SCUOLA DOTTORALE INTERNAZIONALE
"TULLIO ASCARELLI"
Diritto – Economia – Storia

SEZIONE "diritto europeo su base storico comparatistica"

XVII° Ciclo

"LA PROTEZIONE DEI DATI PERSONALI E IL BILANCIAMENTO CON ALTRI DIRITTI PERSONALI NEL DIRITTO DELL'UNIONE EUROPEA"

Ch.mo Prof. Giandonato Caggiano
Tutor

Ilenia Italiano
Dottoranda

Ch.mo Prof. Lorenzo Fascione
Coordinatore

Anno Accademico 2014-2015

INDICE

Premessa p. 6

Riflessioni introduttive sulla tutela dei diritti fondamentali

1. I diritti fondamentali alla privacy e alla protezione dei dati personali p. 8
2. Concetto e definizione p. 11
3. L'evoluzione della giurisprudenza della Corte di giustizia p. 12
4. L'evoluzione della giurisprudenza della Corte EDU p. 13
5. La tematica generale del bilanciamento della Corte di giustizia p. 14
6. *Segue*: della Corte EDU p. 15

Parte I
Il bilanciamento degli interessi da parte del legislatore dell'Unione

Cap. I Definizioni e inquadramento giuridico

1. La Convenzione n. 108 del Consiglio d'Europa p. 21
2. Le basi giuridiche del Trattato di Lisbona p. 22
3. La direttiva 95/46/CE p. 23
4. Il ruolo della direttiva 95/46/CE dalla sentenza *Lindqvist* p. 25
5. La direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche, modificata dalla direttiva 2009/136/C p. 27
6. La direttiva *data retention* p. 29
7. La decisione-quadro 2008/977/GAI p. 31
8. La direttiva 2013/40/UE relativa agli attacchi contro i sistemi d'informazione p. 34

Cap. II La riforma della normativa generale nel mercato interno

1. La riforma secondo l'impostazione della Commissione p. 38
2. Sussidiarietà, destinatari, beneficiari e poteri esecutivi p. 40
3. Lo status del responsabile del trattamento p. 42
4. Le deroghe ammissibili p. 43
5. Ricorsi e risarcimento danni p. 44
6. Proporzionalità e rischi con particolare riferimento alle PMI p. 44
7. La manifestazione del consenso del soggetto interessato p. 46
8. La specifica situazione del consenso per alcune categorie di dati (*opt-out*) p. 47
9. Conservazione e informativa sui dati p. 48
10. Rettifica e oblio p. 50
11. Principali emendamenti del Parlamento europeo in prima lettura sulla proposta di regolamento p. 52

Parte II
La giurisprudenza della Corte di Strasburgo

Cap. I Il bilanciamento con l'interesse pubblico alla sicurezza

1. I dati personali conservati dai servizi d'*intelligence*:
   a) *Rotaru v. Romania* p. 56
   b) *Haralambie v. Romania* p. 58
   c) *Turek v. Slovakia* p. 58
   d) *Segerstedt-Wiberg and O. v. Sweden* p. 60
   e) *Shimovolos v. Russia* p. 62
2. La conservazione del DNA: p. 64
   a) *S. and Marper v. United Kingdom* p. 65
   b) *Peruzzo and Martens v. Germany* p. 68
3. La conservazione dei dati in speciali banche dati:
   a) *Bouchacourt*, *Gardel e M.B. v. France* p. 69
   b) *Khelili v. Switzerland* p. 70
   c) *M.K. v. France* p. 71
   d) *Dalea v. France* p. 71
   e) *E.B v. Austria* p. 72
   f) *Bernh Larsen v. Norway* p. 74
4. Controlli e videosorveglianza:
   a) *Peck v. the United Kingdom* p. 76
   b) *Vetter v. France* p. 77
   c) *Kopke v. Germany* p. 78
   d) *Van Vondel v. Netherlands* p. 80

