46 a) et b) du règlement 45/2001 et à l'article 28§4 de la directive 95/46.

1755 Vir §3-4 de l'art. 28 de la directive 95/46.

1756 Ce pouvoir consiste notamment dans la faculté d'autoriser ou de refuser certaines utilisations de données personnelles. Il correspond ensuite à la faculté d'adopter des règlements relatifs à l'utilisation des données personnelles.

1757 Conformément à l'art. 58 du RGPD.

1758 Agence des droits fondamentaux de l'Union europeenne, « La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données. Renforcement de l'architecture des droits fondamentaux au sein de l'UE II », Luxembourg : Office des publications de l'Union européenne, 2012, 50 p., sp. p. 22.

d'assurer une publication appropriée de ces avis ou celui d'ordonner le verrouillage, l'effacement ou la destruction de données, ou d'interdire temporairement ou définitivement un traitement, ou celui d'adresser un avertissement ou une admonestation au responsable du traitement. Enfin, les articles 46 et suivants du RGPD établissent des règles spécifiques quant au transfert de données à caractère personnel vers des pays extérieurs à l'UE (des pays tiers), avec possibilité d'intervention pour les autorités nationales de contrôle. Ainsi, les autorités de contrôle nationales réunies au sein du G29 ont su participer de façon proactive à son rôle de conseil, y compris avec des avis en matière de sécurité et de justice[1759]. Elles se sont également exprimées, à l'instar du CEPD, sur le projet de règlement remplaçant la directive n° 95/46 CE et le projet de directive remplaçant la décision-cadre sur la protection des données[1760]personnelles en matière de sécurité et de justice. Ce pouvoir de conseil, en vertu duquel les autorités de protection des données peuvent être consultées par les juridictions aussi bien dans l'ordre juridique interne que dans l'ordre juridique de l'Union européenne, peut s'activer d'office sans qu'elles soient sollicitées par les juridictions. Concernant le pouvoir d'intervention, avec l'affaire *Google Spain*[1761] les autorités de contrôle se sont vues ajouter une nouvelle tâche : celle de vérifier l'existence d'un droit au déréférencement. Il s'agit d'une forme de droit d'opposition qui s'exerce auprès du moteur de recherche et non de l'éditeur du site web divulguant les données personnelles, afin de couvrir l'hypothèse où la divulgation des données personnelles correspond en réalité à une obligation légale licite[1762]. Ce droit au déréférencement est ambigu puisque l'article 17 du règlement 679/20, intitulé droit à l'oubli, ne prévoit pas la manière dont ce droit doit être mis en œuvre tout comme l'arrêt *Google Spain* de la Cour de justice. Ainsi, c'est aux autorités de contrôle d'intervenir, alternativement aux juridictions des États membres, dans le cas où le requérant ne serait pas satisfait de la réponse reçue par le moteur de recherche concernant son droit au déréférencement. L'affirmation du droit au déréférencement et sa mise en œuvre témoignent à quel point les États ne sont plus les titulaires du monopole de la production du droit[1763]. Ce droit permet à la « victime » de se tourner directement vers le moteur de recherche afin d'obtenir la suppression des liens permettant l'accès aux données divulguées. Il est possible de souligner comme la mise en balance entre l'intérêt du public à l'accès à l'information et le respect du droit à la protection des données

---

1759 Voy. Avis du G 29, Avis 7/2010 sur la communication de la Commission européenne relative à la démarche globale en matière de transfert des données des dossiers passagers (PNR) aux pays tiers, WP 178, 12 novembre 2010 ; G 29, Avis commun sur la proposition de décision-cadre du Conseil relative à l'utilisation des données des dossiers passagers (PNR) à des fins répressives présentée par la Commission le 6 novembre 2007, WP 145, 5 décembre 2007 ; G 29, Avis 3/2005 sur l'application du règlement (CE) no 2252/2004 du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres, WP 112, 4 septembre 2012.

1760 S. NERBONNE, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? », *Legicom*, 2009, n° 42, pp. 37 et s., sp. p. 41

1761 CJUE, 13 mai 2014, C-131/12, *Google Spain* SL, Google Inc. cl/Mario Costeja Gonzales e. a.

1762 O. TAMBOU, « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement », *RTD*, avril-juin 2016, p. 249.

1763 Pour une critique du droit à l'oubli: G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalita, Il diritto dell'Informazione e dell'informatica,* Milano Giuffré, *2014, p.591 et ss.* ; C. COMELLA, « Indici, sommari, ricerche e aspetti tecnici della "de-indicizzazione », *Roma Tre Press, 2015,* p. 177 et ss".

personnelles soit confiée à une entreprise privée comme Google. Cependant, les autorités de contrôle disposent du pouvoir d'intervenir dans cette mise en balance. Suite à l'affaire *Google Spain*, la Commission française Informatique et libertés (CNIL) a mis en demeure le moteur de recherche Google de procéder au déréférencement de liens portant atteinte à la protection des données personnelles sur la totalité de ses déclinaisons nationales (google.com, fr, ca, etc.). Etant en désaccord, Google a tranché pour une mise en œuvre purement européenne, bloquant l'accès des Européens (il peut s'agir aussi de non-Européens mais qui se trouvent sur le territoire européen) aux autres déclinaisons mondiales de son moteur de recherche. En réponse, la CNIL, estimant la mesure prise par Google comme insuffisante, a sanctionné la firme d'une amende de 100 000 euros[1764]. Cette dernière a saisi le Conseil d'État et l'affaire est toujours pendante du moment que le Conseil d'État a saisi la Cour de justice d'un renvoi préjudiciel. Cela illustre le difficile équilibre dans les rapports entre les différents acteurs dans un contexte de pluralisme juridique et pose des questions fondamentales quant aux entreprises privées comme productrices de droit. Ainsi assiste-on actuellement à la corégulation du droit au déréférencement par les autorités de contrôle et Google[1765]. Cela a permis l'élaboration de critères pour la mise en œuvre du droit au déréférencement qui ont fait l'objet d'une interprétation commune par les autorités nationales de protection des données réunies au sein du G29, ainsi que par les membres du comité Google[1766]. Il appartient à ces autorités de donner de manière proactive aux utilisateurs et aux fournisseurs d'Internet (en particulier des moteurs de recherche) les indications et les recommandations nécessaires pour assurer une mise en œuvre uniforme et partagée du jugement de la Cour de justice[1767]. Ainsi, au sein du G29, les autorités de contrôle ont élaboré des lignes directrices qui doivent guider l'interprétation commune des autorités nationales dans l'examen des demandes de refus de déréférencement[1768] afin d'établir une mise en balance entre l'intérêt public au maintien de l'information[1769] et la protection de la vie privée et des données personnelles. Les autorités devront prendre en compte

1764 Décis. CNIL n° 2015-047 du 21 mai 2015.

1765 G.M. RICCIO, « Diritto all'oblio e responsabilita` dei motori di ricerca; Dalla Data Retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo? », *Roma Tre Press, 2015*, p. 199 et ss ; F. PIZZETTI, « Le autorita garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: e` tempo di far cadere il "velo di Maya *" », Roma Tre Press, 2015*, p. 255 et ss. Cfr. G. FINOCCHIARO *La giurisprudenza della Corte di Giustizia in materia di dati personali da Google Spain a Schrems* », in *Dir. inf.*, 2015, p. 779 ss.; M. SIANO, Il *diritto all'oblio in Europa e il recente caso spagnolo*, in F. PIZZETTI (dir), *Il caso del diritto all'oblio*, Giappichelli, Torino, 2014, p 83. .

1766 Rapport du Comité Google : exercice d'autorégulation d'un droit à l'oubli, Dalloz actualité, Le droit en débats, 19 février 2015,http://www.dalloz-actualite.fr/cronique/rapport-du-comite-google-exercice-d-autoregulation-d-un-droit-l-oubli.VdsXk5cgy7R.

1767 M. SIANO, « Il diritto all'oblio in Europa e il recente caso spagnolo », in F. PIZZETTI, *op. citée.*

1768 Voy. « Guidelines on the implementation of the Court of Justice of the European Union judgment on *Google Spain* case part of a harmful trend of jurisdicional overreach », Robert Shuman Centre for Advanced Studies Research Paper 215, http://ssrn.com/abstract=2625908.

1769 Dans la prise en compte du droit à l'information, la CEDH pourrait reconnaître que les moteurs de recherche disposent d'un droit à la liberté d'expression qui devrait être pris en compte dans l'exercice d'un droit au déréférencement. On peut donc prévoir que lorsqu'un tiers se sentira lésé par un déréférencement, il tentera de saisir la CEDH en invoquant la liberté d'expression. Sur cette question des rapports entre CJ et CEDH : D. DERO-BUGNY, *Les rapports entre la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme*, Bruylant, 2015, coll, Droit de l'Union européenne ; E. DUBOUT, « Droits fondamentaux et pluralisme constitutionnel dans l'Union européenne », in Les droits fondamentaux dans l'Union européenne, in R. TINIÈRE et C. VIAL, Bruylant, 2015, p 107 et ss.

trois éléments : la qualité de la personne requérante[1770], la particularité de l'information dont il est demandé le déréférencement et enfin le facteur du temps. La mise en œuvre du droit au déréférencement illustre les enjeux du droit à la protection des données personnelles à l'ère numérique : ni le règlement général de la protection des données personnelles ni le juge dans l'arrêt *Google Spain* n'abordent vraiment la manière dont ce droit au déréférencement doit être mis en œuvre. Google a rapidement réagi à cette condamnation en établissant un comité consultatif chargé d'évaluer les demandes soumises au formulaire sur la suppression des données personnelles[1771], mais l'appréciation s'avère difficile si l'on considère que l'on ne peut être à la fois « juge » et « partie »[1772]. Une des conséquences de ce flou est la compétence partagée dans la mise en œuvre du droit au déréférencement entre *Google* et les autorités de contrôle nationales[1773]. Cela montre à quel point les États ne détiennent plus le monopole du droit à l'ère du numérique.

a) La mise en œuvre territoriale du droit au déréférencement

209 L'application européenne *versus* l'application mondiale du droit au déréférencement. Concernant les difficultés de la mise en œuvre du droit au déréférencement[1774], Google a mis en œuvre une approche purement européenne du droit à l'oubli qui se heurte à la vision des autorités de contrôle, lesquelles revendiquent une application mondiale du droit au déréférencement. Ainsi, le comité consultatif de Google recommande de se contenter de déréférencer les liens apparaissant sur les sites correspondant aux noms de domaines nationaux (par exemple « google.fr » ou « google.uk ») ou européens, et considère que le domaine international (google.com) ne doit pas être concerné, alors que le G29 s'est prononcé pour une suppression sur toutes les extensions du moteur de recherche. L'autorité de contrôle française (CNIL) a imposé à Google d'effacer des résultats de recherche de l'extension Google.com, pour ne pas limiter l'effectivité du droit à l'oubli au nom de domaine national Google.fr. L'affaire est pendante devant le Conseil d'État qui devra s'exprimer. Finalement, la mise en œuvre

1770 En harmonie avec la jurisprudence de la CEDH, le rôle joué par la personne dans la vie privée est un élément décisif dans l'évaluation de la mise en balance avec la liberté d'expression.

1771 Voy. le site du Comité consultatif de Google: https://www.google.com/advisorycouncil/

1772 Sous réserve de prouver son identité et d'identifier le lien litigieux aux services de Google, il est désormais possible de demander l'effacement des résultats de recherche qui incluent les données personnelles et qui seraient inadéquats, pas ou plus pertinents ou excessifs au regard des finalités du traitement. Voy. sur ce point l'article de A. Fournier, « Google lance son formulaire oubli pour les Européens », *Le Monde*, 30 mai 2014.

1773 Voy. sur cet aspet L. FLORIDI, « Right to be forgotten poses more questions than answers Google's advisory council held its final meeting last week on the European court of justice's privacy ruling. One of the council members gives his thoughts on the issues raised », *theguardian.com*, Tuesday 11 November 2014, disponible à l'adresse: https://www.theguardian.com/technology/2014/nov/11/right-to-be-forgotten-more-questions-than-answers-google.

1774 Les questions liées à l'application territoriale du droit au déréférencement pourraient faire l'objet d'un futur recours préjudiciel devant la Cour de justice.

européenne du droit au déréférencement a été acceptée par le Comité Google[1775], ce qui exprime la volonté de collaborer avec les autorités nationales de protection des données personnelles. Pourtant, dans sa vision originaire, Google voulait se fonder sur une approche nationale s'appuyant sur l'origine de la demande, car selon elle plus de 95% des utilisateurs ne cherchent qu'à travers leur version nationale[1776]. Ainsi, la portée du droit à l'effacement n'est pas limitée au territoire de l'UE. Enfin, l'article 17, § 2 du règlement prévoit que le responsable du traitement doit informer tout autre responsable de traitement ayant copié ou reproduit ces données de la demande d'effacement de ses données à caractère personnel présentée par la personne concernée. À cet égard, un des défis du droit à l'oubli est sa réalisation dans un contexte technologique (si l'on pense au stockage des données par l'informatique en nuage) pouvant donner lieu à une republication incessante des données[1777]. Il faut souligner que, même si le débat sur le besoin social d'un droit au déréférencement commence à se faire sentir, y compris aux États-Unis, il n'existe pas de consensus mondial sur le droit au déréférencement. Ainsi, une loi fédérale de 2015[1778] (loi Californienne dite *Eraser Law*) impose aux opérateurs Internet de retirer des contenus qu'un mineur aurait pu mettre sur un site. Cependant ceci est bien loin du droit au déréférencement européen, et s'applique seulement aux mineurs californiens.

b) La mise en œuvre matérielle du droit au déréférencement

210 La discrétionnalité de la mise en œuvre du droit à l'oubli par le moteur de recherche. Selon les professeurs Ost et De Kerchove, « est effective la règle utilisée par ses destinataires comme modèle pour orienter leur pratique »[1779]. Le droit au déréférencement comporte quatre types de destinataires : les individus, les moteurs de recherches, les autorités administratives indépendantes et les juges[1780]. Si la nature et le régime de ce droit restent complexes, sa mise

---

1775 Rapport du Comité Google :exercice d'autorégulation d'un droit à l'oubli, Dalloz actualité, Le droit en débats, 19 février 2015, http://www.dalloz-actualite.fr/cronique/rapport-du-comite-google-exercice-d-autoregulation-d-un-droit-l-oubli.VdsXk5cgy7R.

1776 Lettre signée P. Fleisher en réponse à la présidente du G29, disponible sur http://docs.google.com/file/d/0B8syaai6SSfiT0EwRUFyOENqR3M/edit.

1777 V. notamment le rapport de l'ENISA, « The right to be forgotten : beetween expectations and practice », Novembre 2010 p. 10.

1778 Voy. Art. 22581 du Senat Bill n° 586 Business and Professions Code appelé aussi « Privacy Rights for Minors in the digital World », http://leginfo.legislature.ca.gov./faces/billNavClient.xhtml?bill_id=201320140SB568. Le principal questionnement porte sur la compatibilité du droit au déréférencement avec la conception américaine de la liberté d'expression, selon certains auteurs cette loi serait contraire au Premier amendement sur la liberté d'expression. Voy. sur ce point E. Goldman, California's New « Online Eraser » Law Should Be Erased, 24 septembre 213, www.forbes.com/sites/ericgoldman/2013/09/24californias-new-online-eraser-law-should-be-erased/477fe36c399d.

1779 F OST., et M. VAN DE KERCHOVE., *De la pyramide au réseau, pour une théorie dialectique du droit*, publication universitaire des facultés de Saint Louis, 2002, p. 330.

1780 Les moteurs de recherche les individus utilisent ce droit, (sous le contrôle des autorités de protection des données et des juges), ce qui montre son l'utilité juridique. Ainsi 56,9 % des demandes ont donné lieu à un déréférencement. Voy. en ce sens

en œuvre par les régulateurs demeure également peu transparente. La mise en œuvre concrète de l'arrêt *Google Spain* pose un problème concernant l'absence de consensus sur le champ d'application matériel[1781] du droit à l'oubli car la Cour de justice pose une obligation de déréférencement pour les moteurs de recherche sans préciser si cela s'applique à tous les moteurs de recherche ou seulement à certains d'entre eux[1782]. Google a réagi à l'arrêt *Google Spain* avec la création d'un formulaire en ligne pour recevoir les demandes de déréférencement et a institué un comité d'expert afin d'évaluer ces demandes[1783]. Il s'agit d'une mesure non exigée par la Cour de justice, Google ayant opéré de façon autonome. Cette mesure aurait pu être prise par une évaluation de la part de l'autorité judiciaire ou de l'autorité de contrôle pour la protection des données. Ainsi, la décision a été exécutée par Google de manière discrétionnaire en exacerbant ses lacunes. Dans la décision *Google Spain*, manque l'encadrement de la procédure de désindexation et du dialogue avec les autorités de protection des données[1784]. Par conséquent, la suppression d'un contenu, surtout lorsqu'il concerne les médias en ligne, doit être soigneusement équilibrée avec la liberté d'information. À ce jour, cet équilibre ne semble pas facile, tant que la décision a été qualifiée comme censure[1785]. Le G29, dans ses lignes directrices, a apporté son interprétation en estimant qu'« en principe l'obligation de déréférencement ne devrait pas s'appliquer aux moteurs de recherche ayant un champ d'action limité »[1786]. De plus, le comité consultatif de Google recommande de se contenter de déréférencer les liens apparaissant sur les sites correspondant aux noms de domaine nationaux ou européens sans que le domaine international ne soit concerné, alors que le G29 dans ses directives demande une suppression sur toutes les extensions du moteur de recherche. Ainsi la mise en œuvre matérielle du droit au déréférencement est *de facto* dans les mains du moteur de

---

les statistiques disponibles à la page : http://www.google.com/transparencyreport/removals/europeprivacy/ et celui de Microsoft https://www. microsoft.com/en-us/about/corporate-responsibility/crrr

1781 L. FLORIDI, *Right to be forgotten: who may exercise power, over which kind of information?*, *The Guardian*, Tuesday 21 October 2014, https://www.theguardian.com/technology/2014/oct/21/right-to-be-forgotten-who-may-exercise-power-information.

1782 Trois ans après, le récent arrêt Manni atteste qu'au-de- là des moteurs de recherche, les individus peuvent obtenir d'autres acteurs la limitation de l'accès par des tiers à des données personnelles qu'ils traitent, à l'issue d'un certain délai. Voy. CJUE 9 mars 2017, Camera di Commercio c. S. Manni, aff. C-398/15.

1783Voy. Le formulaire on line sur le droit au déréférencement : Voy.https://support.google.com/legal/contact/lr_eudpa?product=websearchhttps://support.google.

1784 Compte tenu des difficultés liées à la conciliation entre les intérêts confrontés, plusieurs guides sur l'application du droit à l'oubli ont été établis. Voy. sur cet aspect : les lignes directrices du Groupe « Article 29» (Guidelines on the implementation of the Court of Justice of the European Union judgement on « *Google Spain* and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González» C-131/12, mises à jour par un rapport adopté le 16 décembre 2015) et le guide élaboré par un comité consultatif réuni sur demande de Google (The Advisory Council to Google on the Right to be Forgotten).

1785 La décision de la CJUE s'oppose aux précautions prises par la CeDH en ce qui concerne les pétitions d'effacement de données conservées par une autorité publique. Voy., dans ce sens, les arrêts de la CeDH dans les affaires S. et Marper c. Royaume-Uni (4 décembre 2008) et Brunet c. France (18 septembre 2014). Sur le premier, voy. également BELLANOVA, Rocco & P. DE HERT, *Le cas S. et Marper et les données personnelles : l'horloge de la stigmatisation stoppée par un arrêt européen*, in Culture & Conflits, 2009, vol. 76, pp. 101-114.

1786 WG29, Lignes directrices du 26 novembre 2014 » Guidelines on the implementation of the Court of Justice of the European Union judgment on *Google Spain* and inc v. Agencia española de protección de datos (aepd) and Mario Costeja González c-131/12.

recherche. Une des critiques[1787] est sans doute le manque de transparence, car Google, à l'issue de l'arrêt *Google Spain*, a mis en ligne un formulaire qui permet à toute personne d'exercer son droit au déréférencement mais sans savoir selon quelles règles et par qui les demandes sont traitées. Si la personne demandant le déréférencement n'est pas satisfaite de la décision de Google, elle pourra ensuite se tourner vers une autorité de contrôle afin de faire valoir ses droits. La logique voudrait que les acteurs qui interviennent dans la mise en œuvre du droit au déréférencement puissent avoir une coordination efficace et transparente car, actuellement, il n'existe aucune coordination entre les moteurs de recherche[1788]. Une solution pourrait être la création d'une coordination entre les moteurs de recherche grâce à la création d'un formulaire commun et l'adoption d'un code de conduite à l'échelle européenne avec l'intervention des autorités nationales de protection des données, le Comité européen à la protection des données (qui remplacera le G29) et la Commission européenne qui pourrait le déclarer par un acte d'exécution de portée générale au sein de l'UE[1789]. Le Comité consultatif mis en place par Google ne semble pas résoudre les difficultés liées à la mise en œuvre concrète du droit à l'effacement[1790]. La doctrine a tenté d'analyser juridiquement le rôle joué par Google dans la mise en œuvre du droit au déréférencement. Certains y voient une « agence administrative privée »[1791], c'est-à-dire « des entités ayant ou non un but lucratif et des organisations non gouvernementales qui exécutèrent des fonctions destinées à servir un large public par une délégation de pouvoir formelle ou informelle du gouvernement »[1792]. Pour intéressante qu'elle puisse paraître cette théorie n'est pas acceptable dans le cadre actuel car ni la Cour de justice ni aucune institution de l'Union européenne n'a jamais délégué de pouvoir à la société Google pour la mise en œuvre du droit au déréférencement. Le comité Google mène une activité totalement spontanée[1793]. En réalité, d'autres auteurs n'ont pas manqué de souligner qu'aucune « agence administrative privée » n'a été créée en exécution d'une décision de justice et que cette théorie reste purement descriptive d'un phénomène de corégulation du droit européen de la protection des données personnelles par un acteur économique transnational[1794]. D'autres

---

1787 Cette absence de transparence sur la mise en œuvre par Google du droit au déréférencement a été l'objet d'une lettre ouverte de la part de quatre-vingts universitaires, voy. « Dear Google open letter from 80 academics on "right to be forgotten"», *The Guardian*, 14 mai 2015, www.theguardian.com/technology/2015/mai/14 dear-google-open-letter-from-80-academics-on-right-to-be-forgotten-requests.

1788 B. HANDY, « Application dans l'espace de la directive 95/46/CE: la géographie du droit à l'oubli », *RTD eur*, 2014, p.879.

1789 O. TAMBOU, « Protection des données personnelles : les difficultés de la mise en œuvre du droit au déréférencement », in *RTDEur*, 2016, p 271.

1790 Ainsi tant la composition du comité (huit membres) que la mainmise ont été contestées. Voy. le Rapport of the Advisory Council to Google on the right to be forgotten, 6 février 2015.

1791 E. LEE définit ce concept comme : « des entités ayant ou non un but lucratif et des organisations non gouvernementales qui exécutent des fonctions destinées à servir un large public par une délégation de pouvoir formelle ou informelle du gouvernement. ».

1792 Voy. E. LEE préc.

1793 O. TAMBOU, « Rapport du comité Google : exercice d'autorégulation d'un droit à l'oubli », *Dalloz actualité*, 19 février 2015. Disponible à l'adresse : http://www.dalloz-actualite.fr/chronique/rapport-du-comite-google-exercice-d-autoregulation-d-un-droit-l-oubli#.VUhvlJOyLpK

arguments sur la corégulation sont en revanche pertinents comme celui concernant le manque d'impartialité de Google dans sa prise de décision (tournée notamment vers des intérêts économiques et d'accès à l'information), le manque de motivation des décisions ou le manque de possibilité d'appel de la part de Google. L'impossibilité de trouver un équilibre constant entre le droit au respect de la vie privée et l'intérêt du public à être informé soulignent l'exigence d'élaborer un cadre uniforme parmi les autorités de contrôle nationales. Le risque de la mise en œuvre du droit au déréférencement est le conflit d'interprétation avec la Cour européenne des droits de l'homme en matière de liberté d'expression ou d'information. En effet, la CourEDH semble préférer une approche nuancée du droit à l'oubli. Ainsi elle a confirmé sa jurisprudence précédente dans l'affaire *Fuchsmann c. Allemagne*[1795] et elle a conclu que le droit à la liberté d'expression (art. 10 de la Convention) prévaut sur le droit à la vie privée (art.8 de la Convention) lorsque l'information publiée contribue à un débat public et la personne concernée est une personnalité publique.

2) Le Pouvoir d'être saisies d'une demande et d'ester en justice

211 Un pouvoir quasi juridictionnel. Conformément à la Convention 108, à la Directive 95/46/CE et au règlement 679/16, la législation nationale doit prévoir des voies de recours et des sanctions appropriées contre les infractions au droit à la protection des données[1796]. Dans le droit de l'Union, le législateur national doit prévoir un recours judiciaire et un recours auprès d'une autorité de contrôle nationale[1797]. Le caractère obligatoire ou non de la prise de contact avec une autorité de contrôle avant de saisir le tribunal est laissé au législateur national. Il convient de se tourner d'abord vers le responsable du traitement qui doit donner une réponse « sans délai excessif » [1798] . Toute personne ayant déposé une demande d'accès ou s'étant opposée à un traitement ne recevant pas de réponse opportune et satisfaisante peut soumettre une demande d'assistance à l'autorité nationale de contrôle des données personnelles [1799] . Contre toute décision rendue par des autorités nationales de contrôle, il est possible de former un recours devant les tribunaux nationaux[1800] . Conformément à l'article 28, paragraphe 4, section 1, de la directive relative à la protection des données, les autorités de contrôle devraient

1794 O. TAMBOU, « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement », in *RTDeur*, 2016, p.271.

1795 Le texte intégrale de l'arrêt est disponible à l'adresse : https://hudoc.echr.coe.int/eng#{"itemid":["001-177697"]}

1796 Ainsi l'article 22 de la directive relative à la protection des données codifie l'obligation générale pour les États membres de prévoir : « sans préjudice du recours administratif qui peut être organisé, toute personne dispose d'un recours juridictionnel en cas de violation des droits qui lui sont garantis ».

1797 Les recours possibles sont : a) recours administratifs devant l'autorité de protection des données ; b) recours non juridictionnels devant l'autorité de contrôle (en tant qu'alternative à une action judiciaire, qui, une fois commencée, empêchent toute réclamation devant une autorité judiciaire) ; c) recours juridictionnels, disponibles devant un tribunal ordinaire.

1798 Article 12 de la directive 95/46/ CE et l'article 8 point b) de la Convention108.

1799 Article 28,§4 de la directive 95/46/ CE.

1800 Cela vaut pour toute personne partie à la procédure, aussi bien pour la personne concernée que pour le responsable du traitement.

bénéficier du pouvoir d'être saisies par toute personne, ou par une association les représentant, d'une demande relative à la protection de ses droits et libertés à l'égard du traitement de données à caractère personnel et d'informer la personne concernée des suites données à sa demande. La possibilité d'intervention pour les associations a été renforcée avec le règlement 679/16: la personne concernée a le droit de mandater un organisme, une organisation ou une association à but non lucratif, qui a été valablement constitué conformément au droit d'un État membre, dont les objectifs statutaires sont d'intérêt public et qui est actif dans le domaine de la protection des droits et libertés des personnes concernées dans le cadre de la protection des données à caractère personnel les concernant, pour qu'il introduise une réclamation en son nom, exerce en son nom les droits de recours visés par le règlement et exerce en son nom le droit d'obtenir réparation lorsque le droit d'un État membre le prévoit. Conformément à l'article 28, paragraphe 3, section 1, troisième tiret, les autorités de protection des données doivent pouvoir ester en justice en cas de violation des dispositions nationales en matière de protection des données ou porter ces violations à la connaissance de l'autorité judiciaire. Enfin, l'article 28, paragraphe 3, section 1, deuxième tiret, permet aux autorités de contrôle de saisir les parlements nationaux ou d'autres institutions politiques. Ainsi, les autorités de contrôle peuvent: entendre et examiner les demandes et réclamations de personnes concernées; porter l'affaire à la connaissance de la police ou des autorités judiciaires; porter directement l'affaire devant les autorités judiciaires en tant que partie à la procédure devant les tribunaux (à savoir, pouvoir d'ester en justice au sens strict) ; prendre de leur propre chef une décision quant à l'existence ou non d'une violation (avec la possibilité d'infliger une sanction) assurant ainsi une fonction quasi judiciaire; saisir le parlement national ou les institutions politiques, notamment en proposant des mesures législatives et réglementaires en vue de modifier la législation correspondante en matière de protection des données pour traiter les problèmes les plus importants découlant de sa demande et refléter l'évolution des techniques informatiques. Toutes les autorités de contrôle peuvent être saisies par des parties intéressées alléguant une violation de leurs droits en matière de données à caractère personnel et ont le devoir correspondant de leur apporter une réponse dans un délai donné. Si, suite à l'examen, la plainte se révèle fondée, elles peuvent exercer elles-mêmes une fonction quasi judiciaire en décidant du bien-fondé de l'affaire portée par le requérant (en tant qu'alternative aux tribunaux). Les décisions des autorités de contrôle administratives disposant de pouvoirs quasi judiciaires peuvent dans tous les cas être révisées par les tribunaux ordinaires. Il s'agit du corollaire nécessaire de la règle de droit établie à l'article 28, paragraphe 3, section 2, de la directive relative à la protection des données. Conformément à l'article 24 de la directive relative à la protection des données, les États membres sont tenus de « déterminer notamment les sanctions à appliquer en cas de violation » de la législation en matière de protection des données. Diverses sanctions peuvent être imposées par les autorités de protection des données. Au-delà de l'avertissement ou de l'admonestation au sous-traitant et au responsable des traitements, l'autorité de contrôle peut ordonner la suspension du traitement de données à caractère personnel, le verrouillage et l'effacement de données. Elle est également habilitée à ordonner des sanctions pécuniaires. Toutefois, les dispositions de la directive relative à la protection des données concernant les recours, les sanctions et la responsabilité ne fixent que l'objectif à atteindre par les États membres sans préciser de critères détaillés à respecter. On constate un certain nombre de différences parmi les États membres. C'est pour cette raison que le nouveau règlement a

uniformisé le pouvoir de sanction des autorités. Les pouvoirs de sanction ont été renforcés car une injonction sans sanction n'est pas efficace. Des amendes jusqu'à 10 millions d'euros ou 2% du chiffre d'affaire mondial sont prévues pour sanctionner l'entreprise qui ne serait pas organisée de manière conforme au règlement. Les amendes de type 20 millions d'euros ou 4% du chiffre d'affaire mondial sont destinées à sanctionner tout non-respect des droits accordés aux personnes dont les données sont traitées, ainsi que le non-respect des règles de transfert hors UE. Les tribunaux peuvent également ordonner des sanctions pécuniaires, voire des peines d'emprisonnement ou leurs alternatives, telles qu'une peine avec sursis ou des travaux d'intérêt général. Conformément à l'article 23, paragraphe 1 de la directive relative à la protection des données, les États membres « prévoient que toute personne ayant subi dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales prises en application de la présente directive a le droit d'obtenir du responsable du traitement réparation du préjudice subi ». Toutefois, la législation nationale sur la responsabilité civile varie selon la décision des États membres de réglementer spécifiquement le devoir de réparer les dommages subis dans une affaire relative à la protection des données, ou de prévoir simplement une extension du cadre ordinaire de la responsabilité civile au domaine de la protection des données à caractère personnel. Cependant, si le droit à la protection des données garanti par les articles 16 du TFUE et 8 de la Charte a été violé par les institutions ou organes communautaires, la personne concernée peut former une réclamation auprès du CEPD[1801]. En l'absence de réponse du CPD dans un délai de six mois, la réclamation est présumée rejetée.

Les effets juridiques des résultats de la procédure devant les autorités de contrôle nationales dépendent du droit national. Dans certains États membres, les décisions de l'autorité peuvent être légalement exécutées[1802]. Dans d'autres, il est nécessaire de faire appel à un tribunal si le responsable du traitement ne suit pas la décision de l'autorité de contrôle.

3) La compétence de l'autorité chef de file et la coopération avec les autres autorités de contrôle

212 **Une solution de *consensus.*** Lorsqu'il y a un traitement transfrontalier des données[1803], la compétence sera de l'autorité du chef de file de l'établissement principal afin d'éviter le « *data*

1801 L'autorité indépendante de contrôle de la protection des données aux termes du règlement 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données.

1802 C'est-à-dire : sont-elles exécutables par une autorité officielle ?

1803 Voy. Article 4. 23) du RGPD : un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres; ou b) un traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres.

shopping ». Ainsi en présence d'un traitement transfrontière, le RGPD prévoit une compétence de principe au profit de « l'autorité chef de file » et un mécanisme de coopération entre cette autorité et les autres autorités de contrôle nationales. Ces solutions techniques garantissent l'indépendance des organes de contrôle, en limitant l'influence et les pressions des pouvoirs politiques. En cas de traitement transfrontière, la compétence revient à l'autorité de contrôle de l'État membre dans lequel est situé soit l'établissement unique du responsable du traitement ou du sous-traitant, soit à défaut (s'il existe plusieurs établissements au sein de l'Union) l'établissement « principal » du responsable du traitement ou sous-traitant[1804].

Par « établissement principal », il est entendu : en ce qui concerne un responsable du traitement établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union, à moins que les décisions quant aux finalités et aux moyens du traitement de données à caractère personnel soient prises dans un autre établissement du responsable du traitement dans l'Union et que ce dernier établissement a le pouvoir de faire appliquer ces décisions, auquel cas l'établissement ayant pris de telles décisions est considéré comme l'établissement principal ; en ce qui concerne un sous-traitant établi dans plusieurs États membres, le lieu de son administration centrale dans l'Union ou, si ce sous-traitant ne dispose pas d'une administration centrale dans l'Union, l'établissement du sous-traitant dans l'Union où se déroule l'essentiel des activités de traitement effectuées dans le cadre des activités d'un établissement du sous-traitant.[1805]

Le législateur a souhaité unifier les règles de compétence territoriales des autorités de contrôle en créant la notion d'autorité chef de file. Par exception, chaque autorité de contrôle nationale reste compétente si le traitement transfrontalier génère une réclamation ou est à l'origine d'une violation[1806] si l'objet concerne exclusivement un établissement dans l'État membre sont relève l'autorité nationale concernée, ou si les conséquences du traitement des données affectent uniquement des personnes concernées dans l'État membre où l'autorité de contrôle nationale est établie. Afin de permettre une application cohérente et harmonieuse de la réglementation au sein du marché intérieur, le RGPD prévoit un « mécanisme de coopération »[1807] entre l'autorité chef de file et les autres autorités de contrôle concernées. Afin de prendre une décision, l'autorité chef de file doit essayer de parvenir à une solution de consensus, elle doit soumettre son projet de décision aux autres autorités de contrôle concernées en vue d'obtenir leur avis. Les autres autorités sont tenues à rendre leur avis dans le délai de quatre semaines. Ainsi en cas d'objection formulée par une autorité de contrôle, l'autorité chef de file peut : rejeter ou nepas examiner l'objection mais elle doit soumettre l'objection au Comité européen de la protection des données, celui-ci examinera la question en adoptant une décision contraignante[1808]; où elle peut suivre l'objection en soumettant aux autres autorités de contrôle le projet de décision révisé afin d'obtenir leur avis dans un délai de deux semaines. En absence d'avis la décision est approuvée.

1804 Voy. Art. 56 RGPD.

1805 Voy. Art. 4.16 RGPD.

1806 Voy. Art. 56.2 RGPD.

1807 Voy. Article 60 RGPD.

1808 Voy. Article 65 RGPD.

Section II. Des actions de sensibilisation à l'égard du droit à la protection des données personnelles

213 Le rôle des acteurs non institutionnels. Depuis l'adoption de la directive 95/46, cette législation reste encore fort méconnue de la part des citoyens et peu d'entre eux exercent les droits qui leurs sont attribués. Toutefois, dans nos sociétés informatisées le respect de ces règles est essentiel. Les citoyens doivent prendre conscience des enjeux pour leur vie privée afin de les maîtriser. La réforme de la législation de l'Union concernant le droit à la protection des données personnelles entamée en 2012 s'inscrit dans cette démarche. En effet, le droit à la protection des données personnelles peut aussi accroître le rôle d'acteurs non institutionnels tels que les individus eux-mêmes ou les associations de protection des droits fondamentaux qui composent la société civile. La société civile pourrait ainsi participer à la mise en œuvre de ce droit. Pour y parvenir il semble nécessaire que les autorités de protection des données s'efforcent tout particulièrement de cultiver leur image de gardiennes indépendantes du droit fondamental à la protection des données et qu'elles se concentrent sur la sensibilisation culturelle plutôt que sur leur rôle politique/législatif. La participation de la société civile à la mise en œuvre du droit à la protection des données personnelles s'inscrit dans le mouvement général de démocratisation des processus décisionnels [1809] . Ainsi, de toutes les autorités indépendantes, les autorités de contrôle de la vie privée sont celles qui ont su établir le meilleur dialogue avec la citoyenneté. À cette fin, elles ont mis en place leurs site web officiel où elles publient leurs interventions et les services mis à la disposition des utilisateurs[1810]. Toutefois, il est possible de relever que certaines autorités de protection des données ne se sont pas consacrées aux actions de sensibilisation (par exemple, l'Estonie et la Roumanie). Ainsi, dans certains États membres (comme en Bulgarie, en Lituanie, et en Slovaquie), les autorités de contrôle n'ont pas encore mis en place de site web convivial ou complet permettant au public d'accéder à toutes les informations sur la protection des données et de consulter facilement les avis et les règlements élaborés par l'autorité de protection des données. De plus, des préoccupations concernant la publicité et la transparence effectives des activités de l'autorité de protection des données ont été soulevées dans certains pays (comme en Bulgarie et à Malte), notamment lorsque l'autorité de contrôle négocie des résolutions à l'amiable des différends avec les contrevenants à la loi relative à la protection des données, sans les rendre accessibles au public (par exemple, au Royaume-Uni)[1811].