Cap. II Il bilanciamento con la tutela della salute

1. *Armonienė v. Lithuania* p. 83
2. *Gillberg v. Sweden* p. 84
3. *Avilkina and others v. Russia* p. 86

Cap III Il Bilanciamento con la libertà di espressione e il diritto alla reputazione

1. *Von Hannover v. Germany* p. 88
2. *Axel Springer AG v. Germany* p. 89
3. *Mosley v. United Kingdom* p. 90
4. *Nagla v. Latvia* p. 91

Parte III
La giurisprudenza della Corte di giustizia

Cap. I L'esercizio di poteri pubblici
1. *Österreichischer Rundfunk* p. 94
2. *Huber* p. 96
3. *YS* p. 100

Cap. II Le autorità indipendenti di controllo sui dati
1. *Commissione c. Germania* p. 102
2. *Commissione c. Austria* p. 103
3. *Commissione c. Ungheria* p. 104

Cap. III Accesso agli atti
1. *Volker und Markus Schecke* p. 107
2. *Commissione c. Bavarian Lager* p. 108

Cap. IV Altre questioni interpretative della direttiva 95/46/CE
1. *Asociación Nacional de Establecimientos Financieros de Crédito* p. 111
2. *Deutsche Telekom AG* p. 112
3. *Institut immobiliere* p. 113
4. *Ryneš* p. 114

Parte IV
Profili specifici di internet

Cap. I Giurisprudenza della Corte di Strasburgo
1. Introduzione p. 119
   a) *KU v. Finland* p. 119
   b) *Editorial Board di Pravoye Delo e Shtekel v. Ukraina* p. 120
   c) *Ahmet Yildirim v. Turkey* p. 121
   d) *Animal Defenders International v. United Kingdom* p. 121
   e) *Delfi AS v. Estonia* p. 123
   f) *Times Newspapers Limited v. United Kingdom (n. 1 e 2)* p. 126
   g) *Ashby Donald e Neij e Sunde Kolmisoppi* p. 127
   h) *Węgrzynowski and Smolczewski v. Poland* p. 129

Cap. II Giurisprudenza della Corte di giustizia

1. *SABAM* p. 133
2. *Promusicae* p. 135
3. *UPC Telekabel Wien* p. 136
4. *Digital Rights* p. 137
5. *Google Spain* p. 142

Bibliografia

Manuali e monografie p. 149
Articoli p. 150

PREMESSA

Il titolo e l'oggetto di questa tesi è "la protezione dei dati personali e il bilanciamento con altri diritti personali nel diritto dell'Unione europea".

La questione generale approfondita nella presente tesi è quella del bilanciamento (ponderazione o verifica dell'equilibrio) con gli altri interessi e diritti protetti a livello pubblico o privato, in relazione alla necessità delle limitazioni o finalità (principio di proporzionalità).

La prospettiva dei diritti e degli interessi in gioco è esaminata mediante l'esame del bilanciamento effettuato dal legislatore dell'Unione e dalle due Corti europee. Al riguardo, analizzeremo la giurisprudenza della Corte di Strasburgo, in riferimento all'interesse pubblico alla sicurezza, la tutela della salute, la libertà di espressione e il diritto alla reputazione. Per la giurisprudenza della Corte di giustizia, saranno oggetto di approfondimento il ruolo delle autorità indipendenti di controllo sui dati, l'accesso agli atti, il diritto d'autore.

Una parte della tesi sarà dedicata alle questioni specifiche poste da internet davanti alle due Corti europee. Un'attenzione specifica sarà dedicata alle sentenze di annullamento della direttiva *data retention* e sul diritto all'oblio di *Google Spain*. Quest'ultima riguarda il bilanciamento fra il diritto alla libertà di espressione e il diritto alla libertà di impresa su internet in relazione all'attività dei motori di ricerca che ne potenziano l'utilizzo.

Riflessioni introduttive sulla tutela dei diritti fondamentali

– 1. I diritti fondamentali alla privacy e alla protezione dei dati personali. – 2. Concetto e definizione. – 3. L'evoluzione della giurisprudenza della Corte di giustizia. – 4. L'evoluzione della giurisprudenza della Corte EDU. – 5. La tematica generale del bilanciamento della Corte di giustizia. – 6. *Segue*: della Corte EDU.

1. Il diritto al rispetto della vita privata ed il diritto al trattamento dei propri dati personali sono ormai inseriti nel diritto primario dell'Unione europea (sono in altri termini "costituzionalizzati") dagli articoli 7 ed 8 della Carta dei diritti fondamentali dell'UE.

Tra le due previsioni normative, l'art. 8 della Carta presenta una maggiore portata innovativa perché introduce l'autonomia del principio della "protezione dei dati personali" rispetto a quello della protezione della privacy. Anche se le Spiegazioni allegate all'art. 8 sembrano voler restringere la portata della norma in parola ad una mera riproposizione dell'*acquis*, il carattere innovativo della norma appare evidente soprattutto nella giurisprudenza più recente[1]. Infatti, l'autonomia del "diritto alla protezione dei dati personali" determina il superamento dell'esclusività della protezione di tali dati nella dimensione del mercato interno a favore di una dimensione che può anche riguardare il diritto della persona. La medesima norma determina inoltre un ruolo para-costituzionale dei Garanti nazionali per la protezione dei dati personali che costituiscono l'unica tipologia di autorità indipendente nazionale citata dalla Carta.

Il diritto alla protezione dei dati personali rientra pertanto nel diritto dell'Unione tra i diritti della personalità, quali il diritto di rettifica, il diritto alla riservatezza, il diritto alla reputazione, il diritto all'immagine e il diritto al nome, tutelando il bene giuridico dell'identità personale. Quest'ultima è intesa nelle sue varie forme ed espressioni: le informazioni, l'immagine sociale, l'immagine sui media, ecc.

All'interno della categoria dei diritti personali, si può affermare che: il diritto all'identità personale consiste nel diritto di vietare un travisamento dell'immagine sociale di un soggetto; il diritto di rettifica comporta una forma di controllo sull'immagine sociale di un soggetto e il diritto di richiedere la correzione delle pubblicazioni scorrette o false; il diritto alla riservatezza comporta un controllo del soggetto sulle vicende e sulle informazioni che lo riguardano; il diritto alla reputazione tutela la stima sociale di un soggetto; il diritto al nome va inteso come

[1] Nelle Spiegazioni all'art. 7 si legge che "I diritti di cui all'art. 7 corrispondono a quelli garantiti dall'art. 8 della CEDU. Per tener conto dell'evoluzione tecnica, il termine comunicazioni è stato sostituito a corrispondenza. Conformemente all'art. 52, par. 3, il significato e la portata di questi diritti sono identici a quelli del corrispondente articolo della CEDU. Le limitazioni che vi possono legittimamente essere apportate sono pertanto quelle autorizzate ai sensi del suddetto art. 8".
All'art. 8: "Questo articolo si fonda sull'art. 286 del Trattato che istituisce la Comunità europea, sulla direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati , in *GU* L 281 del 23 novembre 1995, nonché sull'art. 8 della CEDU e sulla Convenzione del Consiglio d'Europa sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale del 28 gennaio 1981, ratificata da tutti gli Stati membri. Il diritto alla protezione dei dati personali si esercita alle condizioni previste dalla suddetta direttiva e può essere limitato alle condizioni previste dall'art. 53 della Carta".

strumento di identificazione di un soggetto; il diritto all'immagine può anche essere inteso come tutela dell'immagine sociale, oltre che dell'immagine fisica di un soggetto. L'identità personale è la sintesi dei tanti elementi di natura diversa che muta col tempo.