1809 J. RIVERO, *L'administration face au droit administratif*, AJDA, 1995, pp. 147 et s. ; J. RIVERO, *A propos des métamorphoses de l'administration d'aujourd'hui : démocratie et administration*, Pages de doctrine, Tome 1, p. 821.

1810 U. DE SIERVO, *Tutela dei dati personali e riservatezza, in Diritti, nuove tecnologie, trasformazioni sociali. Scritti in memoria di Paolo Barile*, Cedam, Padova, 2004, 298.

1811 Voy. Rapport de l'Agence des droits fondamentaux précitée, p. 48.

Ainsi, la participation de la société civile peut se réaliser seulement s'il y a une coopération avec les pouvoirs publics. Toutefois, on constate que ni dans l'ancien texte de la directive 95/46 ni dans le règlement 679/16, il n'existe l'obligation d'information de la société civile en matière de protection des données personnelles. Il n'existe pas non plus, dans les ordres juridiques des États membres, une obligation qui imposerait aux autorités publiques de prévoir la participation de la société civile au processus décisionnel. L'importance de cette mission d'information à destination de la société civile est de plus en plus nécessaire face à la diminution de la vigilance citoyenne. Ainsi, la participation de la société civile à la mise en œuvre du droit à la protection des données personnelles ne résulte pas d'une institutionnalisation mais d'une action spontanée (§1). Toutefois, le législateur a prévu dans l'article 37 du RGPD, la désignation d'un *Data protection Officer* (ci-après DPO). Cela montre que le législateur est attentif à la sensibilisation des acteurs non institutionnels mais qui participent à l'application et mise en œuvre du droit à la protection des données. Deplus, le règlement a renforcé les obligations pesant sur le responsable du traitement afin de responsabiliser en amont les acteurs participant à la mise en œuvre du droit à la protection des données personnelles (§2).

§1. Le rôle de la société civile

Le droit à la protection des données personnelles a permis aux autorités institutionnelles, comme les autorités de contrôle, de jouer un rôle quasi juridictionnel. Ce droit pourrait aussi accroître le rôle des acteurs non institutionnels tels que les individus eux-mêmes ou les associations de protection des droits fondamentaux qui composent la société civile. La société civile est une notion floue qui a évolué au fil du temps. De plus, le droit positif ne la définit pas. C'est la doctrine qui l'a expliquée comme un phénomène juridique tels que l'intervention des groupements et/ou des individus sur des problématiques générales, notamment dans certaines branches du droit[1812]. Selon J. Habermas, la société civile est constituée de l'ensemble des acteurs non institutionnels ayant pour objectif d'exercer une influence sur les sujets d'intérêts général[1813]. La participation accrue de la société civile est essentielle à la mise en œuvre efficace des règles concernant la protection des données personnelles[1814].

1812 A. POMADE, *La société civile et le droit de l'environnement. Contribution à la réflexion sur les théories des sources du droit et de la validité*, LGDJ, coll. Bibliothèque de droit privé, t. 523, 2010, 698 p., sp. p. 4.

1813 J. HABERMAS, *Droit et Démocratie*, Gallimard, 1997, 551 p., sp. p. 394 : « La société civile se compose de ces associations, organisations et mouvements qui à la fois accueillent, condensent et répercutent en les amplifiant dans l'espace public politique, la résonance que les problèmes sociaux trouvent dans les sphères de la vie privée. Le cœur de la société civile est donc constitué par un tissu associatif qui institutionnalise dans le cadre d'espaces publics organisés les discussions qui proposent de résoudre les problèmes surgis concernant les enjeux d'intérêt général ». Pour une analyse de la définition de J. HABERMAS v. A. POMADE, *La société civile et le droit de l'environnement. Contribution à la réflexion sur les théories des sources du droit et de la validité*, préc., sp. p. 8.

1814 J. FRAYSSINET, « La régulation de la protection des données personnelles », *Legicom*, 2009, n° 42, p. 5-9.

A cet égard, le nouveau règlement renforce le rôle de la société civile et établit que les États membres, les autorités de contrôle, le Comité et la Commission doivent encourager l'élaboration de codes de conduite par les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants, puisque les codes de conduites sont destinés à contribuer à la bonne application du règlement. L'autorité de contrôle rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le règlement et approuve le projet. Lorsque le projet de code, la modification ou la prorogation sont approuvés et lorsque le code de conduite concerné ne porte pas sur des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle enregistre et publie le code de conduite. Toutefois, il est possible de remarquer que si la participation de la société civile à l'application des règles s'est progressivement développée, elle demeure insuffisante (A) et la participation de la société civile à l'élaboration des normes juridiques en matière de protection des données personnelles est très faible, voire presque inexistante (B).

A. La participation croissante de la société civile à l'application des règles

214 Une sensibilisation progressive. La possibilité pour la société civile d'avoir accès aux informations et de participer à l'élaboration des normes juridiques s'inscrit dans le mouvement général de démocratisation des processus décisionnels [1815] . Toutefois, le droit positif à la protection des données personnelles ne prévoit pas une telle participation de la société civile. Un pas en avant vers la démocratisation des règles a été accompli par le nouveau règlement en matière de protection des données car il prévoit une nouvelle mission des autorités de contrôle, consistant dans l'information et la sensibilisation du public, dans sa compréhension des risques, des règles, des garanties et des droits relatifs au traitement. De plus, il est prévu que les activités destinées spécifiquement aux enfants font l'objet d'une attention particulière. Il est possible de remarquer une prise de conscience de l'importance de l'information des citoyens par les autorités de contrôle. Conscient du rôle de la société civile dans la mise en œuvre du droit à la protection des données personnelles, le législateur a prévu dans ce règlement que tout organisme, organisation ou association œuvrant dans le domaine de la protection des données personnelles, peut introduire une réclamation auprès d'une autorité de protection des données personnelles au nom d'une ou de plusieurs personnes concernées, ou de manière indépendante. Il est à noter que certains ordres juridiques nationaux prévoyaient déjà des recours collectifs. Tel est le cas de la Cour constitutionnelle allemande saisie par 34 939 personnes contre la loi allemande transposant la directive de 2006/46/CE. La Cour constitutionnelle autrichienne a également été saisie par 11 130 personnes d'un recours contre la loi autrichienne transposant la même directive. Ce qui a conduit le juge national à poser une question préjudicielle à la Cour

1815 H. MAISL, *Formes et techniques de participation du public à l'élaboration d'actes législatifs et administratifs*, in CONSEIL DE L'EUROPE, AFFAIRES JURIDIQUES (dir.), *Formes de participation du public à l'élaboration des actes législatifs et administratifs – Actes du 7ème colloque de droit européen*, Strasbourg, 1978, pp. 15 et s., sp. p. 16.; F. VAN DER BURG, *Participation et représentation des intérêts*, in Conseil de l'Europe, affaires juridiques (dir.), *Ibid*., p. 45-49.

de justice sur la conformité de cette directive aux droits fondamentaux garantis dans l'ordre juridique de l'Union européenne. Le renvoi préjudiciel a eu comme conséquence une déclaration d'invalidé de la directive 2006/24 *ab initio* par la Cour de justice [1816]. Il semble nécessaire alors d'affirmer l'existence de « class-actions » dans ce domaine[1817]. L'impossibilité d'exercer de telles actions, à finalité davantage répressive qu'indemnitaire, est analysée comme une entrave à l'application effective des règles portant sur la protection des données personnelles[1818]. En France, la loi du 17 mars 2014 relative à la consommation, dite « loi Hamon », introduit l'action de groupe en droit français. Elle est cependant réservée aux associations de défense des consommateurs qui pourront agir en vue d'obtenir la réparation des préjudices patrimoniaux résultant des dommages matériels subis par les consommateurs. Mais, il n'existe à ce jour en France aucune association de consommateurs spécifiquement dédiée aux questions de protection des données. Toutefois, puisqu'il n'existe pas d'obligation d'information en matière de protection des données personnelles de la part des pouvoirs publiques vis-à-vis de la société civile, l'exercice des droits des citoyens face à l'utilisation des données personnelles est particulièrement difficile et engendre un problème d'efficacité des normes en la matière. En effet, l'exercice d'un droit particulier peut avoir des conséquences sur l'intérêt collectif[1819] . L'enjeu semble être de donner au citoyen les clés lui permettant de comprendre l'essence des risques pour l'exercice de ses libertés, et les autorités de contrôle devront transmettre les valeurs civiques dans la société de l'information [1820] . Cependant, l'obligation d'information pèse sur les autorités de contrôle seulement vis-à-vis des institutions. Celles-ci doivent établir un rapport annuel remis aux pouvoirs publics rendant compte de leurs activités[1821]. Cette tâche d'information des autorités de protection des données personnelles vis-à-vis de la société civile est encore moins importante dans l'ordre juridique de l'Union

---

1816 CJUE, G. Ch., 8 avril 2014, Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres, aff. C-293/12 et C-594/12

1817 Celles-ci sont perçues par la doctrine comme un moyen efficace d'assurer l'application effective des règles relatives à la protection des données personnelles. Voy. P. M. SCHWARTZ, *Property, privacy and personal data*, p. 2112 : « Data trading laws should also allow private rights of action, including class actions, when privacy rights are violated. Such rights of action can be highly effective in increasing compliance with statutory standards ».

1818 P. HUSTINX, « The Role of Data Protection Authorities », in in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (dir.), *Reinventing Data Protection ?*, p. 131 et s., séec. p. 136-137 : « it seems appropriate to also consider introducing the possibility of class actions, empowering groups of citizens to jointly use litigation in matters concerning protection of personal data, as well as actions, initiated by legal persons whose activities are designed to protect the interest of certain categories of persons, such as consumer associations and trade union. Both might be a powerful tool to facilitate the enforcement of data protection law in various situations ».

1819 Y. DETRAIGNE, A.-M. ESCOFFIER, « *Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques* », préc., sp. p. 67.

1820 A. TÜRK, *La vie privée en péril, des citoyens sous contrôle*, Odile Jacob, 2011, p.17.

1821 Agence des droits fondamentaux de l'Union européenne, La protection des données à caractère personnel dans l'Union européenne : le rôle des autorités nationales chargées de la protection des données – Renforcement de l'architecture des droits fondamentaux au sein de l'UE II, préc., sp. p. 28.

européenne. En effet, ni le CEPD[1822] ni le G 29 n'ont cherché à développer cette mission d'information. Cela est flagrant dans le rapport annuel publiés par le CEPD et le G 29[1823] qui demeure essentiellement un outil de communication avec les institutions européennes [1824] . L'accès à l'information de la société civile est une condition préalable à la possibilité d'association au processus décisionnel[1825]. Toutefois, si l'exigence d'information de la société civile est ressentie afin d'appliquer de manière efficace la législation, la participation de cette dernière au processus normatif est quasi inexistante.

B. La participation insuffisante de la société civile à l'élaboration des règles

215 L'absence d'un pouvoir d'influence dans le processus décisionnel. En général, les procédures participatives de la société civile peuvent se réaliser à travers la simple consultation qui permet de recueillir les réserves de la société civile, et à travers la concertation, qui permet d'associer la société civile à la décision finale. Or, dans le droit à la protection des données personnelles, la société civile n'est pas titulaire d'un droit de participation au processus décisionnel. Elle ne peut faire entendre sa voix que dans son opposition aux pouvoirs publics lors de l'élaboration des normes juridiques. Il est possible de remarquer l'absence d'un pouvoir d'influer dans le processus décisionnel, alors que dans d'autres domaines, comme l'environnement et la bioéthique, la prise de décision a été associée à des débats démocratiques avec la société civile[1826].
Une institutionnalisation de la procédure de consultation pourrait être adoptée en matière de protection des données personnelles si l'on considère que plusieurs questions concernent des situations délicates, comme le rôle de la technologie dans notre vie privée, et posent des interrogations morales et philosophiques qui intéressent la société civile. La prise de décision dans ces domaines mérite un débat ouvert. En l'absence d'un droit de participation au processus décisionnel le seul instrument pour se faire entendre est l'opposition aux pouvoirs publics.

1822 L'information de la société civile ne relève pas comme l'une de ses trois missions selon la présentation qui en est faite sur son site Internet : supervision, coopération, consultation

1823 De même, le G29 s'adresse aux Institutions. Voy. S. NERBONNE, « Le Groupe de l'article 29 est-il en mesure de s'imposer comme le régulateur des régulateurs par ses prises de position ? » préc., spéc p. 40.

1824 Art. 48 du règlement n° 2001/45 CE et art. 30 de la directive n° 95/46 CE.

1825 H. MAISL, « Formes et techniques de participation du public à l'élaboration d'actes législatifs et administratifs, in Conseil de l'Europe », Affaires juridiques (dir.), *Formes de participation du public à l'élaboration des actes législatifs et administratifs – Actes du 7ème colloque de droit européen*, Strasbourg, 1978, pp. 15 et s., sp. p. 16.; F. VAN DER BURG, « Participation et représentation des intérêts », in Conseil de l'Europe, affaires juridiques (dir.), Ibid., pp. 45 et s., sp. p. 49.

1826 Sur ce constat en droit de l'environnement : A. POMADE, *La société civile et le droit de l'environnement. Contribution à la réflexion sur les théories des sources du droit et de la validité*, préc., sp. p. 137 ; Concernant la prise de décision dans le domaine de la bioéthique voy. S. MONNIER, « Les États généraux de la bioéthique et le Parlement », *RDP*, 2011, pp.1557 et s. Ces états généraux ont eu un certain succès auprès des parlementaires qui ont décidé d'institutionnaliser, pour l'avenir, ce procédé dans la loi de bioéthique. Cela a conduit à consacrer le caractère obligatoire de cette procédure au départ simplement facultative.

Ainsi, à défaut d'instruments juridiques permettant à la société civile d'intervenir dans la prise de décision, celle-ci peut agir de manière spontanée [1827] . Des associations sont parfois intervenues devant la Cour européenne des droits de l'homme dans des affaires importantes relatives à l'utilisation des données personnelles [1828] . Le nouveau règlement 679/2016 a institutionnalisé cette procédure en prévoyant la possibilité pour tout organisme, organisation ou association œuvrant dans le domaine de la protection des données personnelles d'introduire une réclamation auprès d'une autorité de protection des données personnelles au nom d'une ou de plusieurs personnes concernées ou de manière indépendante[1829]. Toutefois un tel recours à une action collective n'est pas prévu devant les juridictions mais seulement devant l'autorité de contrôle. Il est possible de remarquer qu'au niveau européen, le schéma des recours possibles est en pleine évolution, avec une montée en puissance du rôle joué par les associations et la société civile. De plus, toute personne peut également agir contre les décisions d'une autorité de contrôle, cette dernière étant obligée de donner suite à sa réclamation. Lorsque l'autorité de contrôle se trouve dans un pays de l'Union dans lequel cette personne n'a pas sa résidence principale, celle-ci peut solliciter l'autorité de contrôle de son pays de résidence pour qu'elle agisse en son nom. Cette possibilité vise à régler les difficultés qui se posent lorsque les données d'un citoyen européen sont traitées dans un autre pays membre et que celui-ci ne parvient pas à faire respecter ses droits. La personne qui s'estime victime d'une violation pourra également intenter une action directement à l'égard du responsable ou du sous-traitant soit auprès de la juridiction où se situe leurs établissements, soit auprès de la juridiction dans laquelle elle a elle-même sa résidence principale. Toutefois, la doctrine a relevé à plusieurs reprises la rareté de l'action de l'individu en réparation du préjudice. Cela s'explique par le fait que pour agir en justice il faut être capable de savoir qu'une collecte a eu lieu. Or, certaines collectes sont « invisibles ». Pour remédier à ces difficultés, il a été suggéré, d'une part, de renforcer le rôle d'information et de pédagogie des autorités de contrôle auprès de l'individu[1830] et, d'autre part, d'accroître le rôle des associations sur le modèle d'une association de consommateurs pour aider la personne dans cette phase de la procédure en lui apportant conseils et soutien. Le rôle des associations est perçu par la doctrine du système juridique américain comme un moyen efficace de combattre la passivité de l'individu et d'assurer la mise en œuvre efficace des règles

---

1827 E. DESMONS, « Résistance à l'oppression », in J. ANDRIANTSIMBAZOVINA, H. GAUDIN, J.-P. MARGUENAUD, S. RIALS, F. SUDRE (dir.), *Dictionnaire des droits de l'homme*, préc., pp. 854 et s.

1828 Voy. CEDH [GC], 4 décembre 2008, S. et Marper c/ Royaume-Uni, req. n°30562/04 et n°30566/04, Rec. 2008, §§ 56-57 : Le National Council for Civil Liberties (« Liberty ») « a soumis certains éléments jurisprudentiels et scientifiques illustrant notamment le caractère hautement sensible des échantillons cellulaires et profils ADN » et Privacy International « a invoqué certains principes et règles fondamentaux en matière de protection des données élaborés par le Conseil de l'Europe » et « a fourni un résumé des données comparatives sur le droit et la pratique dans différents pays s'agissant du stockage de données ADN et relevé l'existence de nombreuses limitations et garanties dans ce domaine ». Il est notable de relever que la Cour a consacré ce caractère hautement sensible et s'est appuyé sur l'absence l'existence d'un dénominateur commun en Europe pour exercer un contrôle approfondi et sanctionné la législation britannique.

1829 Voy. art. 57 f du règlement 679/2016.

1830 G. DESGENS-PASANOU, *Informatique et Libertés : une équation à plusieurs inconnues*, préc. p. 86.

relatives à la protection des données personnelles[1831]. Ainsi, comme l'a souligné le législateur français : « si les États-Unis protègent peut-être un peu moins *de jure* les données personnelles privées, les quelques lois en vigueur sont *de facto* rigoureusement appliquées. Les associations de consommateurs, tout comme certaines associations spécialisées dans la protection des données, sont particulièrement puissantes »[1832] . L'importance de reconnaître une action de groupe en la matière a été suggérée par la doctrine[1833] et par la Commission européenne suite à une recommandation du 11 juin 2013 sur les recours collectifs[1834] qui préconisait un champ d'application beaucoup plus large. Pour la Commission, de tels recours collectifs devraient s'appliquer de manière identique dans les domaines de la concurrence et de la consommation mais aussi dans ceux de la protection de l'environnement, de la protection des données personnelles, de la réglementation des services financiers, de la protection des investisseurs mais aussi dans ceux « où les demandes collectives en cessation ou en dommages et intérêts en cas de violation des droits conférés par le droit de l'Union présenteraient un intérêt ». Malgré de nombreuses réflexions sur le rôle qu'une telle « *class action* » pourrait avoir en matière de protection des données personnelles, les mécanismes de recours collectifs sont encore peu développés et faiblement encouragés comme moyen d'assurer l'application du droit à la protection des données personnelles. Il semble que, en attendant une prise de position du législateur sur la possibilité d'action collective en matière de protection des données, il revient aux personnes dont les données sont traitées de jouer un rôle accru dans la mise en œuvre des règles. Leur absence de maîtrise intellectuelle sur les données pourra être remplacée par la mise en place d'associations dans la société civile capables de prendre le relai pour assurer la protection effective des données personnelles. Une pratique encourageante concernant la réflexion sur le rôle de la société civile semble être celle prévue par le règlement et qui encourage l'élaboration de codes de conduite. Ainsi, les associations et autres organismes professionnels représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, des procédures de certification ou de labélisation et les

---

1831 P. M. SCHWAERTZ, « Property, privacy and personal data », préc., sp. p. 2112 : « Data trading laws should also allow private rights of action, including class actions, when privacy rights are violated. Such rights of action can be highly effective in increasing compliance with statutory standards ».

1832 Y. DETRAIGNE, A.-M. ESCOFFIER, « Rapport d'information fait au nom de la commission des Lois constitutionnelles, de législation, du suffrage universel, du Règlement et d'administration générale par le groupe de travail relatif au respect de la vie privée à l'heure des mémoires numériques », p. 96.

1833 P. HUSTINX, « The Role of Data Protection Authorities », in in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (dir.), *Reinventing Data Protection ?*, préc., pp. 131 et s., sp. pp. 136-137 : « it seems appropriate to also consider introducing the possibility of class actions, empowering groups of citizens to jointly use litigation in matters concerning protection of personal data, as well as actions, initiated by legal persons whose activities are designed to protect the interest of certain categories of persons, such as consumer associations and trade union. Both might be a powerful tool to facilitate the enforcement of data protection law in various situations ».

1834 Voy. Recommandation de la Commission européenne du 11 juin 2013 relative aux principes communs applicables aux mécanismes de recours collectif en cessation et en réparation dans les États membres en cas de violation de droits conférés par l'Union européenne.

modifier ou les proroger aux fins de préciser les modalités d'application du règlement. Ces codes de conduite doivent être approuvés par l'autorité de contrôle[1835].

Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite. Mais jusqu'à présent le recours et la délivrance de ces codes de conduite est resté marginal. Quoi qu'il en soit, la pratique des codes de conduites montre l'influence du modèle d'autorégulation anglo-saxon[1836].

§2. Les autres acteurs du droit à la protection des données personnelles

216 Du « CIL » au « DPO ». Suite aux transpositions de la directive 95/46, plusieurs États membres avaient créé la fonction de correspondant informatique et libertés[1837]. Toutefois sa désignation n'était pas obligatoire [1838] . Il faut souligner une évolution en la matière puisqu'aujourd'hui, la fonction de CIL est le pivot de la réforme du régime européen de protection des données à caractère personnel et se situe au cœur de l'application du principe d'*accountability*, témoignant ainsi d'une nouvelle pratique de gouvernance basée sur l'approche de « corégulation » entre organismes publics et privés[1839]. La fonction de CIL n'est pas nouvelle. En France, elle est née avec la transposition en 2004 de la directive de 1995 ; en Allemagne, le « chargé de la protection des données » fait figure de précurseur car il existe depuis 1977 pour le secteur privé et sa fonction a été étendue au secteur public en 2001. Même aux États-Unis, suite à une série de scandales à la fin des années 1990, les sociétés américaines ont instauré des « *Chief Privacy Officer* »[1840]. Ces mécanismes ont inspiré la directive de 1995 laquelle avait envisagé la possibilité pour les États membres de désigner un « détaché à la protection des données » pour les dispenser de certaines formalités auprès de l'autorités de contrôle. Ainsi, le correspondant informatique et liberté a vu son rôle grandir au fil du temps sous l'impulsion des autorités de contrôle et des organisations professionnelles. De plus, le règlement 679/16, dans la continuité de la directive 95/46, a reconnu un rôle central au délégué à la protection des données. Son statut est redéfini et devient obligatoire dans certains cas. Le

1835 A. PANNEAU, « Certification et codes de conduites privée », *in La proposition de règlement européen relatif aux données à caractère personnel : propositions du réseau Trans Europe Expert,* Société de législation comparée, collection Trans Europe Expert, 2014, spéc. P. 345.

1836 A. DEBET J. MASSOT, N. METALLINOS, *Informatique et libertés, la protection des données à caractère personnel en droit français et européen*, Lextenso éditions, 2015, p. 852-855.

1837 La fonction de délégué à la protection des données n'est pas obligatoire seulement dans des secteurs spécifiques. Ainsi plusieurs États membres ont opté par la désignation du CIL : Allemagne, Belgique, Estonie, France, Grèce, Hongrie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Slovaquie, Suède.

1838 E. CAPRIOLI et I. CANTERO, « Le choix d'un correspondant à la protection des données à caractère personnel », *JCPE* 22 juin 2006, n°25, p. 1104-1108.

1839 G. DESGENS-PASANOU et F. NAFTALKI, « Projet de règlement européen sur la protection des données : ce qui va changer pour les professionnels, » *RLDI* 2012/80, N° 2693.

1840 N. METALLINOS, « Maîtriser le risque Informatique et libertés. La mise en place du Correspondant Informatique et Libertés », *Dr. Soc*., 2006, N°4, p.378.

règlement impose la désignation du DPO dans le secteur public[1841] où plusieurs institutions publiques peuvent désigner un DPO commun [1842] et, dans certaines circonstances, dans le secteur privé. Ses qualifications sont précisées à l'image des nouvelles obligations du responsable de traitement et du sous-traitant[1843]. Toutefois, la désignation d'un délégué n'a pas pour effet d'entraîner un quelconque transfert de responsabilité civile ou pénale du responsable de traitement mais souligne la volonté d'un engagement fort du responsable de traitement afin d'assurer l'application de la loi. Ainsi le DPO assure la transparence sur les traitements et instaure une révolution culturelle reposant sur l'autorégulation (A). L'autre acteur de la mise en œuvre du droit à la protection des données personnelles est le responsable du traitement. Ses obligations sont fonctionnelles à l'exercice des droits de la personne concernée. Il s'agit d'une approche de corégulation où la gestion de la conformité n'est pas soumise passivement au contrôle de l'autorité mais implique l'activité de l'ensemble des parties (B).

A. Le délégué à la protection des données

217 Une mesure *d'accountability*. Suite aux transpositions de la directive 95/46 plusieurs États membres avaient créé la fonction du correspondant informatique et libertés. Toutefois sa désignation n'était pas obligatoire. La directive prévoyait dans son article 18 la possibilité pour le responsable du traitement de désigner un détaché à la protection des données à caractère personnel. Une telle désignation exonérait le responsable du traitement des notifications et des formalités administratives[1844]. Initialement conçu comme une simple mesure d'allègement des formalités préalables, le DPO, sous l'impulsion des autorités de contrôle et de la société civile, a vu son rôle grandir et est devenu l'un des éléments centraux de la refonte. L'institution du DPO (*Data protection officer*) ou DPD (délégué à la protection des données) par le règlement 679/16 est l'expression de l'exigence de sensibilisation du public vis-à-vis des règles sur la protection des données personnelles [1845] . Ainsi, les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le règlement. Dans la continuité de la directive de 1995, le règlement 967/16 reconnaît une place aux délégués à la protection des données personnelles et, du fait de leur désignation obligatoire,

---

1841 La désignation du DPO est également obligatoire selon l'art. 32 de la Directive (EU) 2016/680 pour les autorités chargées de l'enquête, la poursuite des crimes.

1842 Voy. Règl. (UE) 2016/679, art. 37, § 2 et 3.

1843 D'ailleurs un chapitre entier lui est consacré alors que dans la directive de 1995 il n'apparaissait qu'à côté des mesures de dispenses que les États membres avaient la faculté de prévoir.

1844 G. DESGENS-PASANOU, *Le correspondant Informatique et libertés*, Lexis Nexis, 2013, p. 2 et s.

1845 G.M. PELLOS, *Il Data Protection Officer. Il Responsabile dei dati personali dopo il D.Lgs. 10 agosto 2018, n°101*, Dike Giuridiche, 2018, p.30 et s.

ils sont destinés à jouer un rôle central. Ce caractère obligatoire concerne les organismes publics, toutefois la mutualisation est possible dès lors la structure organisationnelle de l'organisme le permet. Dans le secteur privé, la désignation est obligatoire dans certaines conditions. Le règlement 2016/679 se caractérise par la mise en place d'une approche dite d' «*accountability*», c'est-à-dire une responsabilisation des acteurs qui traitent des données personnelles via un autocontrôle des entreprises. Le règlement UE prévoit ainsi de passer d'un système de contrôle *ex ante* (le système des notifications et des autorisations) vers un contrôle *ex post* qui prévoit la tenue d'un registre des traitements et son suivi régulier. Le DPO est alors perçu comme un vecteur de sécurité juridique. La nouvelle disposition du règlement 679/2016 prévoit à l'article 37 trois cas dans lesquels la désignation du DPO est obligatoire. Tout d'abord, lorsque le traitement est effectué par une autorité ou un organisme public à l'exclusion de juridictions agissant dans le cadre de leurs compétences. Ensuite, lorsque les activités du responsable consistent en des traitements qui, du fait de leur nature et de leur portée exigent un suivi régulier. La désignation du DPO est obligatoire aussi lorsque les activités du responsable consistent en des traitements à grande échelle de données sensibles. Ce changement de paradigme permettra aux autorités de contrôle de concentrer davantage leurs efforts sur une mission de sensibilisation et d'accompagnement des responsables de traitement de données. Au-delà de ces trois cas, le règlement encourage la désignation du DPO dans le secteur privé et prévoit ses fonctions et le rend obligatoire lorsque « les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle[1846] des personnes concernées » ou lorsque les activités de base[1847] « consistent en un traitement à grande échelle» de données sensibles [1848] . Le DPO peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou travailler dans le cadre d'un contrat de service. Dans ce dernier cas il est essentiel d'éviter tout conflit d'intérêt et de rendre public les contacts du DPO afin de garantir une prise de contact directe et transparente. Concernant les fonctions du DPO, l'article 39 du règlement 679/2016 prévoit une mission d'avis et de conseil, une mission de contrôle et une mission de point de contact avec l'autorité de contrôle. Selon le règlement, le DPO doit exercer ses fonctions de manière indépendante, ce qui implique qu'il ne peut recevoir aucune instruction relative à l'exécution de ses missions. Toutefois, le responsable du traitement reste le seul responsable pour les prises de décisions. Si le responsable du traitement décide de ne pas suivre l'avis du DPO, ce dernier doit pouvoir manifester clairement sa prise de position sur la question. Le DPO doit être informé et consulté avant toute prise de décision sur le traitement des données, lorsque son avis n'est pas suivi le responsable doit le documenter. Ainsi le DPO doit être invité à participer aux réunions, il doit être informé de tout accident ou « *data breach »* relatifs aux traitements des données. Le DPO doit veiller à la légalité et à la transparence des traitements de données effectués par le responsable de traitement ou le sous-traitant qui l'a désigné. Il doit tenir à jour la liste des

1846 L'avis du G29 explique que le terme « large échelle » concerne l'étendue du traitement (par exemple un nombre relevant de la population), la durée du traitement et l'extension géographique du traitement.

1847 L'avis du G29 explique que le terme « activité de base » concerne l'activité qui permet au responsable du traitement d'atteindre son but.

1848 Voy. Règl. (UE) 2016/679, art. 37, § 1.

traitements de données mis en œuvre par le responsable, identifier les opérations de traitement des données à l'égard de leur nature et de leur finalité. Il doit veiller d'une manière indépendante et analyser la mise en conformité avec le règlement. Pour ce faire, il doit conseiller le responsable de traitement et lui adresser ses avis et recommandations, il doit être consulté en amont avant la mise en œuvre de tout nouveau traitement et il doit vérifier la bonne réalisation des études d'impact et le respect des obligations du responsable de traitement en matière de failles de sécurité. Le DPO doit être préalablement consulté pour le traitement à risque (lorsque l'analyse d'impact révèle que les traitements sont du fait de leur nature, de leur portée ou de leurs finalités susceptibles de présenter un degré élevé de risques particuliers). Il doit être associé à la réalisation des études d'impact et il peut recevoir les plaintes et réclamations des personnes concernées. De plus, le DPO est l'officier de liaison avec les autorités de protection des données et devra rendre compte au niveau le plus élevé de sa hiérarchie[1849]. Aussi, tient-il compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

B. Le responsable du traitement

L'autre acteur de la mise en œuvre du droit à la protection des données personnelles est le responsable du traitement. Le responsable du traitement est la personne physique ou morale, l'autorité publique, le service ou l'organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens de traitement. Ainsi, un moteur de recherche peut se considérer comme un responsable du traitement, c'est la conclusion de la Cour de justice dans l'affaire *Google Spain*[1850]. Dans cette affaire, la Cour de justice examine la question de la licéité d'un traitement selon que l'on se place du point de vue de l'éditeur d'un site web ou du moteur de recherche qui indexe les informations contenues sur le site. C'est en effet le moteur de recherche qui collecte, indexe, conserve les informations contenues sur un site web, les conserve sur ses serveurs et, le cas échéant, communique et met à disposition de ses utilisateurs sous forme de liste les résultats de leurs recherches. Il s'agit à chaque fois d'un traitement de données et la Cour de justice insiste sur le rôle décisif du moteur de recherche (dans le choix des finalités et des moyens du traitement) qui rend accessibles aux internautes des données qu'ils n'auraient pas trouvées autrement. De plus, la Cour de justice estime que le moteur de recherche en tant que responsable du traitement est tenu, lorsque la personne concernée lui en fait la demande, à la rectification, l'effacement ou le verrouillage des données en raison du caractère inexact ou incomplet ou pas/plus nécessaire des données. Ainsi, c'est au regard des droits d'effacement et d'opposition que la Cour de justice examine le rôle d'un moteur de

1849 Voy. Règl. (UE) 2016/ 679, art. 38, § 3.

1850 O. POLLICINO, « Un digital right to privacy preso (troppo) sul serio dai giudici di Lussemburgo. Il ruolo degli artt. 7 e 8 della Carta di Nizza nel reasoning di Google Spain », *Roma Tre Press*, 2016, p. 7-28.

recherche en tant que responsable du traitement[1851]. En effet, même un traitement licite de données peut devenir avec le temps illicite lorsque ces données ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées. Le responsable du traitement est tenu à un contrôle de proportionnalité des intérêts en jeu puisque la Cour de justice ne donne pas dans sa décision une réponse absolue sur la portée du droit à l'oubli et sur quel droit doit prévaloir[1852]. Il se peut que la nature de l'information en question et l'intérêt du public à disposer de cette information puisse renverser la balance. La Cour de justice a établi le rôle de responsable de traitement du moteur de recherche et son obligation de respecter les normes de protection des données. Ainsi le moteur de recherche ne peut pas prétendre à un statut d'hébergeur sans maîtrise du contenu. Le responsable du traitement devient alors un acteur à part entière du processus de régulation. Ainsi, dans le contexte du développement exponentiel des technologies de l'information et de l'Internet, le responsable du traitement joue un rôle d'exemplarité en matière de protection des données personnelles, au risque d'engager sa responsabilité juridique et de nuire à l'entreprise, aux organismes publics et aux droits de la personne concernée. De plus, le rôle du responsable du traitement a un impact sur les droits des personnes concernées par le traitement. Les obligations du responsable du traitement sont fonctionnelles à l'exercice des droits de la personne concernée. Ainsi le responsable a tout d'abord l'obligation d'information de la personne concernée et celle de sécurité des données traitées. Concernant l'obligation générale d'information de la personne dont les données font l'objet de traitement, le responsable doit transmettre son identité, les finalités du traitement, le caractère obligatoire ou facultatif des réponses, les conséquences éventuelles d'un défaut de réponse, les destinataires des données ainsi que l'existence du droit d'accès et de rectification. Cette obligation d'information doit être claire et lisible et se fait au plus tard lors de la première communication des données. Le règlement 679/16 renforce les obligations incombant au responsable car il a désormais une obligation de documentation, ou « *accountability* », consistant en la définition des procédures de nature à attester du respect de la législation. De même, il devra réaliser l'étude d'impact préalable à la mise en œuvre de certains traitements considérés comme comportant des risques pour les personnes concernées. L'ensemble de ces mesures est contrebalancé par une suppression quasi totale des formalités préalables auprès de l'autorité de contrôle (à l'exception des formalités liées à certains traitements sensibles et aux transferts de données hors Union européenne). Concernant la responsabilité du responsable du traitement[1853], celui-ci met en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Lorsque deux responsables du traitement, ou plus, déterminent conjointement les finalités et les moyens du traitement, ils sont les responsables conjoints du traitement. Lorsque le responsable est établi dans un pays tiers, il

1851 G. RESTA, V. ZENO ZENCOVICH (a cura di), *Il diritto all'oblio su Internet dopo la sentenza Google Spain*, Roma, 2015, passim F. Pizzetti (; a cura di), *Il caso del diritto all'oblio*, Torino, 2013, passim ; G.B. FERRI, « Diritto all'informazione e diritto all'oblio », in *Riv. dir. civ.*, 1990, I, p. 801 ss. ; M.R. MORELLI, « Oblio (diritto all') », in *Enc. dir., Agg.* VI, Milano, 2002, p. 848 ss.; MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009, Passim, in part. p. 81 ss., p. 199 ss., p. 151 ss.

1852 Sur la nécessité de préciser la portée de cet arrêt, v. le rapport du Conseil d'État, « Le numérique et les droits fondamentaux », Coll. Les rapports du Conseil d'État, La Documentation française, 2014, p. 277.