Uno dei diritti che può entrare in conflitto con il diritto alla protezione dei dati è il diritto alla libertà di espressione. La libertà di espressione è sancita dall'art. 11 della Carta che include la "libertà di opinione e la libertà di ricevere o di comunicare informazioni o idee senza che vi possa essere ingerenza da parte delle autorità pubbliche e senza limiti di frontiera". L'art. 11 corrisponde all'art. 10 della CEDU[2]. Le limitazioni che possono legittimamente essere imposte al diritto garantito dall'art. 11 della Carta non possono pertanto andare oltre quelle previste all'art. 10, par. 2, della CEDU, vale a dire, devono essere previste dalla legge e devono essere necessarie in una società democratica "(…) alla protezione della reputazione o dei diritti altrui".

Il rapporto tra la protezione dei dati personali e la libertà di espressione è disciplinato anche nel diritto secondario dall'articolo 9 della direttiva 95/46/CE , intitolato "Trattamento di dati personali e libertà d'espressione", in base al quale gli Stati membri sono chiamati a prevedere determinate deroghe o limitazioni alle disposizioni in materia di tutela dei dati, e quindi del diritto alla vita privata, previste nei capi II, IV e VI di detta direttiva. E' consentito applicare tali deroghe esclusivamente per scopi giornalistici o di espressione artistica o letteraria, rientranti nel diritto fondamentale della libertà d'espressione, soltanto nei limiti in cui esse risultino necessarie per conciliare il diritto alla vita privata con le norme che disciplinano la libertà d'espressione.

Per la CEDU, la Corte di Strasburgo introduce a partire dal 1987, con un'interpretazione evolutiva, la raccolta e il trattamento di dati personali nell'ambito di applicazione dell'art. 8 CEDU[3]. La Corte ne approfondisce la portata espansiva, in relazione al concetto di vita privata[4]. Successivamente, la Corte riprendeva tale interpretazione estensiva, ma questa volta collegata al "nuovo" elemento

---

[2] Ai sensi dell'art. 52, par. 3, della Carta, nella misura in cui prevede diritti corrispondenti a quelli garantiti dalla CEDU, "il significato e la portata degli stessi sono uguali a quelli conferiti dalla suddetta Convenzione".

[3] *Leander v. Sweden*, 26 March 1987, Series A no. 116.

[4] In particolare: "The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of "private life". However, it would be too restrictive to limit the notion to an "inner circle" in which the individual may live his own personal life as he chooses and to exclude therefrom entirely the outside world not encompassed within that circle. Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings. There appears, furthermore, to be no reason of principle why this understanding of the notion of "private life" should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest, opportunity of developing relationships with the outside world", v. *Niemietz v. Germany*, 16 December 1992, Series A no. 251-B, § 29.

tecnologico degli elaboratori di dati e alla necessaria tutela, facendo leva su un parametro esterno alla CEDU, vale a dire sulla Convenzione del Consiglio d'Europa n. 108/1981 relativa alla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale[5].

La Corte di Strasburgo, nel ribadire che la libertà di informazione comprende la libertà di ricevere informazioni e idee e la libertà di comunicarle, ha garantito la tutela di diversi supporti utilizzati a tali fini, sia di tipo tradizionale sia tecnologico[6], tra cui anche le pubblicazioni elettroniche. La Corte ha, infatti, sottolineato che l'art. 10 della Convenzione non concerne solamente il contenuto delle informazioni, bensì anche i mezzi di trasmissione, poiché le restrizioni che concernono i mezzi incidono anche sulla libertà di ricevere e comunicare le informazioni.

La necessità di garanzie è maggiore se la protezione dei dati personali riguarda scopi di polizia, secondo l'art. 5 della Convenzione n. 108 sulla protezione dei dati e il principio 7 della Raccomandazione R (87) 15 del Comitato dei Ministri. La normativa deve garantire che tali dati siano pertinenti e che non eccedano le finalità per cui sono memorizzati; inoltre devono essere conservati in una forma che consenta l'identificazione dell'interessato per un periodo non superiore a quello necessario per le finalità in base alle quali sono registrate. La normativa dovrebbe contenere altresì garanzie adeguate per evitare l'uso improprio e l'abuso dei dati personali conservati.