1853 A. MANTELERO, « Responsabilita`e rischio nel Regolamento », UE 2016/679, *In Le Nuove leggi civili commentate* 1/2017, Cedam, p. 152 et s.

doit élire un représentant établi dans un des États membres dans lesquels se trouvent les personnes physiques dont les données à caractère personnel font l'objet d'un traitement lié à l'offre de biens ou de services, ou dont le comportement fait l'objet d'un suivi. Concernant la sécurité du traitement, le responsable du traitement et le sous-traitant sont tenus de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque. Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. Une seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent les mêmes risques élevés. En cas de violation de données à caractère personnel, le responsable du traitement en notifie la violation à l'autorité de contrôle compétente et à la personne concernée dans le meilleur délai. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données est effectuée et indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer ce risque. Selon l'article 42 du règlement, les autorités de contrôle, le comité et la Commission encouragent la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Toutefois, la certification ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du règlement et est sans préjudice des missions et des pouvoirs des autorités de contrôle[1854]. Afin de pouvoir exercer ses droits, la personne concernée doit pouvoir contacter le responsable du traitement. Cela ne pose pas de problème lorsque le responsable du traitement est établi dans le même État membre que la personne concernée ou dans un autre État membre. Toutefois, le règlement 679 est intervenu en élargissant le champ d'application de la législation. Ainsi, le règlement s'applique au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union. De plus, le règlement s'applique au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes; ou au suivi du comportement de ces personnes, dans la mesure où il s'agit

---

1854 La certification est délivrée par les organismes de certification visés à l'article 43 du règlement ou par l'autorité de contrôle compétente sur la base des critères approuvés par cette autorité de contrôle compétente en application ou par le comité européen. Lorsque les critères sont approuvés par le comité, cela peut donner lieu à une certification commune, le label européen de protection des données. Les organismes de certification doivent disposer d'un niveau d'expertise approprié en matière de protection des données agrée par l'autorité de contrôle ou par l'organisme national d'accréditation désigné conformément au règlement (CE) no 765/2008 du Parlement européen et du Conseil, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle.

d'un comportement qui a lieu au sein de l'Union. Ainsi la Cour de justice a rattaché l'opération du moteur de recherche *Google Spain* à celle de son établissement Google Inc. afin d'appliquer la législation de l'Union européenne en matière de protection des données personnelles. En effet, dans cette affaire, la société Google a recours à sa filiale espagnole pour la promotion des ventes d'espaces publicitaires générés sur le site web google.com et elle a désigné cette filiale auprès de l'autorité de contrôle espagnole comme responsable du traitement des fichiers enregistrés par Google Inc. Selon la Cour de Justice, *Google Spain* se livre à l'exercice effectif et réel d'une activité au moyen d'un établissement stable en Espagne. Ainsi, il n'est pas nécessaire que le traitement de données soit effectué par l'établissement concerné lui-même mais il suffit qu'il le soit dans le cadre des activités de celui-ci[1855]. En l'espèce, le traitement est fait pour les finalités du moteur de recherche exploité par Google Inc., entreprise ayant son siège dans un État tiers mais disposant d'une filiale et donc d'un établissement dans un État membre. Le traitement est donc effectué dans le cadre de cet établissement si celui-ci est destiné à assurer dans cet État membre la promotion et la vente des espaces publicitaires proposés par le moteur de recherche. La Cour a adopté une conception étendue de la notion de responsable de traitement tout d'abord en retenant une appréciation généreuse de la portée territoriale de la directive 95/46 et le RGPD consacre ce raisonnement et fait apparaître clairement les deux critères essentiels, à savoir la capacité juridique et organisationnelle d'une part et l'autonomie à définir les finalités et les moyens du traitement d'autre part[1856]. Ainsi comme l'indique le groupe de travail du G29, « *la notion de responsable du traitement est une notion fonctionnelle, visant à attribuer les responsabilités aux personnes qui exercent une influence de fait, et elle s'appuie donc sur une analyse factuelle plutôt que formelle »*[1857]. Toutefois, la mise en œuvre de ce crytère n'est pas evidente : Le responsable peut determiner les finalités et les moyens du traitement conjointement avec d'autres. Ainsi selon une première situation, les responsables de traitement déterminent ensemble les finalités et les moyens du traitement et sont alors considérés conjointement responsables de sorte que la victime peut demander réparation de la totalité à l'un d'entre eux à charge, pour ce dernier, de se tourner vers son cocontractant. Dans la seconde hypothèse, ils déterminent indépendamment les finalités et les moyens du traitement ; alors, l'étendue de leurs obligations sera proportionnelle à leur action quand bien même le traitement porte sur les mêmes données. Des affaires récentes, ont été soumises à la Cour de justice par la voie de questions préjudicielles, illustrant la complexité de la réalité des traitements conjoints[1858]. L'avocat général rappelle dans son analyse qu'« il n'est

1855 La notion d'établissement est définie dans le RGDP comme l'exercice effectif et réel d'une activité au moyen d'un dispositif stable, quelle que soit la forme juridique d'un tel dispositif. Il n'est donc pas nécessaire notamment que l'établissement soit doté de la personnalité juridique : règlement (UE) n° 2016/679, cons. 22.

1856 M.C FONTAINE « La plasticité de la notion de responsable de traitement », *Revue des affaires européenne, Bruylant* 2018, p. 35 et s.

1857 Voy. Avis 1/2010, p. 10.

1858 Demande de décision préjudicielle présentée par l'Oberlandes- gericht Düsseldorf (Allemagne) le 26 janvier 2017 – Fashion ID GmbH & Co. KG / Verbraucherzentrale NRW eV, JO, n° R 112, 10 avril 2017 (2017/C 112/32) et CJUE, concl. avocat général Yves Bot, 24 octobre 2017, aff. C-210/16, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein / Wirtschaftsakademie Schleswig Holstein GmbH, en présence de Facebook Ireland Ltd, Vertreter des Bundesinteresses beim Bundesverwaltungsgericht, points 46 à 57, Comm. com. électr.,2018 comm. 5.

pas nécessaire pour être qualifié de responsable de traitement au sens de la directive 95/46 de disposer d'un pouvoir de contrôle sur tous les aspects du traitement. Affirmer le contraire conduirait à limiter sérieusement la protection des données personnelles compte tenu de la complexité actuelle des traitements faisant intervenir plusieurs acteurs aux rôles complémentaires. Enfin, dans un souci de garantir la protection des personnes physiques, il importe de ne pas ouvrir une brèche qui consisterait à échapper aux obligations de responsable de traitement dès lors que l'on a recours aux services d'un tiers. Une interpréta- tion contraire créerait un risque de contournement des règles relatives à la pro- tection des données à caractère personnel » [1859] . Ainsi il appuye son analyse sur une autre affaire (CJUE, Fan page aff. C-210/16)[1860] conduisant à la même conclusion : l'administrateur d'une page ou l'exploitant d'un site web qui intègre le code d'un fournisseur de services de webtracking à son site web contribue à la transmission de données personnelles, l'installation de cookies et la collecte de données au profit du fournisseur de services de webtracking. Le gestionnaire d'un site web qui utilise ces modules sociaux est ainsi également un responsable de traitement au sens de la directive 95/46 (et du RGPD). D'ailleurs la CJUE par son arrêt rendu le 5 juin 2018 reprend les conclusions de l'avocat général. Ainsi la banalisation et généralisation des traitements des données sont à l'origine de l'extension du nombre de personnes ayant la qualité de responsable de traitement[1861]. Les nouvelles règles ainsi que le rôle plus accru du responsable du traitement et les nouvelles missions du DPO sont destinées à renforcer le droit fondamental à la protection des données personnelles.

1859 Voir conclusion de l'Avocat Général Y. Bott, Aff. C-210/16, concl., point 65.

1860 Dans cette dernière affaire dite Fashion ID, le gestionnaire d'un site web, la société Fashion ID a inséré dans son site ce que l'on appelle un « module social » (en l'occurrence le bouton « j'aime » de Facebook) d'un fournisseur externe (c'est-à-dire Facebook), qui entraîne une transmission de données à caractère per- sonnel de l'ordinateur de l'utilisateur du site web au fournisseur externe. Une association de protection des consommateurs reproche à la société Fashion ID d'avoir ainsi permis à Facebook l'accès aux données à caractère personnel des utilisateurs de ce site, sans leur consentement et ce, en violation des obliga- tions d'informations. La question posée à la CJUE consiste à déterminer si la société Fashion ID est un responsable de traitement.

1861 M.C. FONTAINE « La plasticité de la notion de responsable de traitement », *Revue des affaires européenne, Bruylant* 2018, p. 35 et s.

CONCLUSION DU CHAPITRE I

Le droit fondamental à la protection des données personnelles présente la particularité d'avoir justifié l'intervention d'autres acteurs que le législateur et le juge. Il s'agit tant d'acteurs institutionnels que d'acteurs non institutionnels. Les acteurs institutionnels tels que les autorités de contrôle nationales exercent un pouvoir à la fois d'influence et de contrainte. Les autorités de contrôle nationales sont un élément essentiel du droit européen de la protection des données qui est consacré à l'article 8, paragraphe 3, de la charte. Afin de mener à bien leurs missions, elles doivent jouir d'une véritable indépendance vis-à-vis du pouvoir public. Ainsi, dans la mise en œuvre de leurs tâches, elles ont acquis un rôle essentiel dans le processus normatif. Ces autorités se sont vues attribuer une nouvelle tâche concernant la mise en œuvre du droit à l'oubli. Deux ans après l'arrêt *Google Spain*, la mise en œuvre du droit au déréférencement pose encore de nombreuses difficultés. Ainsi le G29, dont la position est relayée par les autorités nationales a publié des directives sur la manière de mettre en œuvre l'arrêt *Google Spain*. De plus, la composante transfrontière internationale du droit à la protection des données personnelles pose un défi en matière de coopération entre autorités de contrôle tant européennes que mondiales. En effet, l'existence d'une autorité de protection des données personnelles « ne doit pas justifier une prise de décision isolée, sur des questions ayant vocation à intéresser la société toute entière. Il est indispensable de politiser et de démocratiser les choix techniques qui engagent des choix de société. Ceci est un gage d'efficacité : seuls un large débat social et une représentation suffisamment large d'individus peuvent mettre en cause des choix qui peuvent parfois s'imposer d'eux-mêmes, compte tenu des progrès techniques ou des avancées économiques escomptés »[1862]. Ainsi le RGPD établit un mécanisme de guichet unique pour les cas de traitement transfrontalier. Certaines entreprises mènent des activités de traitement transfrontalières en raison du traitement de données à caractère personnel dans le cadre des activités d'établissements situés dans plusieurs États membres ou dans le cadre d'un établissement unique dans l'Union, mais affectent sensiblement les personnes concernées dans plusieurs États membres. Dans le cadre de ce mécanisme, ces entreprises n'auront à traiter qu'avec une seule autorité nationale de surveillance de la protection des données. Un mécanisme de coopération et de cohérence permettra une approche coordonnée entre toutes les autorités de surveillance impliquées dans l'affaire. L'autorité compétente - de l'établissement principal ou de l'établissement unique - consultera et soumettra son projet de décision aux autres autorités de surveillance concernées. Cependant, la mise en œuvre des règles concernant la protection des données appartient aussi à des acteurs non institutionnels, comme la société civile. Cependant, même s'il y a eu une réflexion et une prise de conscience de l'importance de son rôle, la place qu'occupe la société civile dans le processus normatif et dans la prise de décisions est encore très faible. Le travail des autorités nationales de protection des données est alors indispensable pour parvenir à une compréhension commune des principes des droits sur

1862 G. DESGENS -PASANAU, *Informatique et Libertés : une équation à plusieurs inconnues*, préc., spéc. p. 88.

la protection des données. Un changement d'attitude serait alors nécessaire pour augmenter la publicité donnée à leurs activités et sensibiliser les parties prenantes aux droits liés à la protection des données. C'est sur la base de cette réflexion que le règlement 679/16 a établi dans certaines circonstances l'obligation de désigner un délégué à la protection des données personnelles et a renforcé les obligations qui incombent au responsable du traitement. Il s'agit de deux acteurs qui jouent désormais un rôle accru pour la mise en œuvre efficace du droit à la protection des données personnelles. Ces nouvelles règles apparaissent plus efficaces sur le plan de la protection des personnes et plus contraignantes pour les professionnels. Il est possible de remarquer le passage d'une logique formelle de déclaration préalable à l'autorité de contrôle à une logique substantielle et d'autorégulation au gain du droit de la personne concernée.

CHAPITRE II. LA PROTECTION NON-JURIDICTIONNELLE AU SEIN DE L'UNION EUROPÉENNE

218 Des gardiens de l'architecture des droits fondamentaux. Dans l'architecture du droit de l'Union européenne il est possible de distinguer deux acteurs dont l'objectif est de renforcer le droit à la protection des données personnelles : le Contrôleur européen de la protection des données et le Groupe de protection des personnes à l'égard du traitement des données à caractère personnel (ci-après G29). Ainsi, à l'échelle de l'Union, les autorités nationales de contrôle coopèrent et collaborent dans le cadre du G29. Toutefois, avec l'abrogation de la directive 95/46, le G29 a disparu au profit d'un organe institué par le RGPD: le Comité européen de la protection des données[1863]. Il s'agit d'acteurs qui participent à la mise en œuvre du cadre juridique en matière de protection des données personnelles. Ces acteurs ont été créés à la fois par des textes de droit originaire et par des textes de droit dérivé[1864]. De plus, le législateur a également voulu appliquer les principes de protection des données personnelles aux institutions communautaires, car dans le cadre de leurs missions, les institutions et organes de l'Union sont amenés à traiter des données à caractère personnel. Ainsi, le règlement 45/2001 a institué le Contrôleur européen à la protection des données personnelles (CEPD)[1865], une autorité de contrôle indépendante dont l'objectif est de protéger les données à caractère personnel et de promouvoir les bonnes pratiques dans les institutions et organes de l'Union. Il doit veiller à ce que les institutions et organes de l'Union respectent le droit des citoyens à la protection de leur vie privée lors du traitement de données à caractère personnel. Il s'agit d'un gardien européen de la protection des données qui renforce l'architecture du droit fondamental à la protection des données personnelles. À l'instar des autorités de contrôle nationales il a une mission de conseil mais aussi de contrôle (section I). Ce système de protection est complété par le groupe de travail établi en vertu de l'article 29, paragraphe 1, section 1, de la directive 95/46 relative à la protection des données (Groupe de l'article 29). Ce groupe a un caractère consultatif et indépendant. Toutefois, il s'agit d'un droit souple dépourvu de force contraignante. Ainsi, le règlement 679/2016 a substitué au G29 le Comité européen de la protection des données, lequel aura des pouvoirs plus étendus en matière de protection des données et pourra élaborer des normes contraignantes (section II).

1863 https://edpb.europa.eu/legal-framework_fr

1864 Voy. l'art. 16 TFUE (ex art. 286 TCE) : 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2. Le Parlement européen et le Conseil, statuant conformément à la procédure législative ordinaire, fixent les règles relatives à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union, ainsi que par les États membres dans l'exercice d'activités qui relèvent du champ d'application du droit de l'Union, et à la libre circulation de ces données. Le respect de ces règles est soumis au contrôle d'autorités indépendantes. « Les règles adoptées sur la base du présent article sont sans préjudice des règles spécifiques prévues à l'article 39 du traité sur l'Union européenne. Voy. l'art. 8 de la Charte : 1. Toute personne a droit à la protection des données à caractère personnel la concernant. 2.Ces données doivent être traitées loyalement, à des fins déterminées et sur la base du consentement de la personne concernée ou en vertu d'un autre fondement légitime prévu par la loi. Toute personne a le droit d'accéder aux données collectées la concernant et d'en obtenir la rectification. 3. Le respect de ces règles est soumis au contrôle d'une autorité indépendante. Ainsi sur cette base la Communauté a adopté le règlement 45/2001 du 18 décembre 2000 qui constitue la norme fondamentale dans ce domaine. D'ailleurs la directive 95/46 avait déjà institutionnalisé le G29.

1865 https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_fr

Section I. Le Contrôleur européen à la protection des données personnelles

219 Le respect des données à caractère personnel traitées par les institutions et les organes de l'Union européenne. Un système à part entière de protection des données à caractère personnel impose non seulement de conférer des droits aux personnes concernées et des obligations à celles qui traitent des données à caractère personnel, mais aussi de prévoir des sanctions appropriées pour les contrevenants ainsi qu'une autorité de contrôle indépendante. Afin d'assurer la protection des données à caractère personnel traitées par les institutions et les organes de l'Union européenne le règlement 45/2001/CE instituant le Contrôleur européen à la protection des données personnelles (CEPD) [1866] a été adopté. Le champ d'application organique[1867] du règlement 45/2001 est le plus large possible. Celui-ci s'applique au traitement de données à caractère personnel par toutes les institutions et tous les organes communautaires, dans la mesure où ce traitement est mis en œuvre pour l'exercice d'activités qui relèvent en tout ou en partie du champ d'application du droit communautaire[1868]. Cependant, les institutions et organes créés dans le cadre de l'ancien troisième pilier (par exemple Europol, Eurojust) ne sont pas couverts par le règlement 45/2001. En revanche, d'autres textes de droit dérivé[1869] ont étendu la compétence du CEPD aux systèmes d'informations gérés par ces institutions. Ainsi, le CEPD est comparable aux autorités du même type mises en place par les États membres conformément à la directive 95/46/CE relative à la protection des données[1870]. Les citoyens pourront ainsi directement porter plainte auprès de ladite autorité s'ils estiment que les droits protégés par le règlement ne sont pas respectés. Concernant le champ d'application matériel, les dispositions du règlement 45/2001 reprennent la directive 95/46. Notamment, les données traitées par les institutions et organes de l'Union doivent être : traitées loyalement et licitement ; collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ; adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ; exactes et, si nécessaire, mises à jour ; conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont collectées ou pour lesquelles

---

1866 Voy. articles 41 à 48.

1867 F. MAIANI, *Le cadre réglementaire des traitements de données personnelles effectués au sein de l'Un*ion, *RTD eur*. 2002, p.283 et s., spéc. p. 296.

1868 Toutes les institutions listées à l'art. 13 TFUE et tous les organes créés par les traités (par exemple la Banque européenne d'investissement) et par des actes de droit dérivé pris sur la base des traités (par exemple l'Agence des droits fondamentaux) lui sont soumises.

1869 Voy. par exemple la décision 2009/371JAI du Conseil du 6 avril 2009 réalisant la « communautarisation d'Europol » qui prévoit l'intervention du CEPD ; s'agissant du système Schengen le CEPD a repris les compétences exercées par l'Autorité de contrôle commune Schengen ; enfin le système sur les visas institué avec le règlement 767/2008 prévoit aussi l'intervention du CEPD.

1870 http://europa.eu/legislation_summaries/information_society/data_protection/l14012_fr.htm.

elles sont traitées ultérieurement. De plus, le règlement fixe la condition de traitement pour les données sensibles [1871] . Tout comme dans la directive 95/46, les éventuelles dérogations à l'interdiction du traitement de ces données doivent se fonder sur le consentement explicite de la personne concernée ou sur la nécessité de respecter des obligations issues du droit du travail, sur la prise en compte de raisons médicales et sur la sauvegarde des intérêts vitaux des personnes concernées. Toutefois, d'autres dérogations sont possibles « sous réserve de garanties appropriées et pour un motif d'intérêt public important » (par exemple si l'on pense aux fichiers d'infractions)[1872]. Concernant le droit des personnes, les droits consacrés par le règlement 45/2001 sont similaires à ceux de la directive : il existe un droit à l'information, un droit d'accès et de rectification, un droit d'opposition. Enfin, comme dans la directive 95/46, il est prévu tant un recours juridictionnel[1873] que la saisine du CEPD et les recours contre les décisions du CEPD[1874] . Ainsi, le champ d'application matériel est similaire à celui de la directive 95/46. Et les difficultés d'interprétation du règlement sont similaires à celles de la directive 95/46. Toutefois le législateur a décidé d'exclure le règlement 45/2001 des propositions de révision de la directive 95/46[1875]. Le règlement 45/2001 calque les droits prévus par la directive 95/46[1876], et les décisions du CEPD peuvent être contestées devant la Cour de justice. Ainsi plusieurs décisions du CEPD ont été contestées devant la Cour, mais les recours ont été rejetés ou retirés[1877]. Ni agence, ni institution, à travers l'étude de la composition du CEPD et de son fonctionnement (§1), il est possible de présenter son action et les enjeux auxquels il est confronté (§2).

§1. Une autorité de contrôle indépendante de plus en plus influente

1871 La jurisprudence a précisé la notion de données sensibles. Ainsi dans l'affaire Fiorella Vinci, le Tribunal de la fonction publique a considéré que la collecte de données médicales par l'employeur, en l'espèce, l'insertion par la direction des ressources humaines de la BCE dans le dossier de la requérante d'un courrier l'informant de la nomination d'un expert indépendant pour procéder à un examen médical et du certificat du médecin conseil de la BCE, lui permettant d'évaluer la capacité des personnes en congé de maladie à exercer leur fonction était nécessaire afin de respecter les obligations et droits spécifiques du responsable de traitement en matière de droit du travail. TFPU, 16 septembre 2009, aff. F-130/07, Fiorella Vinci.

1872 Voy. art. 10.4 et 10.5 du règlement 45/2001. Toutefois l'adoption de telles dérogations doit être entourée par des garanties procédurales : elles ne peuvent être adoptées que par un traité ou acte de droit dérivé ou sur décision du Contrôleur européen.

1873 Voy. par exemple concernant les conditions d'une action cherchant à mettre en cause la responsabilité non contractuelle de la Commission au sujet de fuites dans la presse : TPICE, 11 mai 2010, aff. F-30/08, Fotios Nanopulos c. Commission européenne.

1874 Voy. art. 32 et 33 du règlement.

1875 Voy. les observations critiques du CEPD sur l'application du règlement général sur la protection des données proposé aux Institutions européennes le 9 décembre 2013 (en ligne sur son site).

1876 Ainsi le CEPD peut ordonner le droit d'accès, de rectification, de blocage et de suppression de données à caractère personnel figurant dans les fichiers tenus par les institutions et les organes communautaires.

1877 Voy. par exemple, l'affaire T-164/09 et l'affaire T-237/16, ayant pour objet la demande d'annulation de la décision du Contrôleur européen de la protection des données, du 18 mars 2016, rejetant la plainte relative à la divulgation des données à caractère personnel concernant la partie requérante, dans les conclusions préliminaires d'un rapport établi par le Médiateur européen.

220 Le champ d'intervention du CEPD. Le Contrôleur européen de la protection des données (CEPD) est une autorité de contrôle indépendante de l'Union européenne chargée, en vertu de l'article 41, paragraphe 2, du règlement (CE) no 45/2001 du Parlement européen et du Conseil[1878], « de veiller à ce que les libertés et droits fondamentaux des personnes physiques, notamment leur vie privée, soient respectés par les institutions et organes communautaires », et « […] de conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel ». Une décision de la Commission a complété en 2002[1879] le cadre du règlement 45/2001. L'autorité de contrôle doit en particulier agir en toute indépendance, ce qui implique l'indépendance du pouvoir de décision vis-à-vis de toute influence extérieure directe ou indirecte. Il en découle que dans sa mission de conseil et de contrôle, le CEPD est indépendant. L'obligation d'indépendance des autorités de contrôle est prévue dans la législation, à savoir à l'article 16, paragraphe 2, du traité sur le fonctionnement de l'Union européenne (TFUE) et à l'article 8, paragraphe 3, de la Charte des droits fondamentaux de l'Union. La Cour de justice de l'Union européenne a souligné à de nombreuses reprises que le contrôle indépendant exercé par une autorité est un élément essentiel du droit à la protection des données et a fixé les critères de cette indépendance. Ainsi, le CEPD dans sa mission de protection des données à caractère personnel est chargé de contrôler les traitements des données personnelles effectués par l'administration de l'Union, de donner des conseils sur les politiques et les textes législatifs et de coopérer avec les autorités nationales afin de garantir un cadre juridique cohérent. Le rôle de conseiller indépendant que joue le CEPD auprès des institutions de l'Union couvre tous les aspects du traitement de données à caractère personnel, notamment les initiatives visant à renforcer la sécurité dans l'UE et les nouveaux outils d'échange de données utilisés par les services répressifs. En effet, le CEPD a publié de nombreux avis sur des initiatives visant à étendre le partage d'informations à des fins répressives au sein de l'UE, notamment sur le système d'entrée/sortie et les données PNR de l'UE, mais également au-delà des frontières de l'Europe, comme pour l'« *Umbrella Agreement* » (l'« accord-cadre ») avec les États-Unis et les accords PNR avec des pays tiers. Sa composition permet une indépendance vis-à-vis des institutions de l'Union européenne (A) lesquelles doivent respecter les dispositions du règlement 45/2001 dans le traitement des données à caractère personnel (B).

A. Composition et fonctionnement

1878 Règlement (CE) nº 45/2001 du Parlement européen et du Conseil du 18 décembre 2000 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions et organes communautaires et à la libre circulation de ces données, JO L 8 du 12.1.2001, p. 1.

1879 Voy. Décision n° 1247/2002/CE du 1 juillet 2002 relative au statut et aux conditions générales d'exercice des fonctions de CEPD.

221 Un rôle progressivement plus accru. Concernant la composition du CEPD, le Parlement européen et le Conseil nomment, d'un commun accord, sur une liste établie par la Commission, à la suite d'un appel public à candidatures, le contrôleur européen de la protection des données pour une durée de cinq ans. Un contrôleur adjoint est nommé selon la même procédure et pour la même durée. Il assiste le contrôleur dans l'ensemble de ses fonctions et le supplée en cas d'absence ou d'empêchement. Le contrôleur européen de la protection des données est choisi parmi les personnes offrant toutes garanties d'indépendance et qui possèdent une expérience et une compétence notoires pour l'accomplissement des fonctions de contrôleur européen de la protection des données, par exemple parce qu'ils appartiennent ou ont appartenu aux autorités de contrôle visées à l'article 28 de la directive 95/46/CE. Le Contrôleur européen et le contrôleur adjoint sont assistés par un bureau (secrétariat) composé de juristes expérimentés, d'informaticiens et d'administrateurs. Les fonctionnaires et les autres agents du secrétariat sont nommés par le contrôleur européen de la protection des données, qui est leur supérieur hiérarchique et dont ils relèvent exclusivement. Leur nombre est arrêté chaque année dans le cadre de la procédure budgétaire. Les fonctionnaires et les autres agents du secrétariat du contrôleur européen de la protection des données sont soumis aux règlements et réglementations applicables aux fonctionnaires et autres agents des Communautés européennes. Le CEPD a élaboré son règlement intérieur établissant les règles de fonctionnement de l'institution et encadre ses pouvoirs et ses missions [1880] . Pour garantir son indépendance, l'autorité budgétaire veille à ce que le contrôleur européen de la protection des données dispose des ressources humaines et financières nécessaires à l'exécution de sa mission. Ainsi le budget du contrôleur européen de la protection des données figure sur une ligne spécifique de la section VIII du budget général de l'Union européenne. Le Contrôleur européen de la protection des données exerce ses fonctions en toute indépendance. Dans l'accomplissement de sa mission, il ne sollicite ni n'accepte d'instructions de quiconque. Il s'abstient de tout acte incompatible avec le caractère de ses fonctions et, pendant la durée de celles-ci, ne peut exercer aucune autre activité professionnelle, rémunérée ou non. Dans le cadre de ses missions, le CEPD publie chaque année un rapport annuel public et destiné aux institutions européennes afin de garantir une bonne gouvernance de la protection des données personnelles[1881]. On notera qu'à l'origine le CEPD n'avait qu'un rôle mineur et conseillait seulement les institutions et organes de l'UE. Cependant, du fait de son rôle proactif, le CEPD s'est imposé sur des dossiers sensibles en participant au recours contre l'accord PNR conclu entre l'UE et les États-Unis et surtout en prenant position dans l'élaboration des bases de données en matière de sécurité dans l'ELSJ. Le CEPD représente désormais la seule autorité compétente pour contrôler Europol et Eurodac. De plus, les textes régissant les règles du SISII et VIS reconnaissent son rôle. Il est ainsi devenu une autorité incontournable des systèmes de base de données biométriques et, grâce à son volontarisme, les règles de protection tendent à s'unifier. Par ailleurs, la réforme relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel

1880 Décision du Contrôleur européen de la protection des données du 17 décembre 2012 concernant l'adoption du règlement intérieur (2013/504/UE).

1881 Le rapport du 2016 est disponible à l'adresse : https://edps.europa.eu/sites/edp/files/publication/17-04-27_annual_report_2016_executive_summary_fr.pdf

et à la libre circulation de ces données à élargi les compétences du CEPD. Sa mission s'inscrit désormais dans l'application cohérente du droit à la protection des données en Europe et donc va au-delà de ses attributions limitées aux institutions et organes de l'UE. Ainsi grâce à la création du Comité européen de protection des données, en substitution du G29, composé des directeurs des autorités de contrôle des États membres et du Contrôleur européen à la protection des données par le règlement 679/16, le rôle du CEDP continuera à croître. En effet, il sera chargé du secrétariat du Comité européen de protection des données (Comité) et en assumera soit la présidence, soit la vice-présidence. Son rôle devient celui d'une Agence européenne pour la protection des données sauf dans les domaines de l'ex-troisième pilier puisque la directive 680/16 ne prévoit rien. Il semble ainsi que grâce à l'accroissement de ses compétences et de son champ d'action, le CEPD sera amené à jouer un rôle important dans la mise en œuvre des règles de protection des données personnelles en Europe. Toutefois, si les institutions et organes de l'UE doivent traiter les données personnelles conformément au règlement 45/2001 et que le Contrôleur est chargé de veiller à sa bonne application, les institutions doivent aussi pondérer le droit à la protection des données personnelles avec d'autres droits, notamment avec le droit d'accès aux documents détenus par l'Union. Ainsi, le règlement 1049/2001[1882] relatif aux principes d'ouverture et de transparence, dont l'objectif est d'accroître leur participation des citoyens au processus décisionnel, de la forme la plus ouverte possible, confère la plus large portée possible au droit d'accès du public aux documents.

B. La justification de son existence dans la mise en œuvre du règlement 45/2001 par les institutions

222 Le CEPD devant la Cour de justice. L'une des missions du CEPD consiste à intervenir dans les affaires traitées devant la Cour de justice de l'Union européenne (CJUE), le Tribunal de l'Union européenne et le Tribunal de la fonction publique. Ainsi il peut porter une affaire devant la Cour. Toutefois, à ce jour, le CEPD n'a jamais saisi la Cour de justice[1883]. Dans ses ordonnances du 17 mars 2005 relatives aux affaires concernant les données des dossiers passagers (données PNR), la CJUE a décidé que le droit d'intervention du CEPD s'étendait à toutes les questions concernant le traitement des données à caractère personnel. Cela signifie concrètement que le droit du CEPD à intervenir dans des affaires portées devant la Cour ne se limite pas aux dossiers dans lesquels des institutions ou des organes de l'UE ont traité des données à caractère personnel mais s'étend à toutes les questions touchant à la protection des données à caractère personnel, que ce soit au niveau de l'Union européenne ou des États membres[1884]. Concernant son droit d'intervention dans les affaires portées devant la CJ, le

1882 Règlement (CE) no1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission.

1883 Aux termes de l'article 47, paragraphe 1, du règlement n° 45/2001: « Le contrôleur européen de la protection des données peut: saisir la Cour de justice des Communautés européennes dans les conditions prévues par le traité et intervenir dans les affaires portées devant la Cour de justice des Communautés européennes.»

1884 Voy. point 18 de l'ordonnance. En effet, conformément à l'article 41, paragraphe 2, second alinéa, du règlement n° 45/2001, le contrôleur est chargé non seulement de surveiller et d'assurer l'application des dispositions de ce règlement et de

terme « affaires » a été interprété en ce sens qu'il exclut les renvois préjudiciels au titre du traité sur le fonctionnement de l'Union européenne (article 267 du TFUE) ainsi que les demandes d'avis à la CJ (article 218, paragraphe 11, du TFUE). Pour combler cette lacune, la Cour a, à plusieurs occasions, invité le CEPD à répondre à des questions ou à fournir des renseignements sur la base de l'article 24 de son statut. Le Contrôleur européen de la protection des données veille à ce que les institutions et organes de l'Union respectent leurs obligations en matière de protection des données, telles qu'elles sont fixées dans le règlement (CE) nº 45/2001 sur la protection des données. Ainsi le règlement 45/2001 a été adopté sur le fondement de l'article 286 CE, cet acte normatif constitue le principal élément de protection des données à caractère personnel lorsqu'elles reçoivent un traitement quelconque de la part des institutions communautaires. Il fait partie d'un ensemble de mesures législatives qui constituent l'acquis communautaire en matière de protection des données à caractère personnel. Cependant, le droit à la protection des données peut rencontrer une limite dans l'exigence des institutions de communiquer et de publier certaines informations dans le respect du principe de transparence. La transparence et la protection des données sont deux éléments essentiels de la vie démocratique dans l'UE, qui contribuent tous deux à la bonne gouvernance. L'interaction entre ces droits – c'est-à-dire la manière de faciliter l'accès du public aux documents contenant des données à caractère personnel, peut toutefois être perçue comme difficile. Ainsi, la liberté d'expression, garantie par l'article 11 de la Charte des droits fondamentaux et par l'article 10 de la CEDH, protège non seulement le droit de communiquer mais aussi celui de recevoir des informations. Le droit d'accès garantit la transparence qui est un principe fondamental pour le bon fonctionnement d'une société démocratique [1885] . Ce droit peut s'opposer au droit à la protection des données si l'accès aux documents peut avoir comme conséquence de révéler les données à caractère personnel de tiers. Il s'agira alors de pondérer le droit à la protection des données personnelles qui figurent dans les documents demandés. Ainsi, le vingt-deuxième considérant du règlement 45/2001 indique que « les droits accordés à la personne concernée et l'exercice de ces droits ne doivent pas porter préjudice aux obligations imposées au responsable du traitement ». De plus, le droit d'accès aux documents des institutions communautaires a été inscrit, après le traité d'Amsterdam, dans l'article 255 CE : tout citoyen de l'Union et toute personne physique ou morale résidant ou ayant son siège dans un État membre a un droit d'accès aux documents du Parlement européen, du Conseil et de la Commission. De plus, l'article 42 de la Charte des droits fondamentaux déclare que « tout citoyen ou toute citoyenne de l'Union ou toute personne physique ou morale résidant ou ayant son siège statutaire dans un État membre a un droit d'accès aux documents du Parlement européen, du Conseil et de la Commission ». Enfin, la déclaration 17 annexée à l'acte final du traité de Maastricht a affirmé la transparence du processus de décision comme étant un renforcement du caractère

tout autre acte communautaire concernant la protection des libertés et droits fondamentaux des personnes physiques à l'égard des traitements de données à caractère personnel effectués par une institution ou un organe communautaire, mais également de conseiller les institutions et organes communautaires pour toutes les questions concernant le traitement des données à caractère personnel. Cette mission consultative ne vise pas uniquement les traitements de données à caractère personnel effectués par ces institutions ou organes. À ces fins, le contrôleur exerce les fonctions prévues à l'article 46 dudit règlement et les compétences qui lui sont conférées à l'article 47 du même règlement. Ainsi le contrôleur européen de la protection des données est admis à intervenir dans l'affaire C-317/04 à l'appui des conclusions du Parlement européen.

1885 L'article 42 de la Charte et l'article 15 §3 du TFUE ont étendu ce droit d'accès aux documents des institutions, organes et organismes de l'Union, quelle que soit leur forme. Conformément à l'article 52 §2 de la Charte, le droit d'accès s'exerce dans les conditions et limites définies à l'article 15 §3 du TFUE.

démocratique des institutions et de la confiance du public envers l'administration ; elle invitait la Commission à présenter des mesures destinées à améliorer l'accès du public aux informations détenues par les institutions communautaires. Concernant la mise en balance entre la protection des données personnelles traitées par les institutions européennes et le droit d'accès du public aux documents établi par le règlement n° 1049/20011886, la Cour de justice a fait prévaloir le droit à la protection des données personnelles[1887]. Selon l'article 4 du règlement n° 1049/2001, relatif aux exceptions au droit d'accès, les institutions refusent l'accès à un document dans le cas où la divulgation porterait atteinte à la protection de la vie privée et à l'intégrité de l'individu, notamment en conformité avec la législation communautaire relative à la protection des données à caractère personnel. Ainsi dans l'affaire *Commission c. The Bavarian Lager Co. Ltd*[1888] , la Cour de justice fait prévaloir le souci de protection du droit fondamental à la protection des données sur celui de transparence. S'agissant d'une demande d'accès aux documents de la Commission, du procès-verbal d'une réunion à laquelle avaient participé des représentants de la Commission, de l'administration britannique et de la confédération des brasseurs du marché commun, la Commission a transmis à la société requérante, *Bavarian Lager*, le document demandé, en indiquant toutefois qu'en application de l'article 4, paragraphe 1er, sous b), du règlement n° 1049/2001, cinq noms avaient été occultés. La Commission a en effet considéré que ces dispositions renvoyaient directement à l'article 8, sous b) du règlement n° 45/2001 et que les conditions prévues par celui-ci pour la transmission de données personnelles n'étaient pas réunies, deux personnes s'étant expressément opposées à la divulgation de leur identité et trois autres n'ayant pas pu être contactées pour donner leur accord. N'étant pas satisfaite de cette position, *Bavarian Lager* a saisi le Tribunal qui a annulé la décision de la Commission par un arrêt du 8 novembre 2007. Sur pourvoi de la Commission, la Cour de justice a cassé cet arrêt. Elle a jugé que l'article 4, paragraphe 1, sous b), du règlement n° 1049/2001 établissait un régime spécifique et renforcé de protection d'une personne dont les données à caractère personnel pourraient, le cas échéant, être communiquées au public. L'appréciation de l'atteinte à la vie privée et à l'intégrité de l'individu ne doit donc pas se limiter aux situations dans lesquelles il y aurait une violation au sens de l'article 8 de la CEDH, mais doit tenir compte de la législation de l'Union relative à la protection des données à caractère personnel, et notamment du règlement n° 45/2001, qui était donc intégralement applicable en l'espèce, comme le soutenait la Commission. C'est donc à bon droit que la Commission a vérifié si les participants à la réunion consentaient à la divulgation de leur nom et qu'en l'absence du consentement de cinq d'entre eux, elle a diffusé une version du procès-verbal de la réunion expurgée de leurs noms. De plus, selon la Cour, le requérant *Bavarian Lager*, n'avait fourni aucune justification expresse et légitime et aucun argument convaincant pour déterminer la nécessité du transfert de ces données personnelles. Afin de démontrer la nécessité du transfert de ces données personnelles, la Commission n'a pu ni mettre en balance les différents intérêts des parties en cause, ni vérifier s'il existait des raisons de penser que ce

1886 Règlement (CE) no1049/2001 du Parlement européen et du Conseil du 30 mai 2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission.

1887 CJUE, Gr. Ch, Bavaria Lager, aff. C-28/08, 29 juin 2010.

1888 CJUE, Gr. Ch, du 29 juin 2010, aff. C-28/08.

transfert pourrait porter atteinte aux intérê ts légitimes des personnes concernées. Dans ces conditions, c'est à bon droit qu'elle a rejeté la demande de *Bavarian Lager*. Selon la Cour de justice, une ingérence dans le droit à la protection des données personnelles à l'égard de l'accès à des documents requiert un motif spécifique et justifié. Le droit d'accès à des documents ne peut pas automatiquement écarter le droit à la protection des données. La Cour a fait prévaloir le souci de protection des droits fondamentaux sur celui de transparence. Il est intéressant de remarquer que pour ce faire, elle procède à l'interprétation des textes en cause à la seule lumière de l'article 8 de la Charte des droits fondamentaux, ce qui traduit « une volonté d'autonomisation »[1889] par rapport à l'article 8 de la CEDH. Dans l'affaire ***Shecke***[1890], la Cour de justice a annulé certaines règles communautaires prévoyant la publication annuelle a posteriori des noms des bénéficiaires du Fonds européen agricole de garantie (FEAGA) et du Fonds européen agricole pour le développement rural (Feader), ainsi que les montants perçus par chaque bénéficiaire au titre de chacun de ces fonds. Tout en reconnaissant que, dans une société démocratique, les contribuables ont le droit d'ê tre informés de l'utilisation des fonds publics, la Cour considère qu'il est nécessaire de trouver un juste équilibre entre le droit à la transparence, d'une part, et le droit à la protection des données personnelles des personnes physiques, d'autre part. Cependant, en raison de l'absence dans le droit de l'Union de critères permettant de réduire au minimum les interférences avec les données personnelles (par exemple, la définition des périodes pendant lesquelles ces personnes ont reçu une aide, la fréquence de l'aide ou sa nature et son montant), la Cour a considéré que le Conseil et la Commission dépassaient les limites de la proportionnalité. En fait, les dérogations aux droits dont jouissent les personnes physiques au titre des articles 7 et 8 de la Charte ne doivent être applicables qu'en cas de stricte nécessité. Ainsi, dans les deux décisions, la Cour de justice a décidé de faire prévaloir le droit à la protection des données sur le droit d'accès à des documents administratifs. D'autres décisions en ce sens ont été rendues et le CEPD a rédigé un document sur la question[1891]. Concernant la jurisprudence en matière du traitement par les institutions européennes, il s'agit surtout des juridictions de première instance[1892].

1889 Voy. le commentaire de F. Kauff-Gazin, europe n° 10, octobre 2010, comm 299.

1890 Affaires jointes C-92/09 et C-93/09.

1891 Voy. « Accès du public aux documents contenants des données à caractère personnel après l'arrêt Bavarian Lager », 24 mars 2011, disponible en ligne à l'adresse : https://edps.europa.eu/sites/edp/files/publication/11-03-24_bavarian_lager_en.pdf

1892 Voy. TPICE, 18 février 2004, aff ; T-320/02, Monika Esch-Leonhardt et a.c. BCE ; TPICE, 12 septembre 2007, aff. T-259/03, Kallopi Nikalaou c. Commission.

§2. Les missions du Contrôleur européen à la protection des données

223 Un pouvoir de conseil et de contrôle. Le CEPD doit conseiller les institutions et organes communautaires et les personnes concernées pour toutes les questions concernant le traitement des données à caractère personnel, afin de promouvoir l'élaboration responsable des politiques [1893] de l'UE en matière des données personnelles. Conformément à l'article 28, paragraphe 2, du règlement nº 45/2001, la Commission a l'obligation, lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, de consulter le CEPD. Le CEPD peut également donner des avis de sa propre initiative. Toutefois ces avis ne sont pas contraignants. Ce qui illustre les limites de cette autorité. L'autre mission du CEPD est celle de supervision. Lorsque les institutions de l'UE ne respectent pas les règles en matière de protection des données, le CEPD peut utiliser ses pouvoirs d'exécution en vertu du règlement. Il peut notamment : adresser un avertissement ou une admonestation à l'institution européenne qui traite les informations à caractère personnel de manière illégale ou déloyale ; ordonner à l'institution de satisfaire les demandes d'exercice des droits (par la personne concernée) ; interdire temporairement ou définitivement un traitement de données spécifique et porter une affaire devant la Cour de justice de l'Union européenne. Ainsi, le Contrôleur européen à la protection des données exerce des missions similaires de celles des autorités de contrôle nationales. Il a un pouvoir de conseil (A) et de contrôle (B).

A. Une mission de conseil

224 Des avis non contraignants. Le Contrôleur européen exerce une mission de conseil auprès des institutions et organes européens. Ses conseils peuvent concerner des questions particulières concernant la mise en œuvre du règlement 45/2001, des projets de mesures législatives et administratives que les institutions veulent adopter, ainsi que le conseil des juridictions. Le contrôleur est obligatoirement consulté et intervient dans sa mission de conseil[1894] à l'égard du Parlement européen, du Conseil et de la Commission sur les nouveaux textes législatifs et sur les autres propositions, initiatives et mesures administratives ayant un impact sur la protection des données personnelles[1895]. Ainsi l'article 28 du règlement 45/2001 dispose que les institutions et organes de l'UE doivent informer le CEPD lorsqu'ils élaborent

---

1893 Voy. L'avis no 4/2015 du Contrôleur européen de la protection des données « Vers une nouvelle éthique numérique : données, dignité et technologie » le 11 septembre 2015. Disponible à l'adresse : https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_summary_fr.pdf.

1894 Voy. Sur ce point : « Politique en matière de consultations dans le domaine de la supervision et de la mise en application », 23 novembre 2012; et le CEPD en tant que conseiller des institutions communautaires à l'égard des propositions de législation et documents connexes, 18 mars 2005, en ligne sur le site CEPD, rapport annuel 2013, p. 16

1895 Avec l'expression « mesures administratives » il faut entendre une décision juridiquement contraignante ou un autre acte qui n'est pas juridiquement contraignant de l'administration ayant une portée générale au sujet du traitement des données personnelles par les institutions ou organes de l'UE.

des mesures administratives relatives au traitement de données à caractère personnel. De plus, conformément à l'article 41 du règlement (CE) no 45/2001, le CEPD peut rendre des avis de sa propre initiative comme dans le cas de l'avis sur le rapport d'évaluation de la Commission concernant la directive sur la conservation des données[1896]. Dans son avis, le CEPD estimait que la disponibilité de certaines données de trafic et de localisation pouvait être cruciale pour les services répressifs dans la lutte contre le terrorisme et d'autres infractions graves. Toutefois, dans le même temps, le CEPD n'a eu de cesse d'exprimer des doutes concernant les raisons justifiant la conservation de données dans une telle mesure à la lumière des droits au respect de la vie privée et de la protection des données. Il a ainsi estimé que la conservation des données, telle qu'encadrée par la directive, allait au-delà de ce qui est nécessaire et appelait la Commission à envisager toutes les options, notamment la possibilité d'abroger purement et simplement la directive, de façon exclusive ou combinée avec une proposition de mesure alternative de l'UE plus ciblée. Le CEPD est intervenu plusieurs fois dans le cadre de la réforme de la protection des données. Il a accueilli favorablement le projet de règlement élaboré par la Commission[1897] , alors que le projet de directive relative à la protection des données dans l'espace de liberté, sécurité et de justice (ELSJ) a fait l'objet de critiques[1898], puisque selon le CEPD il n'atteint pas un niveau élevé de protection. Le CEPD a ainsi rendu des avis sur l'espace de liberté, de sécurité et de justice en s'inquiétant de l'ampleur de la collecte, du stockage et de l'échange transfrontalier de données à caractère personnel entre les États membres dans le domaine de la criminalité et du terrorisme et sur la tendance à donner aux services répressifs un accès de plus en plus important aux bases de données nationales ou européennes contenant des données qui n'ont rien à voir avec la commission d'une infraction et qui ont été collectées à d'autres fins. Il a ainsi rendu ses avis en matière de transfert de données[1899] au sujet de la directive 2006/24 sur la conservation des données [1900] tout comme de la directive PNR concernant le traitement des données des passagers aériens européens et les accords avec l'Australie[1901], les États-Unis[1902] et le Canada en vue du transfert de ces données. Il a d'ailleurs commenté la décision de la Commission sur la mise en place d'un système de surveillance du

---

1896 Voy. l'avis du Contrôleur européen de la protection des données sur le rapport d'évaluation de la Commission au Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24/CE) du 23 septembre 2011, disponible à l'adresse: https://edps.europa.eu/sites/edp/files/publication/11-05-30_evaluation_report_drd_fr.pdf et Voy. le rapport d'évaluation de la Commission COM (2011) 225 final du18 avril 2011.

1897 Voy. L'avis du CEPD sur le paquet de mesures pour une réforme de la protection des données, 7 mars 2012 et 15 mars 2013 en ligne sur le site https://europa.eu/european-union/about-eu/institutions-bodies/european-data-protection-supervisor_fr

1898 Voy. Le communiqué de presse du CEPD du 25 janvier 2012 en ligne sur le site.

1899 Voy. L'avis du 4 juin 2014 sur le futur de l'ELSJ.

1900 Voy. L'avis 2011/C et 322/01 du 15 juillet 2011 du CEPD sur la proposition de décision du conseil sur la conclusion d'un accord entre l'Union européenne et l'Australie sur le traitement et le transfert de données des dossiers passagers (PNR) par les transporteurs aériens au service australien des douanes et de la protection des frontières.

1901 Voy. L'avis 2011/C et 279/01 du 31 mai 2011 sur le rapport d'évaluation de la Commission et du Conseil et au Parlement européen concernant la directive sur la conservation des données (directive 2006/24).

1902 Voy. L'avis 2012/C 35/03 du 9 décembre 2011 du CEPD sur la proposition de décision du Conseil sur la conclusion d'un accord entre l'Union européenne et les États-Unis sur l'utilisation et le transfert de données des dossiers passagers (PNR) au ministère américain de la sécurité intérieure, 2 février 2012.

financement du terrorisme (SSFT)[1903], il a rendu des avis sur le fonctionnement d'Eurodac[1904], du SIS [1905], du VIS [1906], et sur le centre européen de lutte contre la cybercriminalité [1907]. Concernant son rôle de conseil des juridictions, le Contrôleur européen de la protection des données personnelles a le droit d'intervenir dans des affaires portées devant la Cour de justice de l'Union européenne mais aussi devant le Tribunal de la fonction publique[1908] et devant le Tribunal de première instance[1909]. Le CEPD peut intervenir de sa propre initiative en se fondant sur l'article 47, h, du règlement n° 45/2001 CE et lorsque les dossiers relèvent de ses compétences (art. 47 i) du règlement 45/2001. Toutefois, ce droit d'intervention a été délimité par la Cour de justice à l'occasion de la première demande d'intervention du CEPD dans l'affaire relative au transfert des données PNR [1910]. Après avoir constaté que ce droit d'intervention prévu par l'article 47 du règlement n° 45/2001 CE était bien conforme à l'article 286 du TCE, la Cour de justice l'a circonscrit à la mission conférée au CEPD. Cela étant, elle retient une appréciation très extensive de cette mission et, par conséquent, du droit d'intervention. Selon la Cour de justice, le droit d'intervention du CEPD se rattache à sa mission consultative et non à sa mission de contrôle[1911]. Dès lors, le droit d'intervention n'est pas limité aux questions relatives aux traitements de données personnelles mis en œuvre par les institutions et organes de l'Union européenne, mais s'étend plus largement à toute question relative aux traitements de données personnelles. Le CEPD peut donc également intervenir sur des questions relatives aux traitements de données personnelles mis en œuvre au sein des États membres et en l'espèce à ceux mis en œuvre par les compagnies aériennes. Cela étant, le droit

---

1903 Voy. Les observations du CEPD concernant la communication de la Commission au Parlement, au Conseil, au Conseil économique et social européen et au Comité des Régions sur la création d'un système de surveillance du financement du terrorisme, 25 octobre 2011, en ligne sur le site.

1904 Voy. Les avis 2010/C 92/01 du 7 octobre 2009, JOUE C92/1 du 10 avril 2010, 2009/C 229/02 du 18 février 2009 et JOUE C 229/6 du 23 septembre 2009 et l'avis sur la refonte pour la comparaison des empreintes digitales du 5 septembre 2012 en ligne sur le site du CEPD.

1905 Voy. L'avis 2012/C 336/06 du 6 juillet 2012 du CEPD relatif à la proposition de règlement du Conseil sur la migration du système d'information Schengen (SIS) vers le système d'information de deuxième génération (SISII).

1906 Voy. L'avis 2006/C 97/03 du 20 janvier 2006 sur le système d'information sur les visas.

1907 Voy. L'avis 2012/C 336/05 du 29 juin 2012 du CEPD relatif à la communication de la Commission européenne au Conseil et au Parlement européen concernant l'établissement d'un Centre européen de lutte contre la cybercriminalité.

1908 Le Tribunal de la fonction publique s'est prononcé pour la première fois sur une demande d'intervention du CEPD en 2008 et a admis cette intervention sur le fondement de l'article 40 alinéa premier du Statut de la Cour selon lequel « [l]es États membres et les institutions de l'Union peuvent intervenir aux litiges soumis à la Cour de justice » : TFPUE (ord.), 20 novembre 2008, Pachtitis c. Commission européenne, aff. F-35/08.

1909 Le Tribunal de première instance a admis pour le première fois une demande d'intervention du CEPD dans l'affaire Bavarian Lager : TPICE, 8 novembre 2007, The Bavarian Lager Co. Ltd c. Commission des Communautés européennes, aff. T-194/04, Rec. II-04523.

1910 CJCE, G. Ch. (ord.), 17 mars 2005, Parlement européen c. Conseil de l'Union européenne, aff. C-317/04, Rec. I-02457.

1911 Cette mission consultative est définie à l'article 28 du règlement n° 45/2001 : « 1. Les institutions et organes communautaires informent le contrôleur européen de la protection des données lorsqu'elles élaborent des mesures administratives relatives au traitement de données à caractère personnel impliquant une institution ou un organe communautaire, seuls ou conjointement avec d'autres. 2. Lorsqu'elle adopte une proposition de législation relative à la protection des droits et libertés des personnes à l'égard du traitement de données à caractère personnel, la Commission consulte le contrôleur européen de la protection des données ».

d'intervention du CEPD reste conditionné par la nature de la procédure introduite devant la Cour. Ainsi, ce droit ne peut pas s'exercer dans le cadre de procédures préjudicielles. La Cour de justice a par exemple jugé irrecevable la demande d'intervention du CEPD dans une procédure préjudicielle portant sur les traitements de données personnelles effectués aux seules fins de journalisme tels que prévus par la directive n° 95/46 CE[1912]. En effet, la Cour considère traditionnellement que le droit d'intervenir des personnes physiques ou morales devant la Cour de justice, régi par l'article 40 de son statut, ne s'applique qu'aux procédures contentieuses tendant à trancher un différend [1913] . Or, les renvois préjudiciels en interprétation et en appréciation de validité ne visent pas à trancher un différend mais seulement à assurer l'unité d'interprétation du droit communautaire par une coopération entre la Cour et les juridictions nationales[1914] . Si le CEPD a un pouvoir de conseil qui lui permet d'intervenir devant les juridictions de sa propre initiative, à ce jour il n'a encore porté aucune affaire devant la Cour de justice. Cela s'explique par le fait que la compétence de la Cour de justice se trouve limitée par les actes juridiques européens, notamment en ce qui concerne les droits de la personne faisant l'objet d'un fichage puisque la prééminence appartient alors aux autorités nationales de contrôle et au juge national. On peut espérer qu'en cas de doute sur ces questions, le CEPD saisira la Cour de justice[1915]. Malgré cette limite, le CEPD est intervenu depuis 2005, sur demande des institutions, dans plusieurs affaires pour clarifier les éléments de la protection des données personnelles [1916]. Ainsi le CEPD a été sollicité pour la première fois en 2011 par le Tribunal de la fonction publique dans une affaire relative au transfert de données médicales entre les services médicaux de la Commission et du Parlement. Celui-ci l'a invité à intervenir après en avoir informé les parties pour qu'elles puissent présenter des observations sur l'opportunité d'une telle invitation [1917]. Le CEPD a été sollicité pour la seconde fois, en 2013, par la Cour de justice de l'Union européenne dans l'affaire relative à l'obligation de conservation des données de connexion par les fournisseurs d'accès à Internet. Saisie d'une question préjudicielle relative à la validité de la directive communautaire qui prévoyait une telle obligation, la Cour a décidé de solliciter le Contrôleur européen sur une série de questions[1918]. Parmi les affaires qui ont abouti à une analyse au fond et, par conséquent, à un examen des interventions, on trouve : le transfert des données PNR des passagers aériens vers les États-

---

1912 CJCE (ord.), 12 septembre 2007, Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy, aff. C-73/07, Rec. I-07075

1913 Il s'agit d'un motif d'ordre procédural, voy. l'ordonnance du Président de la Cour, 12 septembre 2007, aff. Satamedia Oy, C-73/07.

1914 v. par exemple : CJCE (ord.), 26 février 1996, Biogen Inc. c. Smithkline Beecham Biologicals SA, aff. C-181/95, Rec. I-00717.

1915 S. P LAUSINOTTE, *L'identification biométrique, Champs, acteurs et controverses,* Editions de la maison de science de l'homme, 2014, p. 320 et ss.

1916 CEPD, Rapport annuel 2008, Luxembourg, Office for Official Publications of the European Communities, 2009, 130 p., p. 66.

1917 TFPUE, 5 juillet 2011, V c. Parlement européen, aff. F-46/09

1918 Cette demande d'avis se base sur l'article 24 du Statut de la Cour.

Unis [1919], l'indépendance des autorités de protection des données personnelles[1920], la mise en œuvre du droit d'accès à ses propres données personnelles[1921], la conciliation entre le droit d'accès aux documents administratifs et le droit à la protection des données personnelles[1922] et la base juridique de la directive 2006/24/CE sur la conservation de données [1923] . Les observations du CEPD ont été reprises par la Cour de justice dans son avis concernant la conclusion de l'accord PNR avec le Canada[1924], mais avec une conclusion différente du CEPD qui avait estimé l'accord non conforme au droit de l'UE en matière de protection des données[1925]. L'accord envisagé prévoyait que les données de dossiers passagers (*Passenger Name Record*, ci-après les « données PNR »), qui sont collectées par les transporteurs aériens auprès des passagers à des fins de réservation des vols entre le Canada et l'Union européenne, soient transférées aux autorités canadiennes compétentes, puis traitées et utilisées par ces dernières dans le but de prévenir et de détecter des infractions terroristes ou d'autres actes graves de criminalité transnationale, tout en fixant un certain nombre de garanties quant au respect de la vie privée et de la protection des données à caractère personnel des passagers. Selon le CEPD, premièrement, le projet d'accord ne garantissait pas un recours judiciaire effectif. Deuxièmement, le traitement des données PNR à des fins de « prévision policière » était systématique et particulièrement intrusif. Enfin, le contrôle du respect des exigences de la protection des données par le biais d'une autorité indépendante, exigence figurant tant dans la Charte (art. 8 § 3) que dans le Traité (Article 16 § 2 TFUE), n'était pas garanti[1926]. La Cour de justice n'a pas totalement suivi le raisonnement du CEPD et, même si elle a validé le système

---

1919 CJCE, G. Ch., 30 mai 2006, Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes, aff. C-317/04 et C-318/04.

1920 CJUE, G. Ch., 9 mars 2010, Commission européenne c. République fédérale d'Allemagne, aff. C-518/07, Rec. I-01885 ; CJUE, G. Ch., 16 octobre 2012, Commission européenne c. République d'Autriche, aff. C-614/10 ; CJUE, G. Ch., 8 avril 2014, Commission européenne c. Hongrie, aff. C-288/12.

1921 TFPUE, 15 juin 2010, Pachtitis c. Commission européenne, aff. F-35/08

1922 C'est dans l'affaire Bavarian Lager que le CEPD est intervenu sur cette question. Cependant son avis n'a pas été suivi. CJUE, G. Ch., 29 juin 2010, Commission européenne c. The Bavarian Lager Co. Ltd., aff. C-28/08 P, Rec. I-06055 ; TPICE, 8 novembre 2007.

1923 CJUE, G. Ch., 10 février 2009, Irlande c. Parlement européen et Conseil de l'Union européenne, aff. C- 301/06, Rec. I-00593.

1924 Voy. L'Avis 1/15 de la Cour, Gr. Ch. du 26 juillet 2017.

1925 Voy. Les conclusions de l'Avocat général P. Mengozzi présentées le 8 septembre 2016.

1926 Voy. la demande d'avis du Parlement sur le projet d'accord PNR avec le Canada, Avis1/15, du 5 avril 2016, disponible sur le site : https://edps.europa.eu/sites/edp/files/publication/16-04-05_pleading_canada_pnr_en.pdf. Le CEPD avais déjà rendu son avis le 30 septembre 2013 sur les propositions de la Commission du 19 juillet 2013 relatives à la signature et à la conclusion de l'accord envisagé. Dans cet avis, le CEPD soulevait une série d'interrogations quant à la nécessité et à la proportionnalité des systèmes PNR et du transfert massif de données PNR vers des pays tiers, il mettait en doute le choix de la base juridique matérielle et faisait part de diverses observations et propositions quant aux différentes dispositions de l'accord envisagé. Le texte complet de l'avis du CEPD est disponible à l'adresse Internet suivante : https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2013/13-09-30_Canada_FR.pdf.

PNR [1927] estimant que les ingérences envisagées par l'accord étaient susceptibles d'être justifiées par un objectif d'intérêt général de l'Union, elle a censuré les modalités de sa mise en œuvre. Alors que d'autres acteurs comme certaines franges politiques du Parlement européen, le Contrôleur européen de la protection des données ou le G29 (Organe européen composé de représentants des autorités nationales chargées de la protection des données) ont remis en question depuis des années l'existence même du PNR en raison de la surveillance de masse qu'il semble organiser par définition[1928]. On peut noter que si la Cour a souvent suivi l'avis du CEPD, elle s'y est parfois opposée. Cependant, les pouvoirs des autorités de protection des données ne se limitent pas à un pouvoir d'influence. Celles-ci disposent également d'un pouvoir de contrainte.

B. Une mission de contrôle

225 L'extension progressive de la mission de contrôle. Dans sa mission de supervision, le CEPD est chargé du contrôle préalable de certains traitements effectués par les institutions européennes en raison de risques particuliers[1929]. Cette tâche comprend la tenue d'un registre des traitements qui lui sont notifiés. Ces traitements peuvent faire l'objet de recommandations que l'institution ou l'organe doivent mettre en œuvre dans l'objectif de respecter les règles en matière de protection des données personnelles. Le CEPD publie des « lignes directrices » thématiques [1930] afin de faciliter la mise en œuvre des règles dans un mouvement de responsabilisation des institutions en amont[1931] et pour rendre public les critères utilisés dans le cadre des contrôles. De plus, dans sa mission de contrôle il peut, conformément à l'article 33 du règlement 45/2001, recevoir et traiter des plaintes du personnel de l'Union européenne ainsi que de toute autre personne qui estime que ses données n'ont pas été traitées dans le respect des règles de la part des institutions ou organes de l'Union. Il s'agit d'un recours direct, qui n'impose pas d'avoir préalablement épuisé les voies de recours officielles définies par le statut des fonctionnaires de l'Union. Lors de l'ouverture d'une enquête, le CEDP dispose de compétences étendues lui permettant d'avoir accès aux données personnelles et aux locaux du

1927 La Cour note en effet que « l'accord envisagé vise, notamment, à garantir la sécurité publique au moyen d'un transfert des données PNR vers le Canada et de l'utilisation de celles-ci dans le cadre de la lutte contre des infractions terroristes et la criminalité transnationale grave » (§ 148).

1928 Ainsi l'arrêt Digital Rights Ireland pouvait laisser espérer une invalidation du système PNR en général en base à la condamnation que la Cour y prononce de tout stockage de données de masse, et ce de façon indifférenciée, condamnation réitérée dans son arrêt Schrems ou encore dans l'arrêt Tele2 Sverige.

1929 Voy. art. 27 du règlement 45/2001.

1930 Voy. Par exemple les lignes directrices sur le traitement des données de santé, les enquêtes administratives et procédures disciplinaires.

1931 On constate toutefois que dans son rapport annuel de 2011 le CEPD se déclare « déçu » par la mise en œuvre de ses lignes directrices de la part des institutions.

responsable ou du sous-traitant qui traitent les données sans l'autorisation préalable du juge. Dans un objectif de transparence, le CEPD a élaboré un guide méthodologique des inspections[1932]. Si la plainte est jugée recevable, le CEPD mène une enquête et la décision finale est notifiée à l'auteur de la plainte et au responsable du traitement des données. Les pouvoirs dont il dispose peuvent justifier la prise de mesures telles que le simple conseil aux personnes concernées, l'interdiction, la destruction, le verrouillage, l'effacement des données objets du traitement, l'avertissement, l'admonestation au responsable ou la saisine de la Cour de justice. Ses décisions peuvent faire l'objet d'une contestation devant la CJ[1933]. Ainsi, trois décisions du CEPD ont été contestées devant la Cour, mais les requêtes ont été rejetées à un stade précoce[1934]. De plus, depuis janvier 2004 le CEPD s'est vu attribuer un pouvoir de contrôle spécifique concernant le traitement des données par l'unité centrale d'Eurodac. Il intervient notamment en assurant le contrôle des données partagées entre le CEPD et les autorités de contrôle nationales[1935]. Depuis avril 2013, il a repris la responsabilité du contrôle de la protection des données traitées dans le cadre des systèmes Schengen II, Vis, Europol et en partie pour le système d'information des douanes de l'Union. Il s'agit du même modèle de supervision qu'Eurodac, associant dans un mécanisme de coordination les autorités de contrôle nationales concernant les données relevant du niveau national et le CEPD pour les données relevant du niveau européen. Conformément au règlement (UE) 2016/794 du Parlement européen et du 11 mai 2016 du Conseil (« règlement Europol »)[1936], le CEPD a pour tâche, depuis le 1er mai 2017, de contrôler la licéité du traitement de données à caractère personnel par Europol[1937]. Son rôle est de veiller à ce que le bon équilibre soit trouvé entre les droits en matière de protection des données et l'intérêt public essentiel en matière de sécurité. Pour réaliser ce travail de contrôle, le CEPD s'acquitte de différentes tâches, en tenant également compte de la dimension transfrontalière (aux niveaux européen et international) du traitement des données: les inspections effectuées par le CEPD en collaboration avec les autorités de contrôle nationales; le CEPD conseille Europol, de sa propre initiative ou en réponse à une consultation, sur toutes les questions qui concernent le traitement de données à caractère personnel, notamment lorsque l'Agence définit un règlement intérieur ou des mesures administratives liées à la protection des libertés et des droits fondamentaux et aux libertés à l'égard du traitement des données à

1932 Voy. Le document « Inspections conduced by the EDPS, Policy Paper, 2013 » en ligne sur le site du CEPD.

1933 Voy. l'art. 32. 3 du règlement 45/2001.

1934 Voy. Par exemple, l'affaire T-164/09, kitou c. CEPD, non-lieu à statuer.

1935 Voy. Le Rapport annuel CEPD 2009, p. 49 ; et Conférence « Upholding Freedom of Movement: an Improved Schengen Governance » Parlement européen, Bruxelles 8 février 2012, Intervention de M. Peter Hustinx, Data Protection and Schengen Governance.

1936 Le règlement Europol confère à toute personne physique le droit d'être informée du fait que des données à caractère personnel la concernant sont traitées ou non par Europol, de demander la rectification, l'effacement ou la limitation de ces données et, de manière plus générale, le droit à ce que ses données soient traitées conformément aux principes en matière de protection des données, notamment de façon loyale et licite.

1937 Europol est l'organe de l'UE qui collabore activement avec les services répressifs des États membres de l'UE dans la lutte contre la grande criminalité internationale et le terrorisme. Europol travaille également avec de nombreux États tiers partenaires et des organisations internationales, en particulier dans la lutte contre le terrorisme, la criminalité informatique et le trafic d'êtres humains.

caractère personnel ou en référence au transfert et à l'échange de données à caractère personnel ; lorsque de nouveaux types d'opérations de traitement effectuées par Europol (notamment en raison des catégories de données concernées ou de l'utilisation de nouvelles technologies ou procédures) présentent des risques spécifiques pour les personnes physiques, ces opérations de traitement doivent être soumises au CEPD pour consultation préalable. En se fondant sur les faits présentés par Europol, le CEPD examinera le traitement des données à caractère personnel eu égard aux garanties relatives à la protection des données prévues dans le règlement Europol et à tous les principes et règles présentant une pertinence en la matière. Dans la plupart des cas, cet exercice débouchera sur la formulation d'un ensemble de recommandations que le responsable du traitement devra mettre en œuvre afin de s'assurer de la conformité avec les règles en matière de protection des données. Le CEPD reçoit et examine les réclamations des personnes physiques qui estiment que leurs données à caractère personnel ont été traitées de manière incorrecte par Europol. Si une réclamation est recevable, le CEPD mène une enquête. Dans les cas concernant des données provenant d'un ou plusieurs États membres, le CEPD consultera l'autorité de contrôle nationale ou l'État membre concerné. Il adopte ensuite une décision qui est communiquée à l'auteur de la réclamation que ce soit en tant que suivi à une réclamation ou de sa propre initiative, par exemple sur la base des informations qu'Europol doit transmettre au CEPD conformément au règlement Europol (en ce qui concerne les nouveaux projets d'analyse opérationnelle, les données conservées plus de cinq ans, certains transferts vers des pays tiers ou à des organisations internationales, etc.), le CEPD peut mener des enquêtes pour contrôler la conformité concernant un sujet spécifique. Comme cela a été mentionné, l'un des aspects essentiels de ce contrôle réside dans la collaboration avec les autorités de contrôle nationales, notamment au sein du comité de coopération d'Europol récemment créé. Il s'agit d'un forum ayant une fonction consultative et permettant de discuter de questions courantes tout en travaillant ensemble à l'élaboration, par exemple, de lignes directrices et de bonnes pratiques. Afin de contrôler le respect des dispositions fixées par le règlement Europol, le CEPD collaborera avec le délégué à la protection des données (DPO) désigné par Europol.

Section II. Le Groupe de travail (G29)

226 Le droit souple. Un autre acteur qui a énormément contribué à l'application cohérente du cadre juridique en matière de protection des données personnelles est le Groupe de travail article 29 (ci-après G29). L'article 29 de la directive 95/46 du 24 octobre 1995 sur la protection des données et la libre circulation de celles-ci a institué un groupe de travail (G29) rassemblant les représentants de chaque autorité nationale de protection des données. Cette organisation a pour mission de contribuer à élaborer des normes européennes à travers ses recommandations, avis et autres documents. Cette activité a contribué à la mise en œuvre homogène de la directive 95/46 par les États membres. Ainsi, le G29 joue un rôle crucial dans la coopération avec les autorités nationales de protection des données mais aussi avec les autorités européennes et internationales, notamment avec la Commission, le Contrôleur européen à la protection des données, le Conseil de l'Europe et la *Federal Trade Commission*[1938] aux États-Unis en donnant des conseils sur tout projet ayant une incidence sur la protection des données et des libertés des personnes. Tout d'abord, le G29 dispose d'un large pouvoir d'initiative quant aux sujets traités. En effet, en fonction de son indépendance statutaire[1939], le G29 a pu traiter des questions relevant de l'ex-troisième pilier en matière de coopération policière et judiciaire. Ses travaux n'ont aucune force contraignante sur le plan juridique mais font autorité en matière d'analyse et d'interprétation de la directive européenne de 1995. Ainsi, ses avis sont sources d'informations précieuses afin de permettre aux professionnels d'appliquer de façon uniforme la réglementation européenne à des sujets particuliers. L'intense activité de travail du G29 illustre son importance dans l'élaboration des règles européennes en matière de protection des données à caractère personnel (§1). Ainsi, les avis du G29 ont une influence tant sur les acteurs économiques que sur les acteurs institutionnels tels que la Commission européenne[1940] (§2).

§1 Le rôle transgouvernemental joué par le G29 dans la protection des données.

Un réseau transgouvernemental. Le G29 représente une structure originale dans l'architecture européenne. Il semble à mi-chemin entre une agence structurée et un comité classique conseillant la Commission[1941].

1938 La FTC est une agence chargée de réguler les pratiques commerciales et de concurrence. Elle a un bureau en charge de la protection des consommateurs et elle intervient à ce titre dans la protection des données personnelles.

1939 Voy. art. 30 de la directive 95/46.

1940 P. CURCH, *Should you care what the article 29 working party says*, 20 septembre 2011, article publié sur le site du cabinet d'avocats « Linklaters ».

1941 Les avis et recommandations du G29 sont en ligne sur le site Internet de la Commission : http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinion-recommendation/index_en.htm

Si l'article 29 de la directive formalise et institutionnalise cette coopération informelle préexistante entre autorités nationales de protection des données personnelles en Europe, elle ne lui confère cependant pas de pouvoirs d'une portée comparable à ceux de ses membres, puisqu'il ne s'agit que d'une instance consultative, présentant ses avis à la Commission et lui proposant éventuellement d'agir dans le cadre d'actes délégués, soumis de toutes façons à une procédure de comitologie fortement contrôlée et contrainte par les exécutifs nationaux des États membres. Le groupe G29 a été amené à adopter un grand nombre d'avis sur des thèmes variés (A), toutefois ce précieux travail n'a pas été accompagné par l'institutionnalisation de ce réseau transgouvernemental (B).

A. Le pouvoir d'initiative du G29 dans la mise en œuvre de la directive 95/46

227 Un champ d'intervention particulièrement large. L'article 30 de la directive 95/46 prévoit l'intervention du G29 sur « toute question concernant la protection des personnes à l'égard du traitement de leurs données à caractère personnel dans la Communauté »[1942]. Son rôle de conseil de la Commission européenne et dans l'harmonisation des règles en matière de protection des données à caractère personnel lui ont permis d'avoir un statut indépendant[1943]. Ainsi, il dispose d'une grande liberté de choix dans la forme des décisions qu'il prend (avis, recommandations, documents de travail et rapports) et dans les sujets qu'il traite[1944]. L'article 30, paragraphe 1 de la directive 95/46 prévoit les missions du Groupe : il examine toute question portant sur la mise en œuvre des dispositions nationales prises en application de la directive en vue de contribuer à leur mise en œuvre homogène ; il donne à la Commission un avis sur le niveau de protection dans la Communauté et dans les pays tiers ; il conseille la Commission sur tout projet de modification de la directive, sur tout projet de mesures additionnelles ou spécifiques à prendre pour sauvegarder les droits et libertés des personnes physiques à l'égard du traitement des données à caractère personnel, ainsi que sur tout autre projet de mesures de l'Union ayant une incidence sur ces droits et libertés ; il offre un avis sur les codes de conduite élaborés au niveau de l'Union. Ainsi, le Groupe peut émettre de sa propre initiative des recommandations sur toute question concernant la protection des données des personnes à l'égard du traitement de données à caractère personnel dans la Communauté (art. 30.3). Il établit un rapport annuel sur l'état de la protection des personnes physiques dans la Communauté (art. 30.3). Parmi ses travaux, plusieurs avis sont venus préciser le champ d'application et les principes de la directive 95/46. Ses avis peuvent aussi être sollicités par saisine de la

---

1942 Le G29 a contribué à l'élaboration de plus de 124 avis, 13 recommandations et plus de 152 documents de travail et rapports. Sur l'intense activité du G29 voy. le site. http://ec.europa.eu/justice/data-protection.index_en.htm.

1943 Voy. art. 29 de la directive 95/46 et le considérant 65.

1944 Ainsi le G29 est intervenu notamment sur des questions concernant l'ex-troisième pilier, même si la décision cadre 2008/977/JAI ne fait aucune référence au rôle du G29. Voy. sur l'extension de son champ de compétence Y POULLET et S. GUTWIRTH, The contribution of Article 29 Working Party to the Construction of Harmonized European Data Protection System : an illustration of Reflexive Gouverance ?» in M. PEREZ ASINARI P. PALAZZI (dir.), *Défis du droit à la protection de la vie privée*, Bruylant, 2008, p. 570.

Commission, il se prononce alors sur le niveau de protection adéquat des législations des États tiers et aussi sur le niveau de protection des systèmes PNR[1945]. En effet, bien que la directive 95/46/CE, en tant qu'instrument antérieur au traité de Lisbonne, ne soit pas applicable dans une large mesure à l'espace de liberté, de sécurité et de justice (ELSJ), le groupe de travail « Article 29 » rappelle que ses principes sont généralement applicables dans le domaine de la protection des données. De plus, ces principes apparaissent dans d'autres instruments, comme la convention 108, qui sont applicables à l'ELSJ[1946]ainsi que dans la proposition de règlement européen en matière de protection des données personnelles[1947]. Les recommandations visent à harmoniser les modalités particulières d'application de la directive 95/46 notamment dans des domaines spécifiques comme la collecte des données sur Internet. De plus, le Groupe peut se prononcer sur les codes de conduite élaborés au niveau communautaire[1948]. Les autorités de contrôle dans leur ensemble (au niveau national et au niveau de l'UE) forment un réseau assez complet puisqu'elles sont appelées à coopérer entre elles, mais elles constituent également un groupe de protection des personnes à l'égard du traitement des données (G29). Cependant, la prolifération des organismes et autorités chargés de la protection des données n'est pas propice à la sensibilisation des citoyens à leur existence. La présence d'une multitude d'organismes sème la confusion et crée une complexité inutile. En février 2008, deux enquêtes Eurobaromètre ont été publiées. Les principaux résultats de ces enquêtes étaient qu'une majorité des citoyens de l'Union expriment des inquiétudes concernant la protection des données et que les autorités nationales de protection des données restent relativement méconnues de la plupart des citoyens de l'Union européenne. Au niveau européen, une meilleure coopération entre les autorités de protection des données sera nécessaire afin de faire face de manière efficace aux problèmes ayant un impact dans plusieurs États membres. Le Comité européen de la protection des données remplacera le Groupe de l'article 29 et deviendra un organe de l'Union qui possède la personnalité juridique. Il sera composé des autorités nationales et du Contrôleur européen à la protection des données.

1945 Voy. Les avis WP 78, 87 et 178 adoptés le 13 juin 2003, 29 janvier 2004 et 16 décembre 2010. Voy. aussi le communiqué de presse du G29 du 5 février 2015 sur la mise en place d'un système PNR européen.

1946 Voy. L'avis 01/2014 du groupe de travail « Article 29 » sur la protection des données sur l'application des notions de nécessité et de proportionnalité et la protection des données dans le secteur répressif.

1947 G29 WP191, Avis 01/2012 adopté le 23 mars 2012 et WP 199, Avis 08/2012 adopté le 5 octobre 2012.

1948 Voy. L'article 27 de la directive 95/46.

B. La valeur juridique des avis et recommandations du G29

Les recommandations et avis du G29 n'ont pas de valeur contraignante. Cependant ils peuvent faire autorité et être pris en compte par la Cour de justice, par le législateur, par les autorités de contrôle nationales et avoir une influence sur les acteurs économiques et auprès de la Commission[1949]. Ainsi, dans l'affaire *Promusicae*, l'Avocat général Kokott a pris en compte les avis rendus par le G29[1950], estimant qu' « ils sont susceptibles d'apporter une contribution importante à la solution des questions relatives au droit de la protection des données ». Toutefois, c'est seulement en 2014 que la référence à ses avis apparaît dans les décisions de la Cour de justice. Même si ses avis ne lient pas la Cour, dans l'affaire *Google Spain*, l'Avocat Général Jääskinien, dans la présentation de ses conclusions, se fondait ouvertement sur l'avis du G29 concernant les moteurs de recherche [1951] . Le G29 contribue par ses travaux à la construction et à l'interprétation du droit européen en matière de protection des données à caractère personnel. Ainsi, les travaux du G29 ont eu un impact sur l'élaboration des règles internes d'entreprises (BCR) en tant que fondement légal permettant de transférer des données en dehors de l'Union européenne. Ses avis ont aussi eu un impact sur les travaux des institutions communautaires : le Parlement se réfère explicitement aux avis du G29[1952] dans sa prise de position en matière de PNR, dans l'affaire *Swift* ainsi que sur la mise en application de la décision de la Cour de justice dans *Google Spain*[1953]. Ainsi, l'avis émis suite à l'arrêt de la Cour de justice européenne du 30 mai 2006, qui annule la décision d'adéquation de la Commission ainsi que la décision du Conseil relative à la conclusion de l'accord PNR, énonce que conformément à cet arrêt, les institutions communautaires sont tenues de mettre fin à l'accord conclu avec les États-Unis en matière de transfert de données PNR. Par cet avis, le Groupe de travail demande instamment qu'un nouvel accord entre les États-Unis et l'Union européenne soit conclu en temps utile, c'est-à-dire avant l'expiration du délai imparti, afin d'éviter tout vide juridique et de garantir le maintien d'un niveau de protection des droits et libertés des passagers au moins égaux au niveau actuel. L'avis conclut également que l'arrêt de la Cour montre une fois de plus les difficultés dues à la division artificielle entre les piliers et la nécessité d'un cadre cohérent en matière de protection des données[1954]. Dans l'avis sur l'affaire *Swift* concernant le traitement des données à caractère personnel par la Société de télécommunications

1949 Par ailleurs, la Commission européenne est tenue de prendre en compte les avis rendus par le G29 et de l'informer des suites qui y sont apportées, en application de l'art 3§5 de la directive.

1950 CJ, Promusicae c. Telefónica de España SAU, aff. C-275/06, 29 janvier 2008.

1951 Voy. Les conclusions de l'Avocat général, présentées le 25 juin 2013 dans l'affaire *Google Spain,* points 36, 55 et 56. D'ailleurs les juridictions nationales peuvent se prévaloir des avis du G29 dans leurs décisions. Toutefois les décisions citant le G29 sont rares. On peut ici citer la décision du Tribunal de commerce de Paris qui a jugé le 28 janvier 2014 que la notion de « moyens » devait être interprétée dans un sens large, se référant à l'avis du G29 du 4 avril 2008 sur les moteurs de recherche. Voy. En ce sens TGI Paris, 28 janvier 2014, M. Xc/Google Inc. Et Google France.

1952 Voy. Le Rapport du Parlement européen sur le premier rapport de la mise en application de la directive relative à la protection des données personnelles COM/2003/265.

1953 Voy. L'Avis 225 du G29, Guidelines on the implementation of the Court of Justice judgement on *Google Spain,* C131/121.

1954 Voy. L'Avis 5/2006 sur l'arrêt de la Cour de justice du 30 mai 2006 dans les affaires jointes C-317/04 et C-318/04 relatives au transfert de données PNR aux États-Unis.

interbancaires mondiales (Swift), le groupe a souligné que les droits fondamentaux devaient être préservés, même dans le cadre de la lutte contre le terrorisme et la criminalité. Il insiste donc sur le respect des principes de protection des données à l'échelle mondiale[1955]. De même, son influence a pu être observée auprès des acteurs économiques. Il convient de rappeler que les avis et recommandations du G29 peuvent être adoptés à la majorité simple, et ne reflètent pas forcément l'adhésion de toutes les autorités nationales de protection. Toutefois, l'influence de ces textes peut s'expliquer par le fait que leur prise en compte permet d'anticiper la position d'autres autorités et d'apporter une sécurité juridique. Ainsi, les entreprises multinationales et leurs avocats tiennent en compte les avis et recommandations du G29 dans leur politique de mise en conformité[1956]. Ce fut le cas de Google qui face à la demande du G29 de réduire la durée de conservation des données des utilisateurs a publiquement accepté cette invitation[1957]. L'influence du G29 s'illustre aussi auprès de la Commission européenne : ses travaux ont eu un impact sur la construction de « l'acquis » de l'Union en matière de données personnelles[1958] et dans le cadre de la réforme. Ainsi, les travaux du G29 ont inspiré la Commission européenne dans la proposition du règlement européen. Néanmoins, au sein des États membres, les autorités de contrôle nationales reprennent les avis et recommandations du G29 pour motiver leurs prises de positions, bien que le G29 n'ait ni le rôle ni les pouvoirs des autorités de contrôle nationales. Ainsi la Commission a toujours soutenu le travail du G29, invitant les États membres à « adapter leurs pratiques nationales afin de les aligner aux avis du G29 »[1959]. Bien que les avis et recommandations du G29 n'aient pas de valeur contraignante, leur rôle novateur et simplificateur est susceptible de contribuer de manière substantielle à la construction du cadre juridique en matière de protection des données personnelles. Ainsi le Groupe a eu le mérite de permettre une « coopération transgouvernementale »[1960]. Compte tenu de l'influence du G29, le nouveau règlement 679/16 a institutionnalisé son rôle en le remplaçant par le Comité européen de la protection des données à caractère personnel (Comité EDP), avec un statut différent et des pouvoirs renforcés.

1955 Avis 10/2006 sur le traitement des données à caractère personnel par la Société de télécommunications interbancaires mondiales (SWIFT).

1956 Voy. P. Church, « Should you care what the Article 29 working party says? », 20 septembre 2011, article publié sur le site du cabinet d'avocats Linklaters.

1957 Voy. « Google, Response to the Article 29 Working Party Opinion on Data Protection Issues Related to Search Engines », 8 septembre 2008, p. 13, consultable sur le site www.scribd.com

1958 Sur le rôle de groupe de pression institutionnalisé du G29 v. Y. Poullet, S. Gutwirth Serge, O. De Shutter, V. Moreno-Lax, « The contribution of the Article 29 Working Party to the construction of a Harmonised European Data Protection System : an illustration of Reflexive Gouvernance ? », in M. Perez Asinari, P. Palazzi (dir.), *Défis du droit à la protection de la vie privée. Challanges of Privacy and Data Protection Law*, Bruylant, 2008 p. 579.

1959 Voy. En ce sens la Communication de la Commission au Parlement européen et du Conseil : Suivi du Programme de travail pour une meilleure mise en œuvre de la directive sur la protection des données, 7 mars 2007, COM/2007/0087 final.

1960 Sur le rôle de groupe de pression institutionnalisé du G29 v. Y. POULLET, S. GUTWIRTH, O. De SHUTTER, V. MORENO-LAX, *The contribution of the Article 29 Working Party to the construction of a Harmonised European Data Protection System : an illustration of Reflexive Gouvernance* ? , in Jean Yves Carlier, Olivier de Shutteret Marc Verdussen (dir.), *Human Rights in the web of Gouvernence : towoards a learning-based fundamental rights policy for the Europen union*, 2010, p. 253.

§2 L'institutionnalisation du rôle du G29

228 Le Comité européen de la protection des données. L'architecture de coopération entre les autorités nationales de protection a changé avec le règlement 679/16 et un nouvel organe européen : le Comité européen de protection des données (ci-après dénommé « Comité européen »). En effet, l'objectif de la réforme est d'assurer une application plus uniforme et plus cohérente de la réglementation au sein des États membres en améliorant la protection des droits fondamentaux et en contribuant au bon fonctionnement du marché intérieur[1961]. À cet égard, la mise en place d'un organe transnational de régulation est indispensable face aux défis technologiques. Ainsi l'article 68 du règlement prévoit l'instauration du Comité européen de la protection des données à caractère personnel qui remplace le G29. Le Comité européen de la protection des données est un autre acteur important qui veille à ce que les règles de protection des données soient appliquées de manière efficace et cohérente dans l'ensemble de l'UE. Le RGPD a établi le Comité européen en tant qu'organe de l'Union doté de la personnalité juridique. C'est le successeur du groupe de travail « Article 29 ». La composition du Comité européen est inchangée, puisque à l'instar du G29 le Comité européen de protection des données est composé de l'ensemble des présidents des autorités nationales ainsi que du contrôleur européen à la protection des données (EDPS), qui est vice-président de droit du Comité européen. Le Comité sera dirigé par un président et deux vice-présidents qui seront élus à la majorité simple pour un mandat de cinq ans renouvelable une fois. La Commission européenne est habilitée à participer à ses activités bien que n'en étant pas membre. Les missions du Comité sont plus étendues et le règlement prévoit que les autorités de contrôle sont tenues d'approfondir leur coopération pour parvenir « à l'application cohérente du règlement dans l'ensemble de l'Union »[1962]. Ainsi, le règlement instaure une gouvernance harmonisée et attribue à l'Autorité de contrôle une compétence et un pouvoir de mise en œuvre renforcés en créant la notion d'Autorité de contrôle chef de file. Ce faisant, l'établissement principal ou unique du responsable du traitement ou du sous-traitant constitue le critère principal de détermination de l'Autorité de contrôle chef de file[1963]. L'Autorité de contrôle chef de file examinera les plaintes et les violations éventuelles. Elle doit cependant coopérer avec les autres autorités concernées « en s'efforçant de parvenir à un *consensus* »[1964] . En cas de différend c'est au Comité de trancher la question. Ainsi le Comité européen de la protection des données veille à l'application cohérente du règlement par les autorités de contrôle, en émettant, « de sa propre

---

1961 Voy. Les considérants 136 et suivants du règlement et l'exposé des motifs de la proposition de règlement du Parlement européen et du Conseil, COM (2012) 11 final, point 3.

1962 Voy. L'article 56 du règlement. Voy. aussi sur ce point l'audition de Mme Viviane Redding, vice-présidente de la Commission européenne chargée de la justice, des droits fondamentaux et de la citoyenneté par la Commission des lois et la Commission des affaires européennes, le mardi 21 février 2012 : « Le G29 est fortement renforcé, désormais doté d'une cohérence, il pourra influencer les autres régulateurs dans un cadre commun. S'il voit un problème émerger, il pourra initier un processus de cohérence pour clarifier et le résoudre » in Sénat, Rapport n°446, 29 février 2012, p. 48.

1963 Défini à Règl. (UE) 2016/679, art. 4. Il s'agit de la notion de « mécanisme de guichet unique » (Règl. (UE) 2016/679, consid. 127 et 128), en vertu duquel les entreprises bénéficieront, pour leurs fichiers transeuropéens, d'un dispositif leur permettant de choisir en Europe l'État et l'APD qui sera leur interlocuteur direct.

1964 Voy. Règl. (UE) 2016/679, art. 60, § 1.

initiative ou, le cas échéant, à la demande de la Commission des avis sur les projets de décisions » des autorités de contrôle[1965]. Ainsi l'Autorité de contrôle doit tenir « le plus grand compte de l'avis du comité et fait savoir au président du Comité par voie électronique au moyen d'un formulaire type, dans un délai de deux semaines suivant la réception de l'avis, si elle maintiendra ou si elle modifiera son projet de décision et, le cas échéant, son projet de décision modifié »[1966]. Toutefois, si le Comité remplace le G29, son statut est différent et ses pouvoirs plus étendus (A) puisque le Comité pourra désormais rendre des avis contraignants (B).

A. Des compétences élargies

Les missions du G29 sont pour l'entrée en vigueur du RGPD désormais transférées au Comité européen de la protection des données. Le Comité européen de la protection des données est institué en tant qu'organe de l'Union et possède la personnalité juridique. Il exerce les missions et les pouvoirs qui lui sont conférés en toute indépendance, c'est-à-dire que le comité ne sollicite ni n'accepte d'instructions de quiconque dans l'exercice de ses missions et de ses pouvoirs. Ses missions sont augmentées, notamment afin d'assurer une application cohérente du règlement. A cet effet, il surveille et garantit la bonne application du règlement. Ainsi, il a l'obligation de conseiller les autorités de contrôle nationales, avec un avis préalable, sur toutes questions d'application générale ou produisant des effets juridiques concernant les traitements liés à l'offre de biens ou de services à des personnes concernées dans plusieurs États membres ou à l'observation de leur comportement ou encore visant à l'adoption d'une liste des traitements soumis à contrôle préalable de l'autorité de contrôle compétente ou à la détermination des garanties appropriées en matière de transfert de données à caractère personnel en dehors de l'Union européenne. Ainsi, à l´instar du G29, il contribuera à l'élaboration des normes européennes par l´émission d´avis adressés à la Commission au nom des États membres sur des questions relatives à la protection des données et de la vie privée. En effet, le Comité exercera une influence importante dans la prise de décisions communautaire. Il aura également pour mission de publier des lignes directrices sur la procédure de suppression des liens vers des données à caractère personnel. Il devra examiner, de sa propre initiative ou à la demande de la Commission, toute question portant sur l´application du règlement, établissant « une doctrine européenne ». Ainsi le Comité devra encourager l'élaboration de codes de conduite et la mise en place de mécanismes de certification, de labels et de marques en matière de protection des données. Le Comité conservera la mission de rendre à la Commission un avis en ce qui concerne l´évaluation du caractère adéquat du niveau de protection assuré par un pays tiers. En ce sens, le G29 a notamment rendu un avis sur le niveau de protection assuré par le nouveau projet de décision d'adéquation « E.U.-U.S. *Privacy Shield* ». Le Comité maintiendra d'ailleurs sa mission de

1965 Voy. Règl. (UE) 2016/679, consid. 139 et art. 70, § 1.

1966 Voy. Règl. (UE) 2016/679, art. 64, § 7.

promouvoir la coopération entre les autorités nationales de contrôle. Il devra également promouvoir l'élaboration de programmes de formation conjoints et faciliter les échanges de personnel entre autorités de contrôle. Le Comité aura l'obligation d´établir un rapport annuel sur la protection des personnes physiques à l'égard du traitement dans l'Union et, s'il y a lieu, dans les pays tiers et les organisations internationales. Le rapport est rendu public et communiqué au Parlement européen, au Conseil et à la Commission. Le rapport annuel présentera notamment le bilan de l'application pratique des lignes directrices, recommandations et bonnes pratiques, ainsi que des décisions contraignantes.

B. Un pouvoir contraignant

229 L'effectivité de l'action du Comité. Comme son prédécesseur le G29, le Comité va contribuer à la création du droit souple[1967] puisque les avis du Comité tout comme ceux du G29 n'ont pas de caractère contraignant. Toutefois il sera obligatoirement et préalablement consulté par les autorités de contrôle nationales sur toute mesure destinée à produire des effets juridiques concernant des traitements liés à l'offre de biens ou de services à des personnes concernées dans plusieurs États membres en raison du mécanisme de cohérence mis en place par le règlement. Le Comité pourra émettre des avis sur les décisions des autorités de contrôle nationales qui auront un caractère quasi contraignant lorsque les autorités nationales n'entendent pas suivre ou déroger à ses avis puisqu'elles seront obligées d'informer le Comité EDP et la Commission. De plus, le non-respect de ce mécanisme de cohérence et de saisine du Comité emporte l'illicéité de la décision prise par cette autorité qui est « dénuée de validité juridique et de caractère exécutoire »[1968]. Le Comité aura ainsi un rôle accru concernant le transfert transnational des données. Il dispose d'un pouvoir contraignant notamment dans l'hypothèse d'un traitement transnational. En effet, dans une telle hypothèse, l'entreprise en cause devra consulter toutes les autorités nationales concernées. Même si au niveau européen l'entreprise ne connaîtra qu'un guichet unique correspondant à l'autorité de l'État membre où l'entreprise ou l´établissement principal a son siège, l'autorité de l'État en question devra travailler conjointement avec ses homologues européens afin d´arriver à une position conjointe. À cet effet, l'Autorité chef de file proposera une mesure. Les autorités européennes devront exprimer leur accord ou non dans un délai de quatre semaines. Si elles ne sont pas d'accord sur un point de droit, la question remontera au Comité européen de protection des données qui sera compétent pour rendre un avis contraignant. Par conséquent, le Comité disposera du pouvoir d´arbitrer les différends entre les autorités nationales de contrôle, procédure qui a pour objet de renforcer la sécurité juridique. Par ailleurs, le Comité joue un rôle plus important dans le dialogue avec les institutions de l'Union européenne. Ainsi il peut être saisi par le Parlement, le Conseil et la Commission en vue de rendre un avis sur des sujets particuliers. La Commission ne peut d'ailleurs pas adopter d'actes délégués sans la consultation préalable du Comité.

1967 L'adoption de l'instrument du règlement aurait dû mettre fin à l'élaboration du droit souple, cependant le fait que le règlement fait beaucoup de renvois à des actes délégués (caractère incomplet du règlement) a permis et justifié la création du Comité EDP.

1968 Voy. Art. 65 du RGPD

CONCLUSION DU CHAPITRE II

Le Contrôleur européen et le G29 sont des acteurs qui participent à la mise en œuvre du cadre juridique en matière de protection des données personnelles. Le Contrôleur européen de la protection des données est chargé de veiller à ce que les droits fondamentaux et les libertés des personnes physiques, et en particulier le droit à la protection de leur vie privée, soient respectés par les institutions et organismes de l'Union. La tâche de conseil des institutions lors de l'élaboration d'un acte ayant un lien avec la vie privée et les données personnelles revêt une importance particulière en ce qu'elle contribue efficacement à la protection des libertés fondamentales des citoyens de l'Union chaque fois qu'une nouvelle législation est adoptée. Toutefois, dans sa mission de conseil des juridictions, le manque total d'affaires portées devant la Cour de justice à son initiative montre que son rôle et sa légitimité vis-à-vis des institutions doit encore évoluer. Concernant sa mission de contrôle, il est chargé du contrôle préalable de certains traitements, il peut recevoir et traiter des réclamations et dispose d'un pouvoir d'enquête. On notera à cet égard qu'il est devenu une autorité incontournable dans le contrôle des systèmes de bases de données et que grâce à son rôle proactif les règles de protection ont tendance à s'unifier. Sa nouvelle compétence sur la protection des données traitées par Europol et sa compétence depuis 2004 pour Eurodac montrent qu'il a vocation à étendre ses missions dans l'ex-troisième pilier désormais communautarisé. Toutefois, l'existence de règles spécifiques et parfois les fonctions régaliennes des États qui perdurent dans ce domaine semblent limiter sa mission de contrôle. Grâce au nouveau règlement général, le CEDP sera chargé du nouveau rôle de présidence du Comité consultatif. Ainsi, il apportera une plus-value à la protection des données personnelles mise en œuvre par les autorités de contrôle nationales. Les améliorations de la législation existante relative à la protection des données se réalisent par une coopération entre les autorités nationales de protection des données au niveau européen grâce à l'action du Groupe de l'article 29. En particulier, les avis et recommandations du Groupe de travail, dans la mesure où ils sont pris en considération par les autorités nationales de protection des données et juridictions de l'UE contribuent à l'élaboration d'une norme commune de l'UE offrant un niveau élevé de protection des données à caractère personnel. Le Groupe de travail de l'article 29 (G29) est un organe consultatif indépendant sur la protection des données et de la vie privée, institué au titre de l'article 29 de la directive 95/46 sur la protection des données. Il se compose de représentants des autorités nationales de l'Union compétentes en matière de protection des données, du CEPD et de la Commission. Le Groupe de travail émet des recommandations, des avis et des documents de travail. Le groupe de travail sera remplacé par le Comité européen de la protection des données dans le cadre du règlement général sur la protection des données. Les avis et recommandations du Groupe sont généralement pris en considération et cités en référence par les autorités nationales de contrôle en matière de protection des données, et sont particulièrement utiles pour l'élaboration d'une norme européenne sur la protection des données à caractère personnel commune à toutes les autorités nationales de contrôle. Toutefois, il s'agit d'un droit souple dépourvu de force contraignante. Ainsi, le règlement 679/2016 a substitué au G29 le Comité consultatif, lequel aura des pouvoirs plus étendus en matière de protection des données et pourra élaborer des normes contraignantes.

CONCLUSION DU TITRE II

Le droit fondamental à la protection des données personnelles a légitimé l'intervention d'autres acteurs que le législateur et le juge dans le processus normatif. Ainsi, ce droit a favorisé la redistribution du rôle de protection des données personnelles entre des acteurs nationaux et européens. Au niveau national, on retrouve des acteurs institutionnels comme les autorités de contrôle nationales et la « société civile ». Ce droit a aussi fourni une justification à l'extension des compétences de ces acteurs afin de permettre la mise en œuvre efficace des règles en matière de protection des données personnelles. Ainsi, ce droit a rendu obligatoire l'institution des autorités de contrôle qui relèvent de la catégorie juridique des autorités administratives indépendantes qui existent dans les différents ordres juridiques nationaux et dans l'ordre juridique de l'Union européenne[1969]. A côté des pouvoirs d'influence, les autorités de protection des données personnelles disposent aussi de pouvoirs de contrainte qui lient les pouvoirs publics ainsi que les particuliers. Ainsi, le droit fondamental à la protection des données a redéfini les compétences traditionnellement attribuées au législateur et au juge. L'interaction de différents acteurs se concrétise par l'élaboration de normes établies en réseaux [1970] . Ces normes s'inscrivent dans « un univers juridique décloisonné, interactif exigeant la collaboration des pouvoirs (constitués) et le fractionnement des compétences en autant d'autorités administratives et de régulateurs »[1971]. Dans cette interaction, les acteurs du droit à la protection des données personnelles jouent « un rôle d'aiguillon »[1972] dans le processus normatif, tant au niveau de l'élaboration des normes juridiques relatives à l'utilisation des données personnelles qu'au niveau de leur application. Toutefois, si la présence d'une multitude d'organismes s'explique par l'exigence de rendre le processus normatif décentralisé, voire plus démocratique, ce système a créé une complexité et une confusion inutiles et la participation de la société civile reste faible. Le cadre de la reforme a créé un système plus cohérent en vue d'assurer l'application efficace de règles et une participation accrue de la société civile.

1969 La première institution de ce type a été créée aux États-Unis dans les années 1880 pour la gestion des Chemins de fer. Pour une analyse historique v. P. ROSENVALLON, *La légitimité démocratique, Impartialité, réflexivité, proximité*, préc., sp. p. 122 et s.. Ces « Indepedant regulatory agencies » se sont également développées par la suite dans les autres ordres juridiques nationaux et dans l'ordre juridique de l'Union européenne. Pour une analyse en droit comparé v. *Annuaire européen d'administration publique,* 2008, Presses universitaires d'Aix- Marseille, Aix-en-Provence, 2009, 496 p.

1970 Ainsi, traditionnellement il revient au législateur, en tant que représentant du peuple, d'élaborer les règles de la vie en société et au pouvoir exécutif leur mise en œuvre et enfin au juge, d'assurer leur respect lors d'un conflit porté devant lui. Cette théorie de la séparation des pouvoirs ainsi conçue est remise en cause par des modèles interétatiques tels que l'Union européenne. Voy. F. OST, M. VAN DE KERCHOVE, *De la pyramide au réseau ? Pour une théorie dialectique du droit*, Publications Fac. St Louis, 2002, 596 p

1971 Sur ce constat s'agissant d'Internet v. M.-C. ROQUES -BONNET, *La Constitution et l'Internet*, Thèse Université Toulouse 1, 2008, 785 p., sp. p. 640.

1972 CONSEIL D 'ETAT, Etude annuelle 2014. *Le numérique et les droits fondamentaux* , préc., sp. p. 268.

CONCLUSION DE LA PARTIE II

Analyser la protection juridictionnelle et non juridictionnelle des données personnelles a conduit à s'interroger sur son efficacité et son contenu. Le constat est celui du rôle de gardienne constitutionnelle de la Cour de justice. Ainsi une analyse combinée de plusieurs arrêts montre une synthèse du raisonnement de la Cour de justice de l'Union européenne et de la Cour européenne des droits de l'homme qui permet de saisir rapidement les principaux éléments de précision apportés par la jurisprudence à chaque notion ou disposition analysée dans la première partie de la thèse. Si dans son raisonnement la Cour de justice s'est longtemps appuyée sur la jurisprudence de la CourEDH, l'étude des derniers arrêts a montré son processus d'autonomisation. L'inscription du droit à la protection des données personnelles dans le droit primaire a contribué à l'évolution du rôle de la Cour de justice. Cette dernière a démontré sa capacité à effectuer un contrôle approfondi et à développer une identité constitutionnelle du droit fondamental à la protection des données. De plus, l'importance de ce droit a justifié la mise en place d'autorités nationales de contrôle et d'organes de l'Union européenne qui viennent au soutien des juridictions de droit commun. Il s'agit du seul droit de la Charte des droits fondamentaux à faire l'objet d'une protection quasi juridictionnelle. De plus, dans l'ensemble des affaires plus récentes, la Cour de justice insiste sur l'importance du rôle de l'autorité nationale de contrôle chargée de surveiller l'application sur son territoire des dispositions adoptées en application de la règlementation en la matière.

CONCLUSION GÉNÉRALE

Il a été constaté que la protection des données à caractère personnel ne peut pas être réduite à la seule protection de la vie privée, avec laquelle elle entretient un simple lien de parenté. L'accélération des échanges de données personnelles dues à leur valeur marchande a rendu nécessaire une plus grande harmonisation entre les différents États membres de l'Union européenne. Ainsi la directive mère 95/46 a été adoptée afin de concilier le respect des droits des personnes physiques et la liberté de circulation des données. L'architecture de droit dérivé s'est stratifiée par des actes législatifs sur la base juridique de l'article 16 TFUE et, dans certains cas, elle s'est renforcée par une double base juridique[1973] rendant parfois difficile de distinguer la frontière entre les différents « piliers » de l'Union européenne. Cela a été source de contentieux lors de la détermination de la compétence pour l'adoption des actes législatifs[1974]. De plus, sur la base de l'article 16 TFUE, afin de stimuler le marché unique numérique mais aussi pour répondre aux nouvelles menaces pour l'individu, le règlement général sur la protection des données à caractère personnel 2016/679 a été adopté et de nouvelles mesures concernant les communications électroniques sont en cours (à savoir le règlement *e-privacy* sur la vie privée et la communication électronique)[1975]. Cette réforme a concerné également la coopération policière et judiciaire en matière pénale. Ainsi la directive 2016/680 aux fins de prévention, d'enquête, de détection et de poursuite des infractions ou d'exécution des sanctions pénales[1976], la directive sur les données PNR des voyageurs aériens intra-UE[1977] et la directive

1973 Voy. La question sur la double base juridique en matière de coopération policière (article 82 TFUE) dans Partie II Titre I chapitre I.

1974 Voy. Les recours en annulation CJ 30 mai 2006, aff. jointes C-317/04 et C-318/04, Parlement c. Conseil, qui a annulé la décision du Conseil 2004/496/CE du 17 mai 2004 relative à la conclusion d'un accord entre l'UE et les États-Unis concernant le traitement et le transfert de données PNR, et la décision 2004/535/CE de la Commission du 14 mai 2004 relative au niveau de protection « adéquat » des données PNR transférées vers le United States Bureau of Customs and Border Protection ; Voy. aussi CJUE giustizia (Grand Chambre), 10 février 2009, aff. C-301/06, Irlande c. Parlement et Conseil, qui a rejeté le recours en annulation de la directive 2006/24/CE du 15 mars 2006 concernant la collecte de données générales des communications électroniques.

1975 Le projet de règlement relatif à la vie privée et aux communications électroniques (« ePrivacy »), actuellement en cours d'examen dont l'objectif est d'abroger la directive 2002/58 du 12 juillet 2002 et d'harmoniser la législation des États membres en matière de confidentialité des communications électroniques. Voy. v. COM (2017) 10 final, du 10 janvier 2017

1976 Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière. La Déclaration 21, jointe à l'acte final de la Conférence intergouvernementale qui a adopté le traité de Lisbonne, reconnaît la spécificité du secteur de la sécurité. Pour un commentaire voy. DI FRANCESCO MAESA, B*alance between Security and Fundamental Rights Protection : An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR*) , in *EuroJus*, 2016, disponible online.

1977 Directive (UE) 2016/681 du Parlement européen et du Conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière.

sur la lutte contre le terrorisme[1978] ont été adoptées. Dans les relations internationales, l'action de l'Union européenne vise à contribuer à la protection des droits de l'homme dans ce domaine[1979]. Dans ce contexte, la Cour de justice garantit la protection effective de ce droit grâce à un effet d'extraterritorialité, tant vis-à-vis des entreprises opérant au sein du marché unique et ayant leur siège légal hors de l'Union, que des autorités publiques de pays tiers qui collectent des données provenant d'États membres. Le principe permettant les échanges de données à l'international est la protection « adéquate » assurée par les ordres juridiques des États tiers. Il a été illustré que le processus d'intégration européenne a permis au droit à la protection des données personnelles de se développer et de s'affirmer comme un droit fondamental. Toutefois, neuf ans après l'entrée en vigueur du traité de Lisbonne reconnaissant à l'Union une véritable compétence en matière de droit à la protection des données personnelles (art. 16 TFUE), tant dans le champ couvert par l'ex-premier pilier que dans le champ de l'ex-troisième pilier, son déploiement reste incomplet et insuffisant dans le cadre de l'ELSJ. De plus, si des avancées ont été réalisées dans le cadre de la coopération internationale, les accords avec les États tiers sont le fruit d'un compromis politique. Cependant, à travers le régime et le mode de protection offerts aux données à caractère personnel, nous assistons à l'émergence d'une véritable identité européenne. Ainsi a été montré le caractère politique et économique de la donnée.

L'intégration européenne est suffisamment avancée pour qu'une idée d'identité spécifique puisse se développer progressivement. Le droit à la protection des données personnelles a contribué au développement de cette idée d'identité. En effet l'Union européenne exporte ses valeurs identitaires axés autour des principes sécuritaires, économiques et démocratiques à l'extérieur. La protection des données personnelles est donc un enjeu stratégique pour l'Union européenne. Il ressort de notre étude que la fonction première du régime de protection des données personnelles est la protection de l'individu contre les atteintes des acteurs privés mais également des menaces dérivant de l'État dans la mise en place de systèmes de surveillance. La seconde fonction est instrumentale au développement du marché numérique. La donnée est alors un outil pour garantir la compétitivité économique de l'Union européenne. L'effectivité du droit à la protection des données personnelles dérive seulement en partie de son inscription dans le droit primaire de l'Union européenne, elle dépend surtout dans sa mise en œuvre de la jurisprudence de la Cour de justice et des acteurs quasi-juridictionnels dans chaque État membre. Il a été souligné la nature de droit fondamental et les restrictions dont le droit à la protection des données personnelles peut faire l'objet. Ainsi ce droit est susceptible d'être restreint lorsqu'il entre en conflit avec d'autres droits et intérêts individuel ou des limitations dérivant de l'intérêt général. Néanmoins, ces restrictions doivent respecter les conditions formelles de prévisibilité et matérielles de proportionnalité. Malgré les limitations et la dimension internationale de l'Internet et des échanges des données, le droit à la protection des

1978 Voy. La Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil. Pour un commentaire voy. C.C. MURPHY, *The draft EU Directive on Combating Terrorism: Much Ado About What ?*, in *EU Law Analysis*, disponible online; G. DE MINICO, *La risposta europea al terrorismo del tempo ordinario: il lawmaker e il giudice* , in *Osservatorio sulle fonti*, 2017, n. 2, disponible online.

1979 Voy. L'article 3 §5 TUE: « Dans les relations internationales, l'Union affirme et promeut ses valeurs et ses intérêts, contribuant à la protection de ses citoyens ». Pour un commentaire voy. E. SCISO, C. MORVIDUCCI, R. BARATTA, *I valori dell'Unione Europea e l'azione esterna*, Torino, 2016, p. 240.

données à caractère personnel est susceptible d'offrir un renforcement des droits de l'individu puisque l'Union européenne a placé la protection des données au cœur des valeurs de son ordre juridique contribuant ainsi à forger son identité constitutionnelle. Ainsi les droits fondamentaux au-delà de leur fonction de protection des individus exercent traditionnellement une fonction de structuration ou fonction identitaire en ce qu'ils traduisent les équilibres essentiels et fondateurs d'un système [1980] . En effet les droits fondamentaux sont l'expression d'une communauté de valeurs. Dans le domaine de la protection des données personnelles, le rôle de « gardienne constitutionnelle » de la Cour de justice semble être central et stratégique, non seulement à l'échelle européenne, mais à l'échelle mondiale. La reconnaissance de la Charte des droits fondamentaux en tant que source de droit primaire a contribué de manière décisive aux derniers développements de sa jurisprudence en la matière. Il nous semble que le droit fondamental à la protection des données personnelles, en tant que droit transversal touchant différents domaines, peut orienter la politique (interne et externe) de l'Union et peut constituer un vecteur de l'identité de l'Union. La reconnaissance de la Charte des droits fondamentaux en tant que source de droit primaire et l'inscription d'un article spécifique à la protection des données personnelles (art. 8 de la Charte) a contribué de manière décisive aux derniers développements de la jurisprudence en la matière, renforçant le rôle de « gardienne constitutionnelle » de la Cour de justice. L'activité quasi-juridictionnel et de régulation des autorités de contrôle nationales est indispensable pour faire face au nouveau paysage technologique [1981] . En effet les objets connectés (IoT) et les capteurs présents dans l'environnement des utilisateurs sont un risque pour les données personnelles. Ainsi par exemple les détecteurs de fumée *Nest* possèdent un capteur de présence qui permet d'allumer une veilleuse lors du passage nocturne sous le détecteur. Cette fonction « annexe » pourrait avoir des conséquences importantes : l'heure et le nombre de passages sous ce capteur pourraient être révélateurs de troubles du comportement ou de pathologies. Ces données une fois soumises à des algorithmes d'analyse du risque, pourraient modifier le profil assurantiel d'un utilisateur [1982] . D'autres capteurs comme *Linky* installés dans les appartements pour l'analyse de la consommation électrique pourraient aussi être utilisés pour effectuer un profilage ethnique ou religieux des usagers [1983] . Ainsi, l'absence ou la diminution de consommation électrique à des périodes précises permettent de déduire si l'utilisateur modifie sa consommation par exemple lors du mois du ramadan ou le vendredi soir et le samedi pour les personnes qui observent le shabbat. D'autres risques dérivent des automobiles connectées

1980 E. DUBOUT et S. TOUZÉ, « La fonction des droits fondamentaux dans les rapports entre ordres et systèmes juridiques », in E. DUBOUT et S. TOUZÉ, *Les droits fondamentaux: charnières entre ordres et systèmes juridiques* , Pedone, 2010, pp. 11-35, sp. pp. 20-21 ; M. DELMAS-MARTY, *Avant-propos, Les droits fondamentaux: charnières entre ordres et systèmes juridiques*, op. cit., p. 6.

1981 V. MAYER-SCHONBERGER et K. CUKIER, *Big Data. A Revolution That Will Transform How We Live, Work and Think*, London, 2013, p. 171 ss. Concernanr le Big Data voy. CONSULTATIVE COMMITTEE OF THE CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA, « Guidelines on the Protection of Individuals with Regard to the Processing of Personal Data in a World of Big Data, Strasburgo Strasbourg », 23 gennaio 2017.

1982 A. MANTELERO, « Personal data for decisional purposes in the age of analytics: from an individual to a collective dimension of data protection », in *Computer Law and Security Review*, 2016, p. 251 ss.

1983 Voy. B. BENHAMOU, « Données personnelles et objets connectés en Europe perspective technologiques et enjeux de régulation », Rapport 18 avril 2017, Institut Mines Télecom, p. 2 et s.

(radar, sonar, caméras, accéléromètres, thermomètres, détecteurs d'humidité, etc.) coordonnées par un informatique embarqué de plus en plus puissante. Si, dans leur majorité, ces capteurs sont dédiés à l'analyse des paramètres de fonctionnement du véhicule, d'autres sont spécifiquement destinés à analyser les paramètres physiologiques du conducteur ou son style de conduite. Ces capteurs pourraient au-delà de l'évaluation de son niveau de vigilance, devenir une source d'information précieuse, notamment sur la santé du conducteur[1984]. L'analyse de la conduite a donné lieu à des expérimentations par des groupes d'assurance afin de moduler les primes (principe du « *Pay How You Drive* »)[1985]. D'autres enjeux dérivent des évolutions des structures de soins. Selon Éric Topol[1986], le parcours de soins sera alors constitué d'objets médicaux connectés qui éviteront aux patients d'avoir à se rendre à l'hôpital ou dans des laboratoires médicaux et permettront un suivi à distance des paramètres de santé ainsi qu'un développement des mesures de prévention. Les données recueillies par ces objets seront utiles aux professionnels de santé et pourraient être précieuses pour les acteurs de l'assurance. À cet égard, le traitement des données médicales pourrait devenir un enjeu politique et économique majeur à la fois pour les citoyens et pour l'ensemble des acteurs impliqués dans la protection sociale. La sécurité des objets connectés fait désormais partie intégrante de la réflexion sur la protection des données personnelles. En plus d'être une préoccupation majeure pour les citoyens, elle est aussi devenue un enjeu de sécurité nationale pour les États [1987] . Les technologies et les services liés à la sécurité des objets connectés constituent un marché essentiel pour l'ensemble des acteurs des technologies[1988]. Or la sécurité de ces objets reste pour l'instant rudimentaire. De l'absence de mécanismes de chiffrement pour la transmission des données, jusqu'à l'impossibilité d'intégrer des mises à jour de sécurité, la sécurité des objets connectés constitue aujourd'hui l'un des maillons les plus faibles des infrastructures de l'Internet[1989]. A cet égard il est indispensable d'établir une synergie entre régulation et politique industrielle.

Le RGPD introduit ainsi le principe d'une protection des données dès la conception (*Privacy by Design*) et de protection des données par défaut (*Privacy by Default*). Cela signifie que le responsable de traitement doit adopter, en amont, dès qu'il envisage de collecter des données, des mesures destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, la pseudonymisation et l'anonymisation des données.

[1984] D. K. CITRON, F. PASQUALE, « The Scored Society: Due Process For Automated Predictions », in *Washington Law Review*, 2014, p. 89 et s.

1985 Il est à noter que jusqu'ici ces expérimentations ont souvent été jugées trop intrusives par les assurés potentiels Assurances auto: êtes-vous prêt à tout dévoiler pour payer moins cher ? (*L'Express*, 2 février 2016).

1986 Eric Topol est considéré comme le spécialiste américain des technologies de la santé. Voy E. TOPOL, « On the Future of Medicine », *Wall Street Journal*, 7 juillet 2014.

1987 Voy. « The CIA Fears the Internet of Things », *Defense One*, 24 juillet 2014, disponible à l'adresse : https://www.defenseone.com/technology/2014/07/cia-fears-internet-things/89660/

[1988] L. FLORIDI, *The 4th revolution: how the infosphere is reshaping human reality*, Oxford, 2014, p. 96.

1989 Voy. « Computer Viruses Are "Rampant" on Medical Devices in Hospitals », *MIT Technology Review*, 17 octobre 2012, disponible à l'adresse : https://www.technologyreview.com/s/429616/computer-viruses-are-rampant-on-medical-devices-in-hospitals/

De plus, parmi les nouveautés adoptées par le RGDP, figurent également l'encouragement à la mise en place de codes de conduite et « des mécanismes de certification en matière de protection des données ainsi que de labels et de marques ». À l'instar des étiquettes-énergie qui résument les performances énergétiques et permettent de guider le choix des consommateurs, une certification de conformité basée sur le RGPD ou un label de confiance (*Trusted IoT*) pour les objets connectés développés par les acteurs du secteur à destination du grand public pourraient être créés afin d'assurer la transparence sur les différents niveaux de confidentialité et de sécurité.

À terme, la sécurité de nos sociétés pourrait davantage reposer sur le renforcement des technologies de protection des données et donc sur une plus grande « opacité » des données. Pour le juriste Lawrence Lessig[1990], les prochaines étapes de la régulation de la vie privée passeront davantage par le développement de nouvelles générations de technologies de chiffrement des données que par les seules mesures d'encadrement de l'utilisation des données comme les technologies de chiffrement de la *Blockchain*[1991]. Cependant, comme l'a démontré le récent piratage de la plateforme DAO (*Decentralized Autonomous Organization*) qui utilise la crypto-monnaie Ether[1992], les technologies de la *Blockchain* pourraient être remises en cause. Ce piratage est intervenu au cœur de la technologie de sécurité du projet et rappelle la fragilité d'un dispositif économique dont le « code » est largement accessible. Ce piratage a aussi remis en lumière les origines des algorithmes de sécurité de la *Blockchain* qui ont été conçus par la NSA.

Ce que Paul Nemitz, le directeur du département juridique de la Commission européenne évoque en ces termes : « Il est probable qu'à l'avenir les utilisateurs du monde numérique demanderont une meilleure protection de la vie privée et des données personnelles. Comme cela a été le cas avec le mouvement pour l'écologie, qui a commencé en Europe et qui a conduit l'industrie européenne à des gains de compétitivité, mais qui s'est heurté au début des années soixante-dix et quatre-vingt à des résistances, il est très possible qu'avec la protection des données nous soyons confrontés à un mouvement similaire qui partira d'Europe… »[1993].

Comme l'a démontré l'affaire Snowden et plus récemment la remise en cause du *Safe Harbor*, les revendications européennes en matière de protection de la vie privée et de lutte contre la surveillance de masse n'auront de traductions que si des technologies alternatives peuvent être mises en place par les acteurs européens[1994]. Cependant, la difficulté des start-ups françaises et européennes à trouver des financements explique la tentation du rachat par des sociétés

---

1990 Lawrence Lessig, « Technology Will Create New Models for Privacy Regulation », *Wall Street Journal*, 30/12/15 https://blogs.wsj.com/cio/2015/12/30/lawrence-lessig-how-technology-policy-will-evolve/.

1991 F. PASQUALE, *The Black Box Society. The Secret Algorithms That Control Money and Information* , Cambridge, MA, 2015, p. 143 et s.

1992 Voy. « A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency », *New York Times*, 17 juin 2016 : http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-fromexperimental-cybercurrency-project.html.

1993 Voy. V. Mayer-Schonberger, *Delete,* Princeton University Press, octobre 2009.

1994 Voy.B. BENHAMOU, « Les nouveaux défis politiques et économiques de l'Internet », *Les Cahiers de la Documentation Française*, mars 2015, disponible à l'adresse : http://www.ladocumentationfrancaise.fr/var/storage/libris/3303330403921/3303330403921_EX.pd.

américaines ou asiatiques. Ainsi il serait envisageable de conclure un traité transatlantique sur la gouvernance de l'Internet des objets et de la cybersécurité puisque les actions menées à l'échelle européenne en matière de sécurité numérique n'auront d'impact que si elles s'inscrivent dans une stratégie internationale d'élévation des niveaux de sécurité des infrastructures cruciales. Cependant, le premier accord international de limitation du cyberarmement a été conclu entre les États-Unis et la Chine, sans qu'à aucun moment l'Europe n'ait été associée à ces discussions[1995].

Dans un cadre juridique en pleine mutation et des défis technologiques de taille, le rôle de la Cour de justice comme gardienne constitutionnelle des valeurs de l'Union européenne sera crucial.

1995 D. E. SANGER, « U.S. and China Seek Arms Deal for Cyberspace », *New York Times*, 20 septembre 2015. https://www.nytimes.com/2015/09/20/world/asia/us-and-china-seek-arms-deal-for-cyberspace.html.
Il est à noter que des propositions similaires commencent à être évoquées à l'échelle des seuls États-Unis et pourraient être élargies dans le cadre d'un accord transatlantique. Voy.sur ce point : « How to Save the Net: A CDC for Cybercrime », *Wired*, 19 août 2014 : http://www.wired.com/2014/08/save-the-net-peter-singer/

BIBLIOGRAPHIE

Ouvrages généraux et manuels

P. ALSTON, M. BUSTELO, J. HEENAM, *L'Union Européenne et les Droits de l'Homme*, Bruylant Bruxelles, 2001, p. 983, spéc.p.97.

H. ARENDT, *The Human condition*, Chicago University of Chicago Press, 1998, p. 370, spéc. p. 38.

S. BARTOLE, P. DE SENA, V. ZAGREBELSKI (a cura di), *Commentario breve alla Convenzione europea dei diritti dell'uomo*, Padova, 2012, p. 950, spéc. 297.

E. BASSOLI, *La nuova Privacy GDPR dopo il Dlgs. 10 agosto 2018, n° 101*, Dike Giuridica, 2018, p.248.

M. BEHAR-TOUCHAIS, *L'effectivité du droit face à la puissance des géants de l'Internet*, IRJS éd., 2015, p. 394, spéc. p. 117.

P. BELLANGER, *La souveraineté numérique*, Stock, coll. Essais – Documents, 2014, p. 264, spéc. p. 84-87.

W. BENEDEK, M.C. KETTEMANN, *Liberté d'expression et Internet*, Strasbourg, Conseil de l'Europe, 2014, p. 192, spéc.p.12.

A. BEVERE, A. CERRI, *Il diritto di informazione e i diritti della persona: il conflitto della libertà di pensiero con l'onore, la riservatezza, l'identità personale*, Milano, Giuffrè, 2006, p. 308, spéc. p. 45 et ss.

C. M. BIANCA (a cura di), *La protezione dei dati personali: commentario al D.lgs. 30 giugno 2003, n. 196 ; Codice della privacy con l'onore, la riservatezza, l'identità personale*, Padova, 2007, vol. 2, Milano, 2006, p. 2200, spéc. p. 87.

Y. BISMUTH, *Droit de l'informatique*, L'Harmattan, 2017, p. 436, spéc. p.67.

C. BLENGINO, *La condivisione della musica sulle reti peer-to-peer*, Sociologia del diritto, 2011, p. 106, spéc. p. 34.

C. BLUMANN, L. DUBOUIS, *Droit institutionnel de l'Union européenne*, 5e éd., LexisNexis, coll. Manuel, 2013, p. 863, spéc. p. 115.

M. BOCCHIOLA, *Privacy. Filosofia e politica di un concetto inesistente*, Roma, Passim, 2014, p. 165, spéc. p. 57-69.

F. BOEHM, *Information sharing and data protection in the Area of freedom, security and justice: towards harmonised data protection principles for information exchange at EU–level*, Berlin, 2012, p. 427, spéc. p. 175-319.

C. BONNET, *Repenser les rapports entre ordres juridiques*, Lextenso, Paris, 2013, p. 23.

L.BOLOGNINI, *Follia artificiale*, Rubbettino Editore, 2018, p.100.

G. BRAIBANT, *La Charte des droits fondamentaux de l'Union européenne, témoignage et commentaires*, Essais, 2001, p. 336, spéc. p.111-114

T. BRAÜTINGAM, S. MIETTINEN, *Data Protection, Privacya European Regulation in the Digital Age*, Helsinki, December 2016, p. 262, spéc. p. 229-240.

L. BURGORGUE-LARSEN, A. LEVADE, F. PICOD (dir.), *Traité établissant une Constitution pour l'Europe. Commentaire article par article. Partie II La Charte des droits fondamentaux de l'Union*, Bruxelles, Bruylant, p. 658, spéc. p. 668-670.

E. DE BUSSER, *Data protection in EU and US criminal cooperation: a substantive law approach to the EU*, Antwerpen, Maklu Publisher, 2009, p. 473, spéc. p. 127-213.

L. BYGRAVE, *Data Privacy Law: an international perspective*, Oxford, 2014, p. 272, spéc. p. 196-198.

L. BYGRAVE, *Data Protection Law: Approaching Its Rationale, Logic and Limits*, Kluwer Law International, 2002, p. 441, sp. p. 93-165.

F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali: temi e problemi*, Milano, 2004, p. 656, spéc. p 139-164.

M. CARTABIA, *Principi inviolabili e integrazione europea*, Milano, 1995 p.1274, spéc. p.34.

G. CASSANO, *Diritto dell'Internet: il sistema di tutele della persona*, Milano, 2005, p. 400, spéc. p.18.

G. CASSANO, G. VACIAGO, G. SCORZA, *Diritto dell'Internet. Manuale operativo, capitolo I*, Cedam, 2012, p. 908, spéc. p. 222-243.

C. CASTETS-RENARD, *Droit de l'Internet : droit français et européen*, Montchrestien, 3e éd., 2012, p.492, spéc. p.1-93.

C. CASTETS-RENARD (dir.), *Quelle protection des données personnelles en Europe*, Bruxelles, Larcier, 2015, p. 171, spéc. p. 155-165.

F.H. CATE, C. KUNER, O. LYNSKEY, C. MILLARD et D.J.B. SVANTESSON, *When two worlds collide: the interface between competition law and data protection*, International Data Privacy Law, 2014, p. 248, spéc. p. 207-218.

S. COMELLINI, Il Responsabile della protezione dei Dati (Data protection Officer-DPO), Maggioli, 2018, p. 64.

G. CORNU (dir.), *Vocabulaire juridique*, 10e éd., PUF, coll. Quadrige, 2018, p. 1099.

L. COUDRAY, *La protection des données personnelles dans l'Union européenne : naissance et consécration d'un droit fondamental*, Sarrebruck, 2010, p. 700, spéc. p. 327.

DEBET, J. MASSOT, N. METALLINOS, *Informatique et Libertés. La protection des données à caractère personnel en droit français et européen*, Paris, Lextenso, 2015, p. 1296.

D.DERO-BUGNY, *Les rapports entre la Cour de justice de l'Union européenne et la Cour européenne des droits de l'homme*, Bruxelles, Bruylant, 2015, p. 232, spéc. p. 46-55.

G. DESGENS-PASANAU, *Informatique et Libertés : Enjeux, risques, solutions et outils de gestion*, Lamy Conformité, 2013, p. 292, spéc. p. 83-92.

G. DESGENS-PASANAU et E. FREYSSINET, *L'identité à l'ère du numérique*, Presaje, Broché, 2017, p. 170, spéc. p. 52-63.

G. DESGENS-PASANOU, *Le correspondant Informatique et libertés*, Lexis Nexis, 2013, p. 374, spéc. p. 82.

G. DI FEDERICO (ed.), *The EU Charter of Fundamental Rights, From Declaration to Binding Instrument*, Dordrecht, 2011, p. 107, spéc. p.55-75.

M. DI STEFANO (a cura di), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, p. 288, spéc. p.127.

C. DOUTRELEPONT, F. DUBUISSON, A. STROWEL, *Le téléchargement d'œuvres sur Internet : perspectives en droits belge, français, européen et international*, Bruxelles, Lancier, 2012, p.431, spéc. p.112.

W.D. EBERWEINet Y. SCHEMEIL, (éds.), *Normer le monde : énonciation et réception des normes internationales*, L'Harmattan, 2009, p. 308, spéc. p 280.

G. ERCHOVE et A. WEYEMBERGH *Sécurité et justice : enjeu de la politique extérieure de l'Union européenne*, Bruxelles, Institut d'É tudes Européennes, É ditions de l'Université de Bruxelles, 2003, p. 325, spéc. p. 195.

J. EYNARD, *Les données personnelles, quelle définition pour un régime de protection efficace* ?, Michalon, 2013, p. 440, spéc. p.193-335.

E. FALLETTI, *I diritti fondamentali su Internet. Libertà d'espressione, privacy e copyright*, Exeo, Padova, 2011, p. 138, spéc. p. 89-93.

L. FAVOREU (dir.), *Droit des libertés fondamentales*, 6 éd., *Dalloz, coll. Précis*, 2012, p. 744, spéc. p.720.

L. FAVREAU, *La charte des droits fondamentaux de l'union européenne après le traité de Lisbonne*, Bruylant 2010, p.384, spéc. p.185-210.

G. FINOCCHIARO, *Il nuovo Regolamento europeo sulla protezione dei dati*, Zanichelli, 2017, p. 776, spéc. p. 115-160.

G. FIORIGLIO, *Il diritto alla privacy: nuove frontiere nell'era di Internet*, Bologna, 2008, p. 256, spéc. p. 31-46.

L. FLORIDI, *The 4th revolution: how the infosphere is reshaping human reality*, Oxford, 2014, p. 272, spéc. p. 96.

M. FOUCAULT, *Surveiller et punir*, Gallimard, Paris, 1975, p. 360

J.-C. GALLOUX, *De la nature juridique du matériel génétique ou la réification du corps humain et du vivant*, RRJ, 1989, n° 3, p. 156, spéc. p. 121.

M. GAMBINO, A. STAZI, *Diritto dell'informatica e della comunicazione*, Torino, Giappichelli, 2012, p.212, spéc. p. 84.

G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Berlin, 2014, p. 162, spéc.p. 111-162.

S. GORLA, F. FERRARA, F. FORNASERO, G. MONTINI, M. QUADRELLI, *Quaderno del Data Protection Officer*, Maggioli, 2018, p.320.

C. GREWE, H. RUIZ-FABRI, *Droits constitutionnels européens*, PUF, coll. Droit fondamental, 1995, p. 661, spéc. p. 227-228.

A. GROSJEAN, *Enjeux européens et mondiaux de la protection des données*, Bruxelles, Larcier, 2015, p.468, spéc. p.187.

E. GUILD, *The area of freedom, security and justice ten years on: successes and future challenges under the Stockholm Programme*, Brussels, CEPS, 2010, p. 112, spéc. p. 37.

D. GUTMANN, *Le sentiment d'identité. Etude de droit des personnes et de la famille*, Paris, 2000, p. 1042, spéc. p. 974-976.

S. HANNET-UACHEZ, D. HOMAN, *Droits de l'Homme et libertés fondamentales*, Dalloz, 2012, p. 838, spéc. p.168.

H. HIJMANS, *The European Union as Guardian of Internet Privacy. The Story of Art 16 TFEU*, Heidelberg, 2016, p 261, spéc. p. 185-261.

E. KOSTA, *Consent in European data protection law*, Leiden, 2013, p. 441, spéc. p 153-162.

M. LEVINET, *Droits et libertés fondamentaux*, PUF, coll. Que sais-je ?, 2010, p. 126, spéc. p. 48-56.

C. LUCIONI, *Tutela dei dati personali del cittadino dell'Unione e giudizio di non discriminazione in base alla nazionalità*, in Diritto pubblico comparato ed europeo 2009, p.575, spéc. p. 178.

F. MANCINI et V. DI BUCCI, *Le développement des droits fondamentaux en tant que partie du droit communautaire*, RCADE, 1990, vol I-1 p. 438, spéc. 27-38.

N. MARTIAL-BRANZ, J. ROCHEDELD, E. GATTONE, *Quel avenir pour la protection des données à caractère personnel en Europe ? Les enjeux de l'élaboration chaotique du règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation*, Dalloz, 2013, p. 2788.

A. MATHIEU, M. VERPEAUX, *Contentieux constitutionnel des droits fondamentaux*, LGDJ, coll. Manuel, 2002, p.808, spéc. p. 11-12.

A. MATTELARD, *La globalisation de la surveillance : Aux origines de l'ordre sécuritaire*, La découverte Poche, coll. Essai n° 290, 2008, p. 260, spéc. p 114.

F. MATTIATA, *Traitement des données personnelles. Le guide juridique. La loi Informatique et libertés et la CNIL*, Jurisprudences, Eyrolles 2013, p. 18 et ss.

M. MEZZANOTTE, *Il diritto all'oblio. Contributo allo studio della privacy storica*, Napoli, 2009, p. 188, spéc. p. 28.

C.L MONTESQUIEU, *De l'esprit des lois*, Livre XI, Chapitre VI, « De la Constitution d'Angleterre », GF Flammarion, Paris, 1979, p. 301.

P. MUNZI, *La technique de proportionnalité et le juge de la Convention européenne des droits de l'homme. Essai sur un instrument nécessaire dans une société démocratique*, Aix-en-Provence, PUAM, 2005, p. 734, spéc. p. 336.

G. NOLTE, *European and US Constitutionalism*, Cambridge 2005, p. 436, spéc. p. 53.

G. ORWELL, *Big Brother1984*, Gallimard, 1950, p. 384

R.E. PAPADOPOULOU, *Principes Généraux du droit et droit communautaire, Origines et concrétisation*, Bruxelles, Bruylant, 1996, spéc.p. 137-165.

G.M. PELLOS, *Il Data Protection Officer. Il Responsabile dei dati personali dopo il D.Lgs. 10 agosto 2018, n°101,* Dike Giuridiche, 2018, spéc. p. 30-48.

L.E. PETITTI, E. DECAUX, P.H. IMBERT, *La Convention européenne des Droits de l'Homme, Commentaire article par article,* Economica 1999, p. 324, spéc. p. 97-111.

A. POUILLZ, J. ROCHE, *Libertés publiques et droits de l'homme*, Dalloz, 2002, p. 237, spéc. p.67.

M. V. PÉREZ ASINARI et P. PALAZZI, *Défis du droit à la protection de la vie privée, perspective du droit européen et nord-américain*, Bruylant 2008, p. 187, spéc. p. 25-70.

P. PERRI, *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Milano, 2007, p. 156, spéc. p. 84.

L.E. PETITTI, E. DECAUX, P.H. IMBERT, *La Convention européenne des Droits de l'Homme, Commentaire article par article*, Economica, 1999, p. 1230, spéc. p. 305.

F. PIZZETTI, *Il caso del diritto all'oblio*, Giappichelli, Torino 2013, p. 230, spéc. p. 27.

O. POLLICINO et M. BASSINI, *La Carta dei dritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo*, Roma3 Press, 2016, p. 373, spéc. p. 73.

R. RAZZANTE, *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2008, p. 550, spéc. p. 43.

M.-J REDOR, *La vocation de l'Union européenne à protéger les droits fondamentaux*, Leclerc, 1999, spéc. p. 171-200.

T. RENOUX, *Protection des libertés et droits fondamentaux*, La documentation française, 2011,p. 400, spéc.p. 182.

J.F. RENUCCI, *Droit européen des droits de l'homme*, LGDJ, 2017, p. 560, spéc. p. 102 et s.

G. RESTA, *Dignita, persone, mercati*, Torino, 2014, p. 153 ; *Libera circolazione e protezione dei dati personali, t. I e II*, a cura di R. PANETTA, con prefazione di S. RODOTA, Milano, 2006, passim, p. 208, spéc. p. 126.
G.M. RICCIO, G. SCORZA, E. BELISARIO, *GDPR e normativa Privacy*, IPSOA, 2018, p. 380.

J. RIDEAU, *La Coexistence des systèmes de protection des droits fondamentaux dans les États membres de la communauté européenne*, Economica 1991, p. 170, spéc. p.11- 86.

J. ROBERT, J. DUFFAR, *Droits de l'homme et libertés fondamentales*, Montchrestien, 2009 p. 908, spéc. p.174.

F. ROCHELANDET, *Economie des données personnelles et de la vie privée*, La découverte, coll. Repères, 2010, p.125, spéc. p. 46 et s.

S. RODOTÀ, *Tecnologie e diritti*, Bologna, 1995, p. 416, spéc. p.102.

M. RUSSO et P.M. QUADRANI, *La convenzione europea dei diritti dell'uomo e la giurisprudenza della Corte di Strasburgo*, Milano, 2006, p. 262, spéc. p. 89 et s.

S. RUSSO, R. SCAVIZZI, *Manuale di diritto comunitario dell'infomatica*, Giuffrè, Milano, 2010, p. 228, spéc. p. 118.

G. SANTANIELLO, *La protezione dei dati personali*, Padova, 2005, p. 73 et s.

C. SCHMITT, *Théologie politique*, Gallimard, Paris, 1988, p. 204, spéc. p. 22 et s.

O. DE SCHUTTER, *Traité établissant une constitution pour l'Europe, Commentaire article par article*, Bruylant, 2010, p. 178.

E. SCISO, C. MORVIDUCC, R. BARATTA, *I valori dell'Unione Europea e l'azione esterna*, Giappichelli Torino, 2016, p. 240, spéc. p. 37.

S. SICA, V. ZENO-ZENCOVICH (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2009, p. 240, spéc. p. 83.

F. SOUDRE, J-P. MARGUNAUD, J. ANDRIANTIMBAZOVINA, A. GUTTEINOIRE, M. LEVINET, G. GONZALES, *Les grands arrêts de la Cour européenne des droits de l'homme*, Thémis droit, PUF, 2015, p. 948, spéc. p.124

F. SUDRE, *Droit européen et international des droits de l'homme*, PUF, 2016, p. 1006, spéc. p.129.

F. SUDRE, *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'homme*, Némesis-Bruylant, « Droit et justice » n°63, 2006, p. 412, spéc. p.336.

F. SUDRE, R. TINIERE, *Droit communautaire des droits fondamentaux*, Nemesis, 2012, p. 478, spéc. p. 124.

G. TESAURO, *Diritto Comunitario*, Padova, Cedam, 2003, p. 928, spéc. p.130.

B. TEYSSIÉ, *Droit des personnes*, LexisNexis, 2017, p. 667, spéc. p. 187.

T. M. UBERTAZZI, *Il diritto alla privacy: natura e funzione giuridiche*, Padova, 2004, p. 210, spéc.p. 46.

J. VERGES, *Droits fondamentaux de la personne et principes généraux du droit communautaire*, Dalloz 1991, p. 617, spéc. p.513.

P. WIATER, *Le dialogue interculturel dans le système européen de protection des droits de l'homme*, Livre blanc-volume 1, p. 123, spéc. p. 65.

R. ZACCARIA, *Diritto dell'informazione e della comunicazione*, 7 ed., Padova, 2010, p. 688, spéc.p. 68.

G. ZAGREBELSKY G., « Objet et portée de la protection des droits fondamentaux. Cour constitutionnelle italienne », *RIDC*, 1981, vol. 33, n° 2, p. 742, spéc. p. 511.

Z. ZENCOVICH, G. RESTA, *La protezione transnazionale dei dati personali dai "safe harbour principles" al "privacy shield"*, Roma Tre-press, 2016, p. 374, spéc. p. 137.

E. ZOLLER, *Grands arrêts de la Cour suprême des États-Unis*, Paris, PUF, coll. Droit fondamental, 2000, p. 694, spéc. p. 292.

Articles et contributions

B. ACKERMAN, « The Emergency Constitution », *The Yale Law Journal*, 2004, 1029 et s.

A. ADAM, « L'échange de données à caractère personnel entre l'Union européenne et les États Unis. Entre souci de protection et volonté de coopération », *Revue trimestrielle de droit européen*, 2006 p.423 et s.

L. ADAMOVICH, « Marge d'appréciation du législateur et principe de proportionnalité dans l'application des restrictions prévues par la loi au regard de la CEDH », RTDH, 1991, N° 7, p. 291 et s.

M. ALINCAI, « Espoirs et inquiétudes autour de la révision du cadre juridique général de l'Union européenne sur la protection des données à caractère personnel », in *Revue de l'Union européenne*, 2014, p. 170 et s.

D. ALONSO BLAS, « Ensuring effective data protection in the field of police and judicial activities : some considerations to achieve security, justice and freedom », in *ERA-Forum: scripta iuris europaei*, 2010, p. 233 et s.

P. ALSTON, J.-H.H. WEILER, « Vers une politique des droits de l'homme authentique et cohérente pour l'Union européenne », in P. ALSTON (sous la dir.), *L'Union européenne et les droits de l'homme*, Bruxelles, *Bruylant*, 2001, p. 7 et s.

J. ANDRIANTSIMBAZOVINA, « Harmonie ou disharmonie de la protection des droits de l'homme en Europe : quelques considérations sur la jurisprudence de la Cour européenne des droits de l'homme depuis 2005 », *C.D.E.*, 2006/5-6, p. 733 et s.

J. ANDRIANTSIMBAZOVINA, « La Cour de Strasbourg, gardienne des droits de l'homme dans l'Union européenne ? Remarques autour de l'arrêt de Grande chambre de la Cour européenne des droits de l'homme, du 30 juin 2005, Bosphorus », *R.F.D.A.*, 2006 p. 560 et s.

L. AZOULAI, « Le rôle constitutionnel de la Cour de justice des Communautés européennes tel qu'il se dégage de sa jurisprudence », *RTDE*, janvier-mars 2008, pp. 29 et s.

T. AULETTA, « Diritto alla riservatezza e « droit à l'oubli», in ALPA-BESSONE-BONESCHI-CAIAZZA (a cura di), *L'informazione e i diritti della persona*, Napoli, 1983, p. 127 et s.

M.-L BASILIEN-GAINCHE, « Une prohibition européenne claire de la surveillance électronique de masse », in *La Revue des droits de l'homme*, Actualités Droits-Libertés, mis en ligne le 14 mai 2014, consulté le 6 avril 2017, disponible à l'adresse: http://revdh.revues.org/746

V.-L. BENABOU, « L'extension du domaine de la donnée », dossier « Big data : quelle protection pour les données personnelles », *Legicom*, n° 59, 2017/2, p. 3 et s.

B. BENHAMOU, « Données personnelles et objets connectés en Europe perspective technologiques et enjeux de régulation », Rapport 18 avril 2017, Institut Mines Télécom, p. 2 et s.

D. BENJAMIN, « Arrêt Satamedia : la (re)diffusion d'informations publiques dans les médias et les exigences de la protection des données », in *Revue européenne de droit de la consommation*, 2009, p. 560 et s.

F. BENOIT ROHMER, « Note, A propos de l'arrêt Bosphorus Air Lines : L'adhésion contrainte de l'Union à la Convention », *R.T.D.H.*, 2005, p. 584 et s.

A. BENSOUSSAN, « Le droit à l'oubli, un droit de l'homme numérique », *Le Figaro*, 21 juillet 2014, disponible à l'adresse : http://blog.lefigaro.fr/bensoussan/2014/07/le-droit-a-loubli-un-droit-de-lhomme-numerique.html

F. BESTAGNO, « Validità e interpretazione degli atti dell'UE alla luce della Carta: conferme e sviluppi nella giurisprudenza della Corte in tema di dati personali», in *Diritto dell'Unione europea*, 2015, p. 21 et s.

F. BIGNAMI, G. RESTA, « Transatlantic Privacy Regulation: Conflict and Cooperation», *Law and Contemporary Problems*, 2015, p.231 et s.

D. BIGO, « National Programs for Mass Surveillance of Personal Data in EU Member States and Their Compatibility with EU Law », 2013 disponible à l'adresse : http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf.

D. BIGO, R.B.J. WALKER, « Le régime du contre-terrorisme global », in D. BIGO, D. BONELLI, L. DELTOMBE D., (dir.), *Au nom du 11 septembre... Les démocraties à l'épreuve de l'antiterrorisme*, Paris, La Découverte, 2008, p. 13 et s.

F. BIGNAMI, G. RESTA, «Transatlantic Privacy Regulation: Conflict and Cooperation », in *LCP*, 2015, p.101 et s.

F. BIGNAMI, «The US Legal System on Data Protection in the Field of Law Enforcement. Safeguards, Rights and Remedies for EU Citizens », S*tudy for the LIBE Committee*, PE 519.215, May 2015, disponible à l'adresse: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/519215/IPOL_STU%282015%29519215_EN.pdf

C. BLUMANN, « Les compétences de l'Union européenne en matière de Droits de l'homme », *R.A.E. – L.E.A.*, 2006/1, p. 14 et s.

F. BOEHM, « Tit for tat: Europe's revenge for the Canadian and US-American PNR systems? The envisaged European model of analyzing flight passenger data », in *ERA-Forum : scripta iuris europaei*, 2010, p. 251 et s.

L. BOLOGNINI, « Una sentenza politica che non stupisce », in Formiche, novembre 2015, p. 50 et s.

A. BRADFORD, « The Brussels Effect », 107 N.W. U. L. Rev. 1, 2012, p. 22 et s.

G. BRAIBANT, « La protection des droits individuels au regard du développement de l'informatique », *RIDC*, 1971, p. 793 et s.

P. BREYER, « Telecommunications *Data Retention* and Human Rights : The Compatibility of Blanket Traffic *Data Retention* with the ECHR », in *European Law Journal*, Vol. 11, No. 3. (May 2005), p. 365 et s.

E. BRIBOSIA, « In search of a balance between the right to equality and other fundamental rights », 2010 p. 14 et s. disponible à l'adresse : http://www.migpolgroup.com/portfolio/in-search-of-a-balance-between-the-right-to-equality-and-other-fundamental-rights/

I. BROWN, « Keeping our secrets ? : Designing Internet technologies for the public good », in *European Human Rights Law Review*, 2014, n. 4, p. 369 et s.

L. A. BYGRAVE, *Data privacy law: an international perspective*, Oxford, 2014, p.54 et s.

L. BURGORGUE-LARSEN, « La force de l'évocation ou le fabuleux destin de la Charte des droits fondamentaux de l'Union européenne », in *Mélanges en l'honneur de Pierre Pactet*, Paris, Dalloz, 2003, p. 77 et s.

L. BURGORGUE-LARSEN, « L'appréhension constitutionnelle de la vie privée en Europe », in *Le droit au respect de la vie privée au sens de la Convention européenne des droits de l'hommes*, dir. F. Sudre, Bruylant, 2005, p. 69 et s.

H. BURKERT, « Dualities of Privacy – An Introduction to "Personal Data Protection and Fundamental Rights" », *in* A. PALAZZI, M.-V. PEREZ ASINARI (dir.), *Défis du droit à la protection de la vie privée. Perspectives du droit européen nord-américain*, Bruxelles, Bruylant, coll. Cahiers du CRID n°31, 2008, p. 13 et s.

G. CAGGIANO, « La Corte di giustizia consolida il ruolo costituzionale nella materia dei dati personali », *Studi sull'integrazione europea*, 2018, fasc.1., p. 3 et s.

G. CAGGIANO, « L'interpretazione del contesto delle attività di stabilimento' dei responsabili del trattamento dei dati personali », in *Dir. Inf*., 2014, p. 616 et s.

G. CAGGIANO, « La regolazione delle reti delle comunicazioni e dell'energia nel diritto dell'Unione europea », in *Studi sull'integrazione europea*, 2011, p. 41 et s.

G. CAGGIANO, « La riforma del regime delle radiofrequenze nel quadro delle comunicazioni elettroniche », in *Studi sull'integrazione europea*, 2010, p.79 et s.

V. CAIANIELLO, « Il difficile equilibrio delle autorità indipendenti », in *Il diritto dell'economia*, 1998, p. 258 et s.

I. CAMERON, « A Court of Justice Balancing data protection and law enforcement needs: Tele2 Sverige and Watson », in *Common Market Law Review*, 2017, p.1467 et s.

S. CARLSON, « Protection of proprietary data : why published data should not be excluded from protection under Article 21 of Regulation 1924/2006 », in *European Food and Feed Law Review*, 2010, p. 166 et s.

S. CARRERA, E. GUILD, « Safe Harbour or into the Storm ? EU-US Data Transfers after the Schrems Judgment », in *CEPS Liberty and Security in Europe Papers*, November 2015 disponible online

S. CARRERA, M. DE SOMER, B. PETKOVA, « The Court of Justice of the European Union as a Fundamental Rights Tribunal Challenges for the Effective Delivery of Fundamental Rights in the Area of Freedom, Security and Justice », *CEPS*, paper 49, August 2012, p. 3 et s.

C. CASTETS RENARD, « Google et l'obligation de déréférencer les liens vers les données personnelles ou comment se faire oublier du monde numérique », *RLDI*, 2014, n° 106, p. 68 et s.

F.H. CATE, C. KUNER, O. LYNSKEY, C. MILLARD et D.J.B. SVANTESSON, « When two worlds collide: the interface between competition law and data protection », *International Data Privacy Law*, 2014, p. 248 et s.

T. CHRISTAKIS, « Data, Extraterritoriality and the Need for International Law Solutions to Transatlantic Law Enforcement Issues, Legal Opinion on the Microsoft Ireland Case», *CEIS & The Chertoff Group White Paper*, 2017, disponible à l'adresse : https://ceis.eu/wp-content/uploads/2017/12/Whitepaper_EN_WEB.pdf

L.L. CHRISTIANS, « Dimensions philosophique et religieuses des approches juridiques de l'identité », in J. POUSSON-PETIT, *L'identité de la personne humaine. Etude de droit français et de droit comparé*, Bruxelles, 2002, p.63 et s.

D. K. CITRON, F. PASQUALE, « The Scored Society: Due Process For Automated Predictions », in Washington Law Review, 2014, p.89 et s.

M. CLAES, M. DE VISSER, « The Court of Justice as a Federal Constitutional Court: A Comparative Perspective », in Elke Cloots et al. Eds, *Federalism In The European Union*, 2012, p. 83 et s.

M. CLEMENT FONTAINE « La plasticité de la notion de responsable de traitement », *Revue des affaires européenne, Bruylant* 2018, p. 35 et s.

M. CLEMENT FONTAINE « L'union du droit à la protection des données à caractère personnel et du droit à la vie privée », *LEGICOM,* 2017/2 (N° 59), p. 61 et s.

M. CLEMENT FONTAINE « Faut-il se réjouir de la percée du droit à l'oubli numérique ? », *Auteurs & Média*, 2016/ 5, p. 45 et s.

M. CLEMENT FONTAINE « Le droit à l'oubli » avec R. AMARO in *La proposition de règlement européen relatif aux données à caractèr personnel: Proposition du rèseau Trans Europe Experts* N. Martial- Branzet F. Terryn (dir), coll. TEE-SC, tome 54, 2014, p. 422 et s.

G. COHEN-JONATHAN, « La Cour des Communautés européennes et les Droits de l'homme », *Revue du Marché Commun*, 1978, p. 83 et s.

G. COHEN-JONATHAN, « Aspects européens des droits fondamentaux », *Montchrestien* 3e éd., 2002, p. 114 et s.

M. D. COLE, A. VANDRIESSCHE, « From Digital Rights Ireland and Schrems in Luxembourg to Zakharov and Szabb/Vissy in Strasbourg: What the ECtHR Made of the Deep Pass by the CJEU in the Recent Cases on Mass Surveillance », in *Eur. Data Prot. L. Rev*., 2, 2016, p. 127 et s.

B. CORTESE, « La protezione dei dati di carattere personale nel diritto dell'Unione europea dopo il Trattato di Lisbona », *in Dir. Un. eur*., 2013, n. 2, p. 313 et s.

S. CORBETT, « The retention of personal information online ; A call for international regulation of privacy law », *Computer Law & Security Review*, 2013, p. 246 et s.

N. COX, « Delfi AS v Estonia : The Liability of Secondary Internet Publishers for Violation of Reputational Rights Under the European Convention on Human Rights », in *The Modern Law Review*, 2014, p. 619 et s.

M. DAUSES, « La protection des droits fondamentaux dans l'ordre juridique communautaire », *R.T.D.E*., 1984, pp. 401 et s.

N. DECOOPMAN, « À propos des autorités administratives indépendantes et de la déréglementation », in J. CLAM, G. MARTIN, *Les transformations de la régulation juridique*, LGDJ, coll. Droit et Société, n° 5, Paris, 1998, p. 249 et s.

S. DE BIOLLEY, « Liberté et sécurité dans la construction de l'espace européen de justice pénale : cristallisation de la tension sous présidence belge », in G. DE KERCHOVE et A. WEYEMBERGH (dir.), *L'espace pénal européen : enjeux et perspectives*, éd. de l'Université de Bruxelles 2003, pp. 169 et s.

E. DE BUSSER, « Data protection in EU and US criminal cooperation : a substantive law approach to the EU internal and transatlantic cooperation in criminal matters between judicial and law enforcement authorities », *Antwerpen*, 2009, p. 5 et s.

P. DE HERT, « Data protection in the area of freedom, security and justice : a short introduction and many questions left unanswered », in *ERA-Forum : scripta iuris europaei*, 2010, p.159 et s.

P. DE HERT, S. GUTWIRTH, « Data protection in the case law of Strasbourg and Luxembourg, Constitutionalisation in Action », in S. GUTWIRTH, Y. POULLET, P. DE HERT, S. NOUWT, *Springer*, 2009, p. 3 et s.

C. DE TERWANGNE, S. NOUWT (dir.), *Reinventing Data Protection ?*, Dordrecht London, Springer, 2009, p. 3 et s.

G. DE MINICO, « La risposta europea al terrorismo del tempo ordinario : il lawmaker e il giudice », in *Osservatorio sulle fonti*, n. 2/2017, disponible à l'adresse à l'adresse : http://www.europeanrights.eu/public/commenti/BRONZINI12-de_minico.pdf

O. DE SCHUTTER, « Les droits fondamentaux dans l'Union européenne », *Journal de droit européen*, 2010, p. 120 et s.

C. DE TERWANGNE, « Reinventing data protection *?* », *Spirenger Science*, Dordrecht, 2009, p. 3 et s.

C. DE TERWAGNE, « Droit à l'oubli numérique, élément du droit à l'autodétermination informationnelle ? », in D. Dechenaud (Dir.), *Le droit à l'oubli numérique*, Larcier, 2015, p. 78 et s.

D. DERO-BUGNY, « La cohèrence dans le système européen de protection des droits fondamentaux », *mélanges en l'honneur de Claude Blumann, Bruxelles, Bruylant* 2015, p. 109 et s.

D. DERO BUGNY, « Le traité de Lisbonne. Un boulversement des rapports entre la Cour de justicede l'union européenne et la Cour européenne des droits de l'homme? », J. Boudon (dir.), *Concourrence des controles et rivalité des juges*, Paris, Mare&Martin, 2012, p.133 et s.

E. DEFREYNE, « Le droit à l'oubli et les archives journalistiques », *Revue de droit des technologies de l'information,* n°51/2013, p.75 et s.

C. DI FRANCESCO MAESA, « Balance between Security and Fundamental Rights Protection : An Analysis of the Directive 2016/680 for data protection in the police and justice sectors and the Directive 2016/681 on the use of passenger name record (PNR) », in *EuroJus*, 2016, disponible à l'adresse : http://rivista.eurojus.it/balance-between-security-and-fundamental-rights-protection-an-analysis-of-the-directive-2016680-for-data-protection-in-the-police-and-justice-sectors-and-the-directive-2016681-on-the-use-of-passen/

M. DONNARUMMA, « Il processo di costituzionalizzazione dell'Unione Europea e la tensione dialettica tra la giurisprudenza della Corte di Giustizia e le giurisprudenze delle corti costituzionali », in *Riv. it. dir. pubbl. comunit.*, 2010, 02, p.407 et s.

M. DONY, « La dimension externe de l'espace de liberté, de sécurité et de justice au lendemain de Lisbonne et de Stockholm : un bilan à mi-parcours », éditions de l'Université de Bruxelles, Institut d'Etudes Européennes - I.E.E., 2014, p. 105 et s.

O. DORD, « Libertés publiques ou droits fondamentaux ? », in *Les libertés publiques, Cahiers français*, La Documentation française, 2000, p. 11 et s.

S. DOUGLAS-SCOTT, « The EU's area of freedom, security and justice : a lack of fundamental rights, mutual trust and democracy ? », in *Cambridge yearbook of European legal studies*, 2008/2009 (2009), p. 53 et s.

G. DRZEMCZEWSKI, « Le droit au respect de la vie privée et familiale, du domicile et de la correspondance tel que le garantit l'article 8 de la Convention européenne des droits de l'homme », dossier sur les droits de l'homme n°7, Conseil de l'Europe, Strasbourg 1995, p. 10 et s.

E. DUBOUT, S. TOUZÉ, « La fonction des droits fondamentaux dans les rapports entre ordres et systèmes juridiques », in *Les droits fondamentaux : charnières entre ordres et systèmes juridiques*, Pedone, 2010, p. 11 et s.

H. DUMONT et S.VAN DROOGHENBROECK, « La contribution de la Charte à la constitutionnalisation du droit de l'Union européenne », in CARLIER (J.-Y.) et SCHUTTER (O.), (sous la dir.), *La Charte des droits fondamentaux de l'Union européenne. Son apport à la protection des Droits de l'homme en Europe : hommage à Silvio Marcus-Helmons*, Bruxelles, Bruylant, 2002, p.61et s.

J. DUTHEIL DE LA ROCHÈRE, « Charte des Droits Fondamentaux, quel apport à la protection des droits ? », in *Mélanges en l'honneur de Benoit Jeanneau, Les mutations contemporaines du droit public*, Paris, Dalloz, 2002, p. 97 et s.

E. DUBOUT, « Le défi de la délimitation du Champ de la protection des droits fondamentaux par la Cour de justice de l'union européenne », *ELSJ*, 2013, vol I. 6, n. 1, p. 5 et s.

F. DUMORTIER, « La protection des données dans l'Espace européen de liberté, de sécurité et de justice », in *Journal de droit européen,* 2010, p. 33 et s.

J. DUPONT-LASSALLE, « Protection des données personnelles », *Revue mensuelle lexisnexis jurisclasseur N° 368*, octobre 2014

L. FAVOREU, « Les cours de Strasbourg et de Luxembourg ne sont pas des cours constitutionnelles » in *Au carrefour des droits : Mélanges en l'honneur de Louis Dubouis*, 2002, Dalloz, p. 35 et s.

D. FAYON, « Géopolitique d'Internet, Qui gouverne le monde ? », *Economica*, mars 2013

M. FAZLIOGLU, « Forget me not : the clash of the right to be forgotten and freedom of expression on the Internet », International Data Privacy Law, 2013, p. 150 et s.

F. FERRETTI, « Data protection and the legitimate interest of data controllers : much ado about nothing or the winter of rights ? » in *Common Market Law Review,* 2014, p. 843 et s.

F. FERRETTI, « Human Rights in the Digital Age : The European Court of Justice Ruling in the *Data Retention* Case and Its Lessons for Privacy and Surveillance in the United States », *Harvard Human Rights Journal* / Vol. 28, p.65 et s.

J.-F. FLAUSS, « La Cour européenne des droits de l'homme et la liberté d'expression journalistique », in E. ZOLLER (dir.), La liberté d'expression aux États-Unis et en Europe, Dalloz, coll. Thèmes et commentaires, 2008, p. 93 et s., sp. p. 132.

L. FLORIDI, « The 4th revolution : how the infosphere is reshaping human reality », *Oxford*, 2014, p. 96 et s.

L. FLORIDI, « Right to be forgotten poses more questions than answers Google's advisory council held its final meeting last week on the European court of justice's privacy ruling. One of the council members gives his thoughts on the issues raised », *theguardian.com*, Tuesday 11 November 2014, disponible en ligne

R. FLOR, « *Data Retention* ed art. 132 cod. Privacy : vexata quaestio (?) », in *Diritto penale contemporaneo*, 9 mars 2017, p. 67 et s.

G. FOURNIER, « Coopération judiciaire de l'Union européenne en matière pénale : quelle contribution à un universalisme pénal ? », in *La dimension extérieure de l'espace de liberté, de sécurité et de justice de l'Union européenne après le Traité de Lisbonne*, Bruylant, 2013, pp. 457 et s.

J. FRAYSSINET, « La régulation de la protection des données personnelles », *Legicom*, 2009, n° 42, p. 5 et s.

M. FROMONT, « État de droit et principe de proportionnalité. Commentaire de la décision du 15 décembre 1970 de la Cour constitutionnelle fédérale allemande », in P. BON, D. MAUS

(dir.), *Les grandes décisions des cours constitutionnelles européennes*, Dalloz, Paris, 2008, p. 51 et s.

T. E. FROSINI, « Tecnologie e libertà costituzionali », in *Scienza e diritto nel prisma del diritto comparato*, G. COMANDE' e G. PONZALLI (a cura di), Giuffrè, Milano, 2004, p. 189 et s.

Y. GAUDEMET, « Autorités administratives indépendantes », *in* J. ANDRIANTSIMBAZOVINA, H. GAUDIN, J.-P. MARGUENAUD, S. RIALS, F. SUDRE (dir.), *Dictionnaire des Droits de l'Homme,* PUF, coll. Quadrige – Dicos Poche, 2008, p. 91 et s.

J.-C. GALLOUX, « Réflexions sur la catégorie des choses hors du commerce : l'exemple des éléments et des produits du corps humain en droit français », *Les Cahiers de droit*, 1989, vol. 30, n° 4, p. 1011 et s., sp. p. 1029.

C. GAYREL, R. ROBERT, « Proposition de règlement sur la protection des données- Premiers commentaires », *Journal de Droit Européen*, édition Larcier, Juin 2012, n°190, p. 116 et s.

J. GERKRATH, « Les principes généraux du droit ont-ils encore un avenir en tant qu'instruments de protection des droits fondamentaux dans l'Union européenne ? », *R.A.E. – L.E.A.*, 2006/1, p. 31 et s.

L. GILL D. REDEKER, U. GASSER, « Towards Digital Constitutionalism ? Mapping Attempts to Craft an Internet Bill of Rights », *Berkman Center for Internet & Society, Research Pub. N*. 2015-15 (9 Nov. 2015)

GÖTMANN, « The new territorial scope of EU data protection law : Deconstructing a revolutionary achievement », in *Common Market L. Rew.*, 2017, p. 567 et s.

M. P. GRANGER, K. IRION, « The Court of Justice and the *Data Retention* Directive in *Digital Rights* Ireland : Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection », in *European Law Review*, 2014, p. 835 et s.

L. GRARD, « Nouvelle actualité des accords PNR. - Sûreté du transport aérien contre sécurité juridique », *Revue de droit des transports* n° 3, Juillet 2012, p. 3 et s.

G. GREENLEAF, « International Data Privacy Agreements after the GDPR and Schrems », in *139 Privacy Laws & Business International Report*, 2016, p.4 et s.

E. GUILD et E. BROUWER, « The Political Life of Data - The ECJ decision on the PNR Agreement between the EU and the US », *Centre for European Policy Studies, n°109*, 2006

E. GUILD « The area of freedom, security and justice ten years on : successes and future challenges under the Stockholm Programme », *CEPS*, 2010

J. L. HALPPÉRIN, « Vie privée », in *Nouveaux Cahiers du Conseil constitutionnel*, N° 48, Juin 2015, p. 59 et s.

E. HERLIN-KARNELL, « Subsidiarity in the area of EU Justice and Home Affairs law : a lost cause ? », in *European Law Journal*, 2009, p. 351 et s.

E. HERLIN–KARNELL, « Subsidiarity in the area of EU Justice and Home Affairs law : a lost cause?, in E. Kelsey, Google Spain SL and Google Unc v AEPD and Mario Costeja González : protection of personal data, freedom of information and the "right to be forgotten" »,in *European Human Rights Law Review*, 2014, p. 395 et s.

H. HIJMANS, A. SCIROCCO, « Shortcomings in EU data protection in the third and second pillars : can the Lisbon Treaty be expected to help ? », in *Common Market Law Review*, 2009, p. 1485 et s.

H. HIJMANS, « Recent developments in data protection at European Union level in ERA-Forum : scripta iuris » in *Revue trimestrielle de droit européen*, 2010, p. 271 et s.

W. HINS, « Case C-73/07, "Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia O", judgment of the Grand Chamber of 16 December 2008 », in *Common Market Law Review*, 2010, p. 215 et s.

T. HORSEY, « Reflections on the role of the Court of Justice as the « motor » of European integration: Legal limits to judicial lawmaking », *in Common Market Law Review*, 2013, p. 931 et s.

HOTTELIER M., « Le noyau intangible des libertés », *in* P. MEYER-BISCH (dir.), *Le noyau intangible des droits de l'Homme*, éd. universitaire de Fribourg, 1991, pp. 67 et s.

P. HUSTINX, « The Role of Data Protection Authorities », in S. GUTWIRTH, Y. POULLET, P. DE HERT, C. DE TERWANGNE, S. NOUWT (dir.), *Reinventing Data Protection, Dordrecht London*, Springer, 2009, pp. 131 et s.

A. ILIOPOULOU, « Assurer le respect et la promotion des droits fondamentaux : un nouveau défi pour l'Union européenne », *CDE* 3-4/2007, p. 458 et s.

J-P. JAQUÉ, « Communauté des internautes et protection des libertés individuelles dans l'Union européenne », in *Revue trimestrielle de droit européen*, 2010, p. 271 et s.

S. JOHNSON, M. ECHIKSON, M. WILLIAM, « The Internet : Europe's privacy cops », *Business Week*, New York, no. 3586, 2 November 1998, p. 20 et s.

J. JONES, « Control-alter-delete : the "right to be forgotten" – "*Google Spain* SL, Google Inc v Agencia Española de Protección de Datos" », in *European Intellectual Property Review*, 2014, p. 595 et s.

P. KAYSER, « Le Conseil constitutionnel, protecteur de la vie privée à l'égard des lois », *Melanges P. Raynaud* 1985, p. 329 et s.

F. KAUFF-GAZIN, « Note, L'arrêt Bosphorus : quand le juge de Strasbourg décerne au système communautaire un label de protection satisfaisante des droits fondamentaux », *L.P.A.*, 24 novembre 2005, n°234, p. 9 et s.

M. KOEKKOEK et B. VAN ALSENOY, « Internet and jurisdiction after Google Spain : the extraterritorial reach of the right to be delisted», *International Data privacy law*, 2015, p. 109 et s.

J. KOKOTT and C. SBOTTA, « The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR », *International Data Privacy Law*, 2013, p. 222 et s.

L. KONG, « Data protection and transborder data flow in the European and global context », in *European Journal of International Law*, 2010, p. 441et s.

T. KONSTADINIDES, « Destroying democracy on the ground of defending it ? The *Data Retention* Directive, the surveillance state and our constitutional ecosystem », *European Law Review*, 2011, vol. 36, n. 5, p. 722 et s.

T. KONSTANDINIDES, « Analysis and reflections : wavering between centres of gravity: comment on Ireland v.. Parliament and Council », in *European Law Review*, 2010, p. 88 et s.

W. KOTSCHY, « The proposal for a new General Data Protection Regulation, problems solved? », in *International Data Privacy Law*, 2014, Vol. 4, No. 4, p. 274 et s.

H. KRANENBERG, « Access to documents and data protection in the European Union : On the public nature of personal data », in *Common Market Law Review*, 2008, p. 1079 et s.

H. KRANENBERG, « Article 8: Protection of personal data, in The EU Charter of Fundamental Rights : a commentary », in S. Peers T.K. Hervey, J. Kenner, A.Ward [ed. by], *Oxford*, 2014, p. 187 et s.

C. KUNER, « Transborder data flow regulation and data privacy », *Oxford University Press*, 2013

H. LABAYLE, « Architecte ou spectatrice ? La Cour de justice de l'Union dans l'Espace de liberté, sécurité et justice », *R.T.D.E.*, 2006, p. 105 et s.

M. LAGRANGE, « La Cour de justice des Communautés européennes », *E.D.C.E*., 1963, p. 55 et s.

M.A. LEDIEU, « Surveillance des transferts bancaires européens par les autorités américaines : vers une remise en cause des garanties négociées », *Communication Commerce électronique* n° 10, Octobre 2009, p.124 et s.

K. LENAERTS, « The Court's Outer and Inner Selves : Exploring the External and Internal Legitimacy of the European Court of Justice », in M. Adams–H. De Waele–J. Meeusen–G. Straetmans, *Judging Europe's Judges. The Legitimacy of the Case Law of the European Court of Justice*, Oxford- Portland, 2013, p.13 et s.

K. LEANERTS, J.A. GUTIERREZ-FONS, « The place of the Charter in the EU constitutional edifice», in S. PEERS–T. HERVEY–J. KENNER–A. WARD (a cura di), *The EU Charter of fundamental Rights*, Oxford e Portland (OR) 2014, p. 1559 et s.

A.-S. LIND, M. STRAND, « A New Proportionality Test for Fundamental Rights ? The Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR (C-92/09) and Hartmut Eifert (C-93/09) v. Land Hessen », Stockholm, *SIEPS*, 2011

O. LINSKEY, « Deconstructing data protection [electronic resource] : the "added-value" of a right to data protection in the EU legal order », in *International and Comparative Law Quarterly*, 2014, v. 63, n. 3, July, p. 569 et s.

O. LINSKEY, « The *Data Retention* Directive is incompatible with the rights to privacy and data protection and is invalid in its entirety : digital rights Ireland. Joined Cases C-293 & 594/12, *Digital Rights* Ireland Ltd and Seitlinger and others, Judgment of the Court of Justice (Grand Chamber) of 8 April 2014, nyr », in *Common Market Law Review*, 2014, p. 1789 et s.

C. LUCIONI, « Tutela dei dati personali del cittadino dell'Unione e giudizio di non discriminazione in base alla CJUE », in *Revue trimestrielle de droit européen*, 2014, p. 283 et s.

M. MAES, « La refonte du règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents, du Conseil et de la Commission », in *Revue du droit de l'Union européenne*, 2007, p. 411 et s.

P. MAGNETTE, « Prendre la Charte au sérieux. La force politique d'un texte juridique non contraignant », in CARLIER (J.-Y.) et DE SCHUTTER (O.), (sous la dir.), *La Charte des droits fondamentaux de l'Union européenne. Son apport à la protection des Droits de l'homme en Europe : hommage à Silvio Marcus-Helmons*, p. 97 et s.

H. MAISL,*« Formes et techniques de participation du public à l'élaboration d'actes législatifs et administratifs», in* CONSEIL DE L'EUROPE, AFFAIRES JURIDIQUES *(dir.), Formes de*

participation du public à l'élaboration des actes législatifs et administratifs – Actes du 7ème colloque de droit européen, Strasbourg, 1978, p. 15 et s.

N. MALLET-POUJOL, «Une forme d'embargo numérique est nécessaire pour ne pas sombrer dans la tyrannie de la transparence» : *Légipresse* 2002, n° 297, p. 510 et s.

A. MANTELERO, « Responsabilita`e rischio nel Regolamento », UE 2016/679, In *Le Nuove leggi civili commentate* 1/2017, Cedam, p. 152 et s.

N. MARTIALl-BRAZ, **«**Les nouveaux droits des personnes concernées, Droit des personnes concernées, Droit à la mort numérique, mineurs, consentement,Droit à l'information, Droit de rectification, Droit à l'effacement, Droit à l'oubli numérique, Droit à la portabilité**»**, *Revue des affaires européennes, Bruylant*, 2018, p. 7 et s.

R. MASTROIANNI, « Le garanzie dei valori nell'azione esterna e il ruolo della Corte di giustizia » , in E. SCISO, R. BARATT, C. MORVIDUCCI (a cura di), *I valori dell'Unione europea e l'azione esterna*, Torino, 2016, p. 213 et s.

D. MAZEAUD, « L'expertise de droit à travers l'amicus curiae », in M.-A. FRISON -ROCHE, D. MAZEAUD (dir.), *L'expertise, Dalloz, coll. Thèmes et commentaires*, 1997, p. 109 et s.

M. MENDEZ, « Passenger Name Record Agreement : European Court of Justice. Annulment of Commission Adequacy Decision and Council decision concerning conclusion of Passenger Name Record Agreement with US. Grand Chamber judgment of 30 May 2006, joined cases C-317/04 and C-318/04, European Parliament v. Council », in *European constitutional law review*, 2007, p. 127 et s.

MESSINA, « La Corte di Giustizia estende al gestore del motore di ricerca la responsabilità di garantire il diritto all'oblio nei confronti delle persone fisiche », in *Rivista Ordine internazionale e diritti umani*, N. 3/2014, p.617 et s.

M. MESSINA, « La Corte di giustizia Ue si pronuncia sulla proporzionalità delle misure in materia di conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica e ne dichiara la loro invalidità», in *Ordine internazionale e diritti umani*, 2014, p. 396 et s.

N. METALLINOS, J. DEROULEZ, L. TASSONE, « Le droit européenne de la protection des données », *L'Observateur de Bruxelles*, N° 93, 2013

V. MICHEL, « La dimension externe de la protection des données à caractère personnel : acquiescement, perplexité et frustration, note sous l'arrêt su 30 mai 2006, Parlement européen c. Conseil, aff. jtes C-317 et 318/04», *Revue Trimestrielle Droit Européen*, 3/2006, p.535 et s.

H.W. MICKLITZ, « The Internal v. The External Dimension of European Private Law – A Conceptual Design and a Research Agenda », *EUI Working Papers*, 2015, p. 55 et s ;

E. MILLARD, « Effectivité des droits de l'homme », in J. ANDRIANTSIMBAZOVINA, H. GAUDIN, J.-P. MARGUENAUD, S. RIAL, F. SUDRE (dir.), *Dictionnaire des droits de l'homme*, PUF, coll. Quadrige – Dicos Poche, 2008, pp. 277 et s.

V. MITSILEGAS, « The third wave of third pillar law : which direction for EU criminal justice? » in *European Law Review*, 2009, p. 523 et s.

J. MONAR, « The rejection of the EU-US *Swift* Interim Agreement by the European Parliament : a historic vote and its implications », in *European Foreign Affairs Review*, 2010, p. 143 et s.

A. MOORE, Privacy Rights: Moral and legal foundations, University Park PA, The Pennsylvania State University Press, 2010, p. 237 et s.

C.C. MURPHY, « The draft EU Directive on Combating Terrorism : Much Ado About What ? », in *EU Law Analysis*, 2006, disponible à ll'adresse : http://eulawanalysis.blogspot.com/2016/01/the-draft-eu-directive-on-combating.html

F. NAFTALSKI, F. RAYNAL, « Mise en ligne de données personnelles et transfert de données à l'étranger », *Revue Lamy Droit des affaires*, Janvier 2004, chronique p. 15 et s.

M. NINO, « L'annullamento del regime della conservazione dei dati di traffico nell'Unione europea da parte della Corte di giustizia UE : prospettive ed evoluzioni future del sistema europeo di *Data Retention »*, in *Dir. Un. Eur*., 2014, p. 803 et s.

K. NUOTIO, « Security and Criminallaw: A difficult Relationship », in M.FICHERA et J. KREMER (dir.), *Law and Security in Europe : Reconsidering the Security Constitution, Intersentia,* 2013, p. 197 et s.

H. OBERDORFF, « La reconnaissance des droits fondamentaux par l'Union européenne », in *L'odyssée des Droits de l'homme : Fondations et naissances des Droits de l'homme*, L'Harmattan, 2003, pp. 368 et s.

H. OBERDORFF, « Les libertés individuelles face aux technologies de sécurité *», in Libertés. Mélanges Jacques Robert,* Montchrestien, 1998, pp. 177 et s.

P. OLIVER, « The Protection of Privacy in the Economic Sphere before the European Court of Justice in Parliament and Council », in *European Law Review*, 2010, p. 88 et s ;

Y. PADOVA, D. LEBEAU-MARIANNA, « Entre droit des données personnelles et liberté d'expression, quelle place pour les moteurs de recherche ? » *RLDI*, 2013/90 et les références jurisprudentielles commentées.

V. PAPAKONSTANTINOU, P. DE HERT, « The PNR Agreement and transatlantic anti-terrorism cooperation : no vote and its implications », in *European Foreign Affairs Review*, 2010, p. 143 et s.

S. PEERS, « The Domino effect: how many EU Treaties violate the rights to privacy and data protection? », in *EU Law Analysis*, 25 novembre 2014, p.34 et s.

S. PEERS, « Europe v Facebook: the beginning of the end for NSA spying on EU citizens ? », *EU Law analysis*, 18 juin 2014, disponible à l'adresse: http://eulawanalysis.blogspot.gr/2014/06/europe-v-facebook-beginning-of-end-for.html

S. PEYROU, « L'affaire Marper c/ Royaume-Uni : un arrêt fondateur pour la protection des données dans l'espace de liberté, sécurité, justice de l'Union européenne », in *Revue française de droit administratif*, 2009, p. 741 et s.

S. PEYROU, « La Cour de justice, garante du droit « constitutionnel » à la protection des données à caractère personnel », *RTDE*, 2015, n°1, p. 117 et s.

S. PEYROU, « Protection des données à caractère personnel dans le contexte de l'Accord de partenariat économique UE-Japon : des systèmes en voie de convergence », in *Revue des affaires européennes, Bruylant*, 2018, p. 53 et s.

P. PESCATORE, « La Cour de justice des Communautés européennes et la Convention européenne des Droits de l'homme », in *Mélanges, Wiarda*, 2e éd., 1990, p. 441 et s.

F. PICOD, « Le juge communautaire et l'intérpretationeuropéenne », in F. SUDRE, *L'intérpétation de la Convention européenne des droits de l'homme*, *Bruxelles, Bruylant*, 1998, p. 280 et s.

F. PICOD, « Droit de l'Union européenne des Droits de l'homme et des libertés fondamentales », 2007, *J.-Cl. Libertés*, fasc. n° 120, p. 32 et s.

F. PIZZETTI, « Le autorita garanti per la protezione dei dati personali e la sentenza della Corte di giustizia sul caso Google Spain: e` tempo di far cadere il "velo di Maya" », *Roma Tre Press*, 2015, p. 255 et s.

S. POLI, « The legal basis of internal market measures with a security dimension : comment on Case C-301/06 of 10/02/2009, "Ireland v Parliament/Council"», in *European Constitutional Law Review*, 2010, p. 137 et s.

C. PRIETO, « La Liberté d'établissement et de prestation de services », *R.T.D.E*., 2005, p. 867 et s.

M.-C. PONTHOREAU, « La directive 95/46 CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données », *RFDA*, 1997, p. 125 et s.

M.-C. PONTHOREAU, « Droit(s) constitutionnel(s) comparé(s) », *Economica, coll. Corpus Droit public*, 2010, p. 401.

Y. POULLET et S. GUTWIRTH, « The contribution of Article 29 Working Party to the Construction of Harmonized European Data Protection System : an illustration of Reflexive Gouverance ? », in M. PEREZ ASINARI P. PALAZZI (dir.), *Défis du droit à la protection de la vie privée*, Bruylant, 2008, p. 569 et s.

POULLET Y., « Pour une troisième génération de réglementation de protection des données », in M.-V. PEREZ ASINARI, P. PALAZZI (dir.), *Défis du droit à la protection de la vie privée. Challenges of privacy and data protection law. Perspectives du droit européen nord-américain. Perspectives of European north american law*, Bruxelles, Bruylant, coll. Cahiers du CRID n°31, 2008, p. 25 et s.

C. PRIETO, « La Liberté d'établissement et de prestation de services », *R.T.D.E*., 2005, p. 867 et s.

X. PRIOLLAUD et D. SIRITZKY, « Le traité de Lisbonne, Texte et Commentaire article par article des nouveaux traités européens (TUE-TFUE) », *La documentation française*, 2008, p. 124 et s ;

P. PUOTI, « Lotta al terrorismo, sicurezza del trasporto aereo e protezione dei dati personali nel recente contenzioso Usa/Ue » », *in Le scommesse dell'Europa : diritti, istituzioni, politiche*, 2009, p. 421 et s.

S. RIALS S., « Les standards, notions critiques du droit », in C. PERELMAN, R. VANDER ELST (dir.), *Les notions à contenu variable en droit*, Bruxelles, Bruylant, 1984, pp. 39 et s.

G.M. RICCIO, « Diritto all'oblio e responsabilita` dei motori di ricerca; Dalla Data Retention al diritto all'oblio. Dalle paure orwelliane alla recente giurisprudenza della Corte di Giustizia. Quali effetti per il sistema di giustizia penale e quali prospettive de jure condendo? », Roma Tre Press, 2015, p. 199 et s.

N.M. RICHARDS, « The Dangers of Surveillance », *126 Harv. L. Rev*. 2013, p.1037 et s.

E.A. ROSSI, « Il diritto alla privacy nel quadro giuridico europeo e internazionale alla luce delle recenti vicende sulla sorveglianza di massa », in *Dir. com. sc. int.*, 2014, p. 331 et s.

J. ROSSI, « Guide de la jurisprudence européenne en matière de protection des données à caractère personnel », **Cahiers Costech**, mai 2017, n°1, p.58 et s.

D. ROUSSEAU, « Les droits de l'Homme de la troisième génération », in L. FAVOREU (dir.), *Droit constitutionnel et Droits de l'homme, Economica* - PUAM, coll. Droit public positif. Série Travaux de l'Association française des constitutionnalistes, 1987, pp. 125 et s.

A. ROUVORY et Y. POULLET, « The right to informational self-determination and the values of self-developpement : reassessing the importance of privacy for democracy ? », in S. GURWITH and others (eds), *Reinventing Data protection ?* New York, Springer, 2009, p. 47et s.

A. ROUVORY,« Réinventer l'art d'oublier et de se faire oublier dans la société de l'information ? », in S. LACOUR (dir.), *La sécurité de l'individu numérisé. Réflexions prospectives et internationales*, L'Harmattan, 2008, p. 249 et s.

SÁNCHEZ, « The Court and the Charter : The impact of the entry into force of the Lisbon Treaty on the ECJ's approach to fundamental rights », in *Common Market Law Review*, 2012, 1564 et s.

J. SANTOS VARA, « The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon », *Centre for the Law of External Relations*, documenti di lavoro CLEER 2013/2, p. 18 et s.

S. SAURUGGER et F. TREPAN, « La Cour de justice au cœur de la gouvernance européenne », *Pouvoirs*, n°149, 2014, p.59 et s.

L. SCHEECK, U. DE TORRES, « Le dialogue des droits fondamentaux en Europe, fédérateur de loyautés, dissolvant de résistances ? L'Europe des Cours : résistances et loyautés sur la protection des données à caractère personnel », in *Revue de l'Union européenne*, 2014, p. 170 et s.

D. SIMON, « La révolution numérique du juge de l'Union : les premiers pas de la cyber-citoyenneté », *Europe*, juillet 2014, p. 4 et s.

M. SIANO, « Il diritto all'oblio in Europa e il recente caso spagnolo », in F. PIZZETTI (a cura di), *Il caso del diritto all'oblio*, Giappichelli, Torino 2013, p. 37 et s.

R. SICURELLA, V. SCALIA, « Data mining and Profiling in the Area of Freedom, Security and Justice. State of Play and New Challenges in the Balance between Security and Fundamental Rights Protection », in *NJECrimL*, 2013, 4, p. 432 s.

A. SPAGNOLO, « Bilanciamento tra libertà d'espressione su Internet e tutela del diritto d'autore nella giurisprudenza recente della Corte europea dei diritti umani », in *Federalismi.it Focus Human Rights*, n. 2/2013 p. 104 et s.

A. SROWEL, « Le droit à l'oubli du condamné : après le moment du compte rendu, vient le temps du silence », in « L'accélération du temps juridique », Ph. Gérard, F. Osten et M. Van de Kerchove (dir.), *Bruxelles, Publications des FUSL, 20 0000*, p. 737 et spéc. p. 747 et s.

F. SUDRE, « La Communauté européenne et les droits fondamentaux après le traité d'Amsterdam. Vers un nouveau système de protection des Droits de l'homme ? », *Jurisclasseur*, Éd. G., n° 1, 7 Janvier 1998, I, pp. 100 et s.

F. SUDRE « La cohérence issue de la jurisprudenceeuropéennedes droits de l'homme, L'équivalencedans tous ses ètats », in C. PICHERAL et L. COUTRON (dir.), *Charte des droits fondamentaux de l'Union européenne et Convention européenne des droits de l'homme, Bruxelles, Bruylant*, 2012, p. 45 et s.

F. SUDRE, « Les conflits de droits. Cadre général d'approche dans la jurisprudence de la Cour européenne des droits de l'homme », in L. POTVIN-SOLIS (dir.), *La conciliation des droits et libertés dans les ordres juridiques européens*, Bruxelles, Bruylant, coll. Colloques Jean Monnet, 2012, pp. 233 et s.

F. SUDRE, « A propos du dialogue des juges et du contrôle de conventionalité », in *Etudes en l'Honneur de Jean-Claude GAUTRON*, Paris, Pedone, 2004, p. 208 et s.

D. SZYMCZAK, « Le principe de proportionnalité comme technique de conciliation des droits et libertés en droit européen », in L. POTVIN-SOLIS (dir.), *La conciliation des droits et libertés dans les ordres juridiques européens*, Bruxelles, Bruylant, coll. Colloques Jean Monnet, 2012, p. 445 et s.

O. TAMBOU, « Protection des données personnelles : les difficultés de la mise en œuvre du droit européen au déréférencement », *RTD*, avril-juin 2016, p. 249 et s.

O. TAMBOU, « Rapport du comité Google : exercice d'autorégulation d'un droit à l'oubli », Dalloz actualité, 19 février 2015. Disponible à l'adresse : http://www.dalloz-actualite.fr/chronique/rapport-du-comite-google-exercice-d-autoregulation-d-un-droit-l-oubli#.VUhvlJOyLpK

C. TANKARD, « What the GDPR means for business », *Network Security*, 2016, n° 6, p. 5 et s.

V.G. TAUPIAC NOUVEL, « De la protection des données personnelles à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en coopération pénale européenne, La fragmentation de l'Espace de liberté sécurité et de Justice », *Journée d'étude européennes du GDR CNRS ELSJ, Lyon III,* 14 et 15 juin 2012

C. TEITGEN-COLLY, « Les autorités administratives indépendantes » in O. DUHAMEL (dir.), *Dictionnaire constitutionnel,* PUF, 1992, p. 65 et s.

A. TERRASI, « Trasmissione dei dati personali e tutela della riservatezza : l'accordo tra Unione europea e Stati Uniti del 2007 », in *Rivista di diritto internazionale,* 2008, p. 375 et s.

A. TERRASI, « Il rapporto tra diritto alla privacy e protezione dei dati personali tra Corte di giustizia dell'Unione europea e Corte europea dei diritti dell'uomo»,, in DISTEFANO (dir), *La protezione dei dati personali ed informatici nell'era della sorveglianza globale*, Napoli, 2017, p.127 et s.

G. TIBERI, « L'accordo tra la Comunità europea e gli Stati Uniti sulla schedatura elettronica dei passeggeri aerei al vaglio della Corte di giustizia », *Quaderni costituzionali,* 2006, p. 824 et s.

R. TINIERE, « Le principe d'alignement sur le standard pour les droits conventionnels correspondants » in C. PICHERAL et L. COUTRON (dir.), *Charte des droits fondamentaux de l'Union européenne et Convention européenne des droits de l'homme, Bruxelles, Bruylant*, 2012, p. 3 et s.

R. TINIERE, « Article 8 protection des données à caractère personnel », in F. PICOD, S. VAN DROOGHENBROEK, *Commentaire article par article de la CDFUE,* I ere édition, 2018, p. 186 et s.

R. TINIÈRE, « La cohérence assurée par l'article 52§3 de la Charte des droits fondamentaux de l'Union - Le principe d'alignement sur le standard conventionnel pour les droits correspondants », in C. PICHERAL et L. COUTRON (dir.), *Charte fondamental de l'Union européenne et Convention européenne des droits de l'homme*, Bruylant, 2013, p. 14 et s.

M. TROPER, « Le problème de l'interprétation et la théorie de la supra légalité constitutionnelle », in *Recueil d'études à la mémoire de Charles Eisenmann*, éd. Cujas, 1975, p.149 et s.

E. TOPOL, « On the Future of Medicine », *Wall Street Journal*, 7 juillet 2014

B. VAN DER SLOOT, « Privacy in the post-NSA era : time for a fundamental revision ? », JIPITEC 2014, para 1 Chamber of 10 February, *Common Market Law Review*, 2009, p. 1167 et s.

A. VON BOGDANDY, A. VON KOTTMANN, M. ANTPOHLRT, C. DICKSCHEN, J. HENTEI, R. SOLANGE, « Protecting the essence of fundamental rights against EU Member States », *Common Market Law Review* 49.2, 2012, pp. 489 et s.

M.VALERIE, « La dimension externe de la protection des données à caractère personnel: acquiescement, perplexité et frustration », *Revue trimestrielle de droit européen*, 2006, p. 549 et s.

V.N. VANDYSTADT, « Cour de justice : une directive antiterrorisme sur la sellette », *Europolitics*, n°4846, mardi 8 avril 2014, p. 8 et s.

G. VESPERINI-MAISL, « Les autorités administratives indépendantes : protection des libertés ou régulation sociale*? »,* in *Les autorités administratives indépendantes*, Colliard – Timsit, p. 87 et s.

J.-P. WALTER, « La Convention du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données », in A. EPINAY, M. FREIERMUTH (dir.), *Datenschutz in der Schweiz und in Europa – La protection des données en Suisse et en Europe*, Editions universitaires Fribourg Suisse, 1999, pp. 83 et s.

S. WARREN, L. D. BRANDEIS, « The right of privacy », in *Harvard Law Review*, 1890, 4, p.193 et s.

B. WARUSFEL, « Jacques Ellul et la construction ambivalente du droit des nouvelles technologies », in P. TROUDE-CHASTENET (dir.), Jacques Ellul, penseur sans frontières, L'esprit du temps, 2005, pp. 105 et s.

R.H. WEBER, « The Right to Be Forgotten : More Than a Pandora's Box ? », *J.I.P.I.T.E.C.*, 2011, p. 120 et s.

A. WEYEMBERGH, « L'impact du 11 septembre sur l'équilibre sécurité/liberté dans l'espace pénal européen », in E. BRIBIOSA et A. WEYEMBERGH (dir.), *Lutte contre le terrorisme et droits fondamentaux*, Bruylant, 2002, pp. 153 et s.

J. WHITMAN, « The Two Western Cultures of Privacy : Dignity v. Liberty », *The Yale Law Journal*, 2004, 1p. 1151 et s.

L. WOODS, « Zakharov v Russia: Mass Surveillance and the European Court of Human Rights », in *EU Law Analysis*, 2015

L. WOODS, « Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson (Grand Chamber) », in *EU Law Analysis*, 2016

G. XYNOPOULOS, « Proportionnalité », in D. ALLAND, S. RIALS (dir.), *Dictionnaire de la culture juridique, PUF, coll. Quadrige – Dicos Poche*, Paris, 2003, p. 1251 et s.

Z. ZENCOVICH, « Intorno alla decisione nel caso Schrems : la sovranità digitale e il governo internazionale delle reti di telecomunicazione », in G. Resta, V. Zeno-Zencovich (a cura di), *La*

protezione transnazionale dei dati personali dal Safe Harbour principles al privacy Shield, Roma, 2016, p. 7 et s.

J. ZILLER, « Le fabuleux destin des explications relatives à la charte des droits fondamentaux de l'Union européenne », in *Chemins d'Europe-Mélanges, Jean-Paul Jaqué*, Paris, *Dalloz* 2010, p. 83 et s.

J. ZILLER, « Le réseau des protecteurs des données de l'Union européenne et la promotion internationale des autorités indépendantes de protection des données informatiques » in *indépendance : étude offert au professeur Jean-Louis Autin, Presse Université de Montpellier I-CREAM* ; 2012, p. 745 et s.

J. ZILLER, *Le principe de proportionnalité, AJDA*, 1996, p. 185 et s.

E. ZOLLER, « Grands arrêts de la Cour suprême des États-Unis », Paris, PUF, *coll. Droit fondamental*, 2000, p. 694 et s.

Thèses consultées

M. BETTONI, *Libertà di espressione e sorveglianza globale*, Tesi Università di Bologna, 2014

L. COUDRAY, *La protection des données personnelles dans l'Union européenne*, Thèse Paris II, 2005

E. DEBAETS, *Le droit à la protection des données personnelles, recherche sur un droit fOndamental*, Thèse Paris 1 Panthéon-Sorbonne, 2014

H. GAUDIN, *Le parlement européen devant la Cour de justice des Communautés Européennes, Contribution à l'étude des fonctions constitutionnelles de la Cour de justice des Communautés européennes*, Thèse, Toulouse, 1994

E. GRATTON, *Redéfinir la notion de donnée personnelle dans le contexte des nouvelles technologies de l'Internet*, Thèse Paris I, 2010

C. MAUBERNARD, *Les normes juridiques de la jurisprudence de la Cour de justice des Communautés européennes, contribution à l'étude du pouvoir judiciaire communautaire*, Thèse université de Montpellier I, 2001,

N. OCHOA, *Le droit des données personnelles, une police administrative spéciale*, Thèse Paris 1 Panthéon-Sorbonne, 2014

A. REMEDEM, *La protection des droits fondamentaux par la Cour de justice de l'Union européenne*, Droit, Université d'Auvergne - Clermont-Ferrand I, 2013

M.-C. ROQUES -BONNET, *La Constitution et l'Internet*, Thèse Université Toulouse 1, 2008

TABLE DE JURISPRUDENCE

1. CEDH

CEDH, 7 septembre 1976, *Handyside c. Royaume-Uni*, req. n°5493/72, p. **281, 286, 293, 294, 310**

CEDH, 18 janvier 1978, *Irlande c. Royaume-Uni*, req. n°5310/71, *A25* CEDH, 25 avril 1978, *Tyrer c/ Royaume-Uni*, n°5856/72, p.**31, 50**

CEDH, 6 septembre 1978, *Klass c. Allemagne*, req. n°5502971, p. **254, 255, 283, 288, 292, 307, 311, 319**

CEDH, 26 avril 1979, *Sunday Times c. Royaume-Uni*, n°6538/74, p. **278, 292**

CEDH, 9 octobre 1979, *Airey c. Irlande*, n°6289/73,

CEDH, 2 août 1984, *Malone c. Royaume-Uni*, n°8691/79, p. **254, 277, 278, 284, 318**

CEDH, 26 mars 1985, *X. et Y. c. Pays-Bas*, n°8978/80

CEDH, 26 mars 1987, *Leander c. Suède*, n°9248/81, p.**230, 279 à 284, 288, 294, 318**

CEDH, 7 juillet 1989, *Gaskin c. Royaume-Uni*, n°10454/83

CEDH, 20 novembre 1989, *Markt Intern Verlag GmbH et Klaus Beermann c.Allemagne*, n°10572/83

CEDH, 24 avril 1990, *Kruslin c. France*, n°11801/85, p.**284**

CEDH, 25 mars 1992, *Campbell c. Royaume-Uni*, n°13590/88, p. **284**

CEDH, 25 février 1997, *Z. c. Finlande*, req. n°22009/93, p.**284, 288, 293, 294, 314**

CEDH, *M.S. c. Suède*, 27 août 1997, req. n° 20837/92, p. **285, 311**

CEDH [GC], 21 janvier 1999, *Fressoz et Roire* c. France, n° 29183/95, p.**34, 327**

CEDH [GC], 16 février 2000, *Amannc. Suisse*, req. n°27798/95, p. **28, 148, 278, 318, 336, 364**

CEDH [GC], 4 mai 2000, *Rotaru c. Roumanie*, req. n° 28341/95, p. **28, 148, 279, 317, 364**

CEDH, 29 avril 2002, *Pretty c. Royaume-Uni*, req. n°2346/02,p. **32**

CEDH [GC], 11 juillet 2002, *Christine Goodwin c/ Royaume-Uni*, n°28957/95

CEDH, 28 janvier 2003, *Peck c. Royaume-Uni*, req. n°44647/98, p.**284**

CEDH [GC], 13 février 2003, *Odièvre c. France*, n°42326/98, p.**290**

CEDH, 6 mars 2003, *Zdanoka c. Lettonie*, req. n°58278/00

CEDH, 17 juillet 2003, *Perry c. Royaume-Uni*, req. n° 63737/00, p. **33**

CEDH, 18 mai 2004, *Editions Plon c. France*, n°58148/00,

CEDH 24 juin 2004, *Von Hannover c. Allemagne*,n°59320/00,p. **290**, **325, 327, 329, 336**

CEDH [GC], 30 juin 2005, *Bosphorus Hava Yollari Turizm ve Ticaret Anonim Sirketi c. Irlande*, req. n°45036/98, *p.* **250, 269, 380**

CEDH, 20 décembre 2005, *Wisse c/ France*, req. n°71611/01

CEDH [GC], 11 janvier 2006, *Sorensen et Rasmussen c. Danemark*, n°52562//99 et n°52620/99.

CEDH, 3 avril 2007, *Copland c. Royaume-Uni*, req. n° 62617/00,

CEDH, 25 novembre 2008, *Biriuk c. Lituanie*, req. n°23373/03 CEDH, 2 décembre 2008, *K.U. c. Finlande*, n°2872/02, p. **326, 357**

CEDH [GC], 4 décembre 2008, *S. et Marper c/ Royaume-Uni*, n°30562/04 et n°30566/04, p. **28, 148, 167, 271, 283, 293, 294, 314, 317, 320, 417, 428**

CEDH, 27 octobre 2009, *Haralambie c/ Roumanie*, n° 21737/03

CEDH, 17 décembre 2009, *Gardel c/ France*, n°16428/05, *p.***283**

CEDH, 17 décembre 2009, *M.B. c. France*, n°22115/06, p. **283**

CEDH, 17 décembre 2009, *B.B. c.France*, n° 5335/06, p. **283**

CEDH, 18 octobre 2011, *Khelili c. Suisse*, n° 16188/07, p. **283, 310, 311**

CEDH [GC], 2 février 2012, *Von Hannover c. Allemagne (n°2)*, r n°40660/08 et n°60641/08, *Rec. 2012, p.* **328, 336, 347, 357**

CEDH [GC], 7 février 2012, *Axel Springer AG c.Allemagne*,. n°39954/08, p. **328,330**

CEDH, 18 septembre 2014, *Brunet c. France*, n° 21010/10, p. **344, 417**

CEDH, L.H. c. Latvia, 29 April 2014, n°. 52019/07,

CEDH, [GC], 4 decembre 2015, *Roman Zakharov c. Russia*, req. n° 47143/06 : **106, 254 à 258, 262, 273, 307, 308, 317 à 319, 380**

CEDH, 12 janvier 2016, *Szabó and Vissy c. Hungary*, req. n° 37138/14 : **255, 256, 307**

CEDH, [GC], 5 Septembre 2017, *Bă rbulescu c. Romania*, n°. 61496/08

2. Cour de justice de l'Union européenne

CJCE, 17 décembre 1970, *Internationale Handelsgesellschaft mbH c. Einfuhr- und Vorratsstelle für Getreide und Futtermittel*, aff. C-11/70

CJCE, 11 mai 1974, *J. Nold, Kohlen- und Baustoffgroßhandlung c. Commission des Communautés européennes*, aff. 4/73, p. **47, 267**

CJCE, 28 octobre 1975, *Roland Rutili c. Ministre de l'intérieur*, aff. C-36/75, p. **47**

CJCE, 26 juin 1980, *National Panasonic (UK) Limited c. Commission des Communautés européennes*, aff. C-136/79, p.**36**

CJCE, 5 octobre 1994, *X. c. Commission des Communautés européennes*, aff. C-404-92 P,

CJCE, 28 mars 1996, avis n° 2/94, *Adhésion de la Communauté à la convention de sauvegarde des droits de l'homme et des libertés fondamentales*, p. **51, 362**

CJCE, 20 mai 2003, *Rechnungshof c. Österreichischer Rundfunk et autres*, aff. C-465/00, C-138/01, C-139/01, *p.*: **36, 181, 280, 312, 355, 392**

CJCE, 6 novembre 2003, *Bodil Lindqvist*, aff. C-101/01, *p.* **36, 54, 81 à 84, 88, 182, 185, 228, 312, 324 à 326, 336, 339, 340, 378**

CJCE, G. Ch. (ord.), 17 mars 2005, *Parlement européen c. Conseil de l'Union européenne*, aff. C-317/04, *p.* **452**

CJCE, G. Ch., 30 mai 2006, *Parlement européen c. Conseil de l'Union européenne et Commission des Communautés européennes*, aff. C-317/04 et C-318/04, *p.* **36, 76, 84, 85, 100, 165, 224, 226, 227, 284, 302, 303, 447 454, 461, 471**

CJCE, G. Ch., 16 décembre 2008, *Tietosuojavaltuutettu c. Satakunnan Markkinapörssi Oy et Satamedia Oy*, aff. C-73/07, *p.***88, 105, 289, 306, 327, 330, 343, 356, 372, 378, 453**

CJCE, G. Ch., 16 décembre 2008, *Heinz Huber c. Bundesrepublik Deutschland*, aff. C-524/06, *p.* **83, 85, 148, 313**

CJUE, G. Ch., 10 février 2009, *Irlande c. Parlement européen et Conseil de l'Union européenne*, aff. C-301/06, *p.***77, 100, 166, 252, 365, 471**

CJCE, 7 mai 2009, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, aff. C-553/07, p.**87, 92, 213**

CJUE, G. Ch., 9 mars 2010, *Commission européenne c. République fédérale d'Allemagne*, aff. C-518/07, *p.* **54, 93, 378, 395, 454**

CJUE, G. Ch., 29 juin 2010, *Commission européenne c. The Bavarian Lager Co. Ltd.*, aff. C-28/08 P, *p.* **37, 123, 124, 286, 332, 333, 378, 448, 449, 452, 454**

CJUE, G. Ch., 9 novembre 2010, *Volker und Markus Schecke GbR et Hartmut Eifert c. Land Hessen*, aff. C-92/09 et C-93/09, *p.* **83, 87, 105, 270, 273, 278, 281, 296, 306, 312, 321, 323, 332, 356, 364, 370, 379, 380, 449**

CJUE, 5 mai 2011, *Deutsche Telekom AG c. Bundesrepublik Deutschland.*, aff. C-543/09, *p.* **83**

CJUE, 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) et Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, aff. C-468/10 et C-469/10, *p.* **82**

CJUE, 24 novembre 2011, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, aff. C-70-10, *p.* **54, 83, 112, 350 à 353, 372, 379**

CJUE, 19 avril 2012, *Bonnier Audio AB et autres c. Perfect Communication Sweden AB*, aff. C-461/10, p. **350**

CJUE, G. Ch., 16 octobre 2012, *Commission européenne c. République d'Autriche*, aff. C-614/10, p. **454**

CJUE, 17 octobre 2013, *M. Schwarz c. Stadt Bochum*, aff. C-291/12, p.**148, 279, 280, 304, 322**

CJUE, G. Ch., 8 avril 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources et autres et Kärntner Landesregierung et autres*, aff. C-293/12 et C-594/12, p. **25, 62, 102, 105, 149, 176, 180, 203, 206, 236, 252, 262, 273, 279, 280, 281, 285, 299, 301, 303, 305, 307, 315, 355, 385, 392, 426**

CJUE, G. Ch., 8 avril 2014, *Commission européenne c. Hongrie*, aff. C-288/12, p. **93, 404, 405, 454**

CJUE, 13 mai 2014, *Google Spain SL et Google Inc. c. Agencia Española de Protección de* Datos (AEPD) et Mario Costeja González, aff. C-131/12 b , p. **261, 262, 335, 339, 340, 341, 376, 385, 417**

CJUE, 1 October 2015, Weltimmo s. r. o. v. Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14, p. **210**

CJUE, Gr. Ch, 6 octobre 2015, *Maximillian Schrems contre Data Protection Commissioner*, aff. C-362/14, p. **25, 62, 122, 185, 188, 189, 195, 198, 202 à 208, 215, 216, 236, 253, 258, 262, 263, 271, 304, 370, 371, 376, 385, 386, 404, 405, 455**

CJUE, Gr. Ch, 21 décembre 2016, *Tele2 Sverige* AB contre Post- och telestyrelsen et Secretary of State for the Home Department contre Tom Watson e.a. aff. jointes C-203/15 et C-698/15, p. **40, 83, 177, 253, 271, 273, 296, 298, 372,**

CJUE, Breyer, 19 octobre 2016, Patrick Breyer c. Bundesrepublik Deutschland, aff. C-582/14

CJUE, Gr. Cr. 26 juillet 2017, Opinion 1/15

CJUE, 4 mai 2017, Rīgas satiksme, aff. C-13/16

CJUE, 4 mai 2017, Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde c. Rīgas pašvaldības SIA 'Rīgas satiksme', aff.C-13/16

CJUE, 9 mars 2017, Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce c. Salvatore Manni, aff. C-398/15

CJUE, 20 décembre 2017, Nowak, aff. C-434/16

CJUE, 27 septembre 2017, Puškár, aff. C-73/16

CJUE, 25 janvier 2018, Maximilian Schrems c. Facebook Ireland Limited, aff. C-498/16

CJUE, 5 juin 2018, Unabhängiges Landeszentrum für Datenschut SchleswigHolstein/Wirtschaftsakademie Schleswig-Holstein GmbH, aff. C-210/16, **p. 439**

CJUE, 10 juillet 2018, Tietosuojavaltuutettu, aff. C-25/17

CJUE, Gr. Ch. 2 octobre 2018, *Ministerio Fiscal,* aff. C-207/16

<u>Affaires pendantes/ Conclusions Avocat général</u>

Conclusions de l'Avocat Général E. SHARPSTON, le 27 septembre 2018, Aff. C-345/17, *Sergejs Buivid c. Datu valsts inspekcija*

Demande de décision préjudicielle présentée par le Conseil d'État (France) le 21 août 2017 Google Inc. / Commission nationale de l'informatique et des libertés (CNIL), Affaire C-507/17

Demande de décision préjudicielle présentée par l'Augstākā tiesa (République de Lettonie) le 12 juin 2017 – Sergejs Buivids, Aff. C-345/17

Demande de décision préjudicielle présentée par le Conseil d'État (France) le 3 août 2018 – La Quadrature du Net, French Data Network, Fédération des fournisseurs d'accès à Internet associatifs, Igwan.net / Premier ministre, Garde des Sceaux, ministre de la Justice, Ministre de l'Intérieur, Ministre des Armées, Aff. C-511/18

Demande de décision préjudicielle, présentée le 15 mars 2017, G. C. e.a. (Déréférencement de données sensibles), Aff. C-136/17

Demande de décision préjudicielle présentée par le Conseil d'État (France) le 3 août 2018 – French Data Network, La Quadrature du Net, Fédération des fournisseurs d'accès à Internet associatifs / Premier ministre, Garde des Sceaux, ministre de la Justice, Affaire C-512/18

Demande de décision préjudicielle présentée par le Vilniaus apygardos administracinis teismas (Lituanie) le 26 juin 2018 – AW e.a., Affaire C-417/18

INDEX THÉMATIQUE

Les chiffres renvoient aux numéros de paragraphes

-A-

Adresse IP : 35, 175, 180

Autorités de protection des données personnelles / autorités de contrôle : 19, 20, 26, 49,74, 82, 83, 88,100,113,114, 117, 165, 182, 196 à 218, 220, 221, 223, 224, 225, 227 à 229

-B-

Biométrie : 38, 63, 85, 86, 88, 89, 90, 98, 153, 164, 168, 169, 206, 221

-C-

CEDH : 9, 33, 88, 132, 139, 141 à 146, 148, 150, 151, 152, 154, 156 à 158, 167, 168, 171 à 173, 176 à 178, 180, 184, 190, 191 à 194

CJUE :

CourEDH : 5 à 7, 17, 28, 47, 55, 86, 94, 139 à 148, 150 à 158, 165 à 167, 172 à 177, 180 à 183, 188 à 194, 210

Charte des droits fondamentaux de l'Union européenne (article 8) : 9,10,17,31, 83, 130, 182 à 184, 187, 188, 190

Commission nationale informatique et libertés (CNIL) : 79, 88, 208, 209

Contrôleur européen de la protection des données (CEPD) : 24, 50, 85, 88, 90, 95, 98, 130, 134, 143,180, 196, 203, 208, 211, 214, 218 à 225

Comité européen à la protection des données personnelles : 87, 457, 459

Consentement : 10, 12, 37, 47, 54, 66, **68 à 70**, 73, 77, 98, 109, 117, 121, 132, 134, 158, 168, 174, 184, 195, 208, 217, 222

-D-

Données biométriques v. *Biométrie*

Données sensibles : 26, 38, 63, 66, 73, 84, 97, 101, 126, 129, 130, 168, 188, 208, 217, 219

Droit d'accès 37, 45, 46, 68, 73,77, 92, 93, 100, 129, 148, 171, 174, 177, 184, 217, 221, 222, 224

Droit à l'oubli : 76 à 79, 116, 119, 121, 177, 190, 194

Droits fondamentaux (notion) : 2, 5, 9 à 19, 25, 26, 31 à 36, 39, 54, 58, 60, 64, 69, 74, 77, 83 à 85, 90, 93 à 95, 100, 103, 112 à 123, 126, 128, 130 à 132, 141 à 147, 160 à 162, 170, 171, 177, 178, 191 à 197, 200, 222, 225

-E-

Espace de liberté, de sécurité et de justice (ELSJ): 29, 31, 84 à 86, 91, 94, 96, 99, 101, 122, 134, 158, 183, 221, 224, 227

-F-

Fournisseurs d'accès à Internet : 153, 180

-G-

G 29 : 452,453, 455, 457

-I-

Internet des objets : 1, 61

-L-

Liberté d'expression : 316 à 327

-M-

Moteur de recherche : 40, 76, 77, 119, 120, 177, 108, 217

-N-

Nécessité (contrôle de nécessité) :283, 285, 287

-P-

PNR (données des passagers aériens) : 150, 213, 220, 223, 224

Proportionnalité (principe de proportionnalité) :287, 296, 301, 306

-R-

RGPD :21, 101, 102, 105, 127

-S-

Sécurité : 244, 245, 246, 250

Société civile : 414, 421

Système d'information Schengen : 85, 91, 98

-T-

Transparence : 1, 36, 54, 94, 112, 172, 174, 180, 187, 213, 216, 217, 222

-V-

Vie privée : 26,37,219,232,318,322,482

TABLE DES MATIÈRES

INTRODUCTION GÉNÉRALE 17

I - L'ORIGINE DU DROIT A LA PROTECTION DES DONNÉES PERSONNELLES 25
A. Le rattachement au droit au respect de la vie privée 28
B. L'autonomisation du droit à la protection des données personnelles 34
II - LA CONSTITUTIONNALISATION DU DROIT FONDAMENTAL À LA PROTECTION DES DONNÉES PERSONNELLES 46
A. Une protection étroitement liée au droit de la Convention 49
B. Le dialogue entre la Cour de justice et la CourEDH 54
III. L'ÉMERGENCE D'UN MODÈLE EUROPÉEN DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES 56
A. Le cadre législatif au sein de l'Union européenne 56
B. Une approche inhérente à l'identité européenne 64

PARTIE I. UNE EXTENSION PROGRESSIVE DU CHAMP DE LA PROTECTION 72

TITRE I. LA MUTATION INTERNE DU STANDARD DE PROTECTION 76
CHAPITRE I. LE RÉGIME DE PROTECTION DANS LE MARCHÉ INTÉRIEUR 80
Section I. Les sources du droit à la protection des données personnelles, expression législative hétérogène 81
§1. La directive 95/46 comme instrument pour la réalisation du marché intérieur 82
A. L'objet de la protection 83
1) Les principes directeurs 86
a) L'interprétation de la base légale pour le traitement 87
b) Les acteurs du traitement 90
2) Les droits des personnes concernées par un traitement 92
3) Des mécanismes de contrôle indépendants 94
B. Le Champ d'application territorial 96
§2. Les directives sur la vie électronique 98
A. La première législation en matière de communications électroniques 98
B. La directive « *Data Retention* » sur la conservation des données 101
1) Une base légale incertaine 102
2) L'invalidation de la Directive « *Data Retention* » 103
a) L'impact de l'invalidation de la directive « *Data Retention* » 104
b) Le respect du droit à la protection des données à caractère personnel dans la mise en œuvre du droit de l'Union. L'affaire *Tele2/ Watson* 106
Section II. La réforme. La troisième génération de règlementation 111
§1. Le champ d'application du règlement 679/16 113
A. Le champ d'application matériel 114
1) Les exclusions d'application relevant de la répartition des compétences 116
2) Les exclusions d'application relevant du type de traitement 116
3) L'exclusion d'application relevant du traitement de certaines catégories de données personnelles 116
B. Le champ d'application territorial 117
§2. Des nouveaux droits et principes 119
A. Le renforcement des droits existants et l'élaboration des nouveaux droits 119
B. Les nouvelles mesures de conformité 134
CHAPITRE II. LE RÉGIME DE PROTECTION DANS L'ELSJ 141
Section I. L'approche européenne entre protection des droits fondamentaux et sécurité publique 145
§1. L'identification de différentes formes d'échange de données dans l'ELSJ 148

A. Les systèmes d'information en matière d'asile et d'immigration....152
1) Le système d'espace Schengen (SIS)....152
2) Le système d'information sur les visas (VIS)....155
B. Le système d'information en matière de coopération policière....156
§2. Le traitement des données personnelles par les agences européennes....158
A. Le traitement de données personnelles par Europol....159
B. Le traitement des données par Eurojust....163
C. Le traitement des données par Frontex....165
Section II. La réforme dans l'ELSJ....166
§1. Les limites du cadre juridique préexistant....167
A. Des difficultés découlant de la base juridique....167
B. Les difficultés découlant des lacunes de la décision-cadre 2008/977 JAI....169
§2. Le nouveau cadre juridique....170
A. La directive 680/2016 relative à la protection des données à caractère personnel traitées à des fins pénales....172
B. La directive PNR relative à l'utilisation des données des dossiers passagers pour la prévention et la détection des infractions terroristes et des formes graves de criminalité 174
TITRE II. LA PROJECTION INTERNATIONALE DU STANDARD EUROPÉEN DE PROTECTION....181
CHAPITRE I. L'EXTRATERRITORIALITÉ DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES DANS LES RELATIONS COMMERCIALES....183
Section I. Les instruments juridiques permettant le transfert des données personnelles vers des États tiers....186
§1. La décision d'adéquation de la Commission européenne. Condition pour le transfert des données personnelles vers des États tiers....188
A. La décision « d'adéquation » de la Commission européenne....188
B. Du niveau de protection « adéquat » au niveau « substantiellement équivalent » 194
§2. Les instruments de droit privé comme « garanties suffisantes » pour le transfert....196
A. Les clauses contractuelles....197
B. Les codes de conduites et certifications....201
Section II. Les données personnelles, objet d'une politique économique étrangère de l'Union européenne....202
§1 Le bras de fer entre les États-Unis et l'Union européenne....202
A. L'exportation du modèle européen de protection....204
B. Le « *Privacy Shield* ». Un accord de compromis....207
§2. L'extraterritorialité à l'ère du numérique....209
A. « L'affaire *Google Spain* ». L'extension du champ de protection....210
B. La codification de l'extraterritorialité dans le RGPD....213
CHAPITRE II. L'EXTRATERRITORIALITÉ DU DROIT À LA PROTECTION DES DONNÉES PERSONNELLES DANS LE CONTEXTE DE CRISE SÉCURITAIRE...221
Section I. La politique étrangère de sécurité de l'Union européenne. La conclusion d'accords sur la surveillance des données de voyage « PNR »....224
§1. Les accords « PNR » avec les États-Unis....225
A. L'invalidation de la « décision d'adéquation » de la Commission par la Cour de justice....226
B. L'élaboration d'un nouvel accord PNR avec les États-Unis....231
§2. Des conséquences sur le plan des autres négociations....233
A. L'accord PNR avec l'Australie....234
B. L'accord PNR échoué avec le Canada....235
1) Des conséquences sur le plan interne....240
2) Des conséquences sur le plan externe....241

Section II. La politique étrangère de sécurité de l'Union européenne. La conclusion d'accords sur la surveillance des données financières 242
§1. La création du *Terrorist Finance Traking Program* (« TFTP ») 244
A. Le premier accord « TFTP » 247
B. Le nouvel accord « TFTP » 249
§2. La spécificité du modèle de protection européen 251
A. La surveillance dans la jurisprudence de l'Union européenne 254
B. La surveillance dans la jurisprudence de la CourEDH 256

PARTIE II. UNE ARTICULATION COMPLEXE DU RÉGIME DE PROTECTION 267

TITRE I. LA SYSTÉMATISATION D'UNE PROTECTION JURIDICTIONNELLE 271
CHAPITRE I. UNE DOUBLE PROTECTION JURIDICTIONNELLE 273
Section I. La légitimité de l'ingérence selon un contrôle formel et matériel 277
§1. La légitimité de l'ingérence selon un contrôle formel 279
A. L'existence d'une base légale 280
B. La poursuite d'un but légitime 283
1) La sécurité nationale comme intérêt général 286
2) Le développement économique comme restriction relevant de l'intérêt général 288
3) Des motifs d'ordre sanitaire invoqués comme motifs d'intérêt général 289
§2. La légitimité de l'ingérence selon un contrôle matériel 294
A. L'appréciation sur la proportionnalité de la mesure par la CourEDH 296
1) Un besoin social impérieux 297
2) Des motifs pertinents et suffisants 298
B. L'appréciation sur la proportionnalité de la mesure par la Cour de justice 298
1) Le respect du contenu essentiel du droit fondamental à la protection des données personnelles « limite aux limites » 300
a) La non violation du contenu essentiel 301
b) La violation du contenu essentiel du droit à la protection des données personnelles 305
2) L'intensité du test de proportionnalité 307
a) Le contrôle réduit de proportionnalité 312
b) Un contrôle renforcé 317
Section II. Les limites dérivant des interactions avec d'autres droits et intérêts légitimes 326
§1. La pondération avec le droit à la liberté d'expression 327
A. La conciliation avec la liberté d'expression dans la presse 329
1) Des exceptions renforçant la liberté d'expression 332
2) Le principe de transparence comme limite au droit à la protection des données personnelles 334
B. La liberté d'expression sur Internet 337
§2. La pondération avec le droit à la propriété intellectuelle 347
A. Le droit à la protection des données personnelles face au droit de propriété 348
B. Le droit à la protection des données personnelles face à la propriété intellectuelle 351
CHAPITRE II. L'AUTONOMISATION DU STANDARD DE PROTECTION 362
Section I. Une protection spécifique inscrite dans le droit primaire de l'Union européenne 364
§1. Une nouvelle base juridique 366
A - L'influence de l'article 8 de la Charte sur l'évolution constitutionnelle de l'Union européenne 367
B – L'influence de l'article 16 du TFUE sur les compétences de l'Union européenne .369

§2. L'influence de l'article 8 de la Charte sur le contrôle « constitutionnel » opéré par la Cour de justice 372
A. Le contrôle constitutionnel à travers le renvoi préjudiciel 373
B. Le contrôle constitutionnel de la Cour de justice vis-à-vis des actes externes de l'Union 377
Section II. L'émancipation du raisonnement de la CJUE à l'égard de la CEDH 380
§1. Une autonomisation graduelle 381
A. La redevance vis-à-vis de la jurisprudence de la CEDH 381
B. Le dialogue constant des juges 383
§2. Des arrêts historiques confirmant l'autonomisation de la Cour de justice 386
A. La Charte comme norme de référence 386
B. La cristallisation de la jurisprudence de la Cour de justice 389
TITRE II. L'ADJONCTION D'UNE PROTECTION NON- JURIDICTIONNELLE 397
CHAPITRE I. LA PROTECTION NON-JURIDICTIONNELLE AU SEIN DES ÉTATS MEMBRES 399
Section I. Le rôle des autorités nationales de protection des données personnelles 401
§1. La nature juridique des autorités de contrôle 403
A. L'indépendance des autorités nationales de protection 404
1) L'impartialité comme expression d'indépendance 405
2) L'étendue du mandat comme expression d'indépendance 408
B. Une indépendance limitée 410
§2. La mise en œuvre du droit à la protection des données personnelles par les autorités de contrôle indépendantes nationales 412
A. Des pouvoirs consultatifs 413
B. Des pouvoirs de contrainte 415
1) Le pouvoir d'investigation et intervention 416
a) La mise en œuvre territoriale du droit au déréférencement 419
b) La mise en œuvre matérielle du droit au déréférencement 420
2) Le Pouvoir d'être saisies d'une demande et d'ester en justice 423
3) La compétence de l'autorité chef de file et la coopération avec les autres autorités de contrôle 425
Section II. Des actions de sensibilisation à l'égard du droit à la protection des données personnelles 427
§1. Le rôle de la société civile 428
A. La participation croissante de la société civile à l'application des règles 429
B. La participation insuffisante de la société civile à l'élaboration des règles 431
§2. Les autres acteurs du droit à la protection des données personnelles 434
A. Le délégué à la protection des données 435
B. Le responsable du traitement 437
CHAPITRE II. LA PROTECTION NON-JURIDICTIONNELLE AU SEIN DE L'UNION EUROPÉENNE 444
Section I. Le Contrôleur européen à la protection des données personnelles 445
§1. Une autorité de contrôle indépendante de plus en plus influente 446
A. Composition et fonctionnement 447
B. La justification de son existence dans la mise en œuvre du règlement 45/2001 par les institutions 449
§2. Les missions du Contrôleur européen à la protection des données 453
A. Une mission de conseil 453
B. Une mission de contrôle 458
Section II. Le Groupe de travail (G29) 461
§1 Le rôle transgouvernemental joué par le G29 dans la protection des données. 461
A. Le pouvoir d'initiative du G29 dans la mise en œuvre de la directive 95/46 462
B. La valeur juridique des avis et recommandations du G29 464
§2 L'institutionnalisation du rôle du G29 466

A. Des compétences élargies 467
B. Un pouvoir contraignant 468

BIBLIOGRAPHIE 480

TABLE DE JURISPRUDENCE 511

INDEX THÉMATIQUE 518

TABLE DES MATIÈRES.....520