La Corte ha avuto l'opportunità di stabilire alcuni principi che regolano la conservazione dei dati personali. L'ingerenza è considerata "necessaria in una società democratica" per il raggiungimento di uno scopo legittimo, se risponde ad un "bisogno sociale imperativo" e, soprattutto, se è proporzionata allo scopo legittimo perseguito e se le ragioni addotte dalle autorità nazionali per giustificarla appaiano "pertinenti e sufficienti". Se inizialmente rientra nella discrezionalità delle autorità nazionali provare che tali condizioni siano soddisfatte, è responsabilità della

---

[5] *Amann v. Switzerland* [GC], no. 27798/95, ECHR 2000-II: "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 is "to secure in the territory of each Party for every individual [...] respect for his rights and fundamental freedoms, and in particular his right to privacy, Wight regard to automatic processing of personal data relating to him (Article 1), such personal data being defined as "any information relating to an identified or identifiable individual (Article 2)".

[6] V. S. BARTOLE, P. DE SENA, V. ZAGREBELSKY, *Commentario breve alla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali*, Padova, 2012, p. 10. In particolare si fa riferimento ai libri (*Handyside v. the United Kingdom*, 7 December 1976, Series A no. 24); alle opere d'arte (*Müller and Others v. Switzerland*, 24 May 1988, Series A no. 133); ai film (*Otto-Preminger-Institut v. Austria*, 20 September 1994, Series A no. 295-A); alle caricature (*Leroy v. Belgium*, no. 52098/99, 15 July 2005); ai video (*Wingrove v. the United Kingdom*, 25 November 1996, *Reports of Judgments and Decisions* 1996-V); ai pieghevoli di informazione (*Open Door and Dublin Well Woman v. Ireland*, 29 October 1992, Series A no. 246-A); ai manifesti (*Mouvement raëlien suisse v. Switzerland*, no. 16354/06, 13 January 2011); ai volantini di propaganda (*Hoffer and Annen v. Germany*, nos. 397/07 and 2322/07, 13 January 2011).

Corte decidere definitivamente la questione della necessità dell'ingerenza con i requisiti della Convenzione.

Si deve riconoscere a questo riguardo una certa discrezionalità alle autorità nazionali competenti. L'entità di questo margine è variabile e dipende da una serie di fattori tra cui la natura del diritto in questione garantito dalla Convenzione, la sua importanza per l'individuo, la natura dell'ingerenza e lo scopo di quest'ultima. In caso sia in gioco un aspetto particolarmente importante della vita o dell'identità di un individuo, il margine concesso allo Stato è limitato. Quando tuttavia non vi è consenso tra gli Stati membri del Consiglio d'Europa, sia sull'importanza degli interessi coinvolti che sul miglior modo di tutela, il margine di apprezzamento risulta più ampio.

2. La nozione di "dati personali" è particolarmente ampia nel diritto dell'Unione. La Corte di giustizia ha precisato che comprende, per esempio, "il nome di una persona accostato al suo recapito telefonico o ad informazioni relative alla sua situazione lavorativa o ai suoi passatempi"[7], il suo indirizzo[8], i suoi periodi di lavoro e di riposo nonché le relative interruzioni o pause[9], gli stipendi corrisposti da taluni enti ed i loro beneficiari[10], i dati sui redditi da lavoro e da capitale nonché sul patrimonio delle persone fisiche[11], le banche dati sugli stranieri presenti sul territorio[12]. Nei limiti in cui le informazioni riguardano una persona fisica identificata o identificabile, il loro contenuto può riguardare tutti gli aspetti relativi alla vita privata o professionale in una sfera pubblica[13]. La forma può essere scritta, sonora o visiva[14].

Un'altra nozione importante è quella della nozione di "flusso transfrontaliero dei dati" che riguarda la comunicazione diretta "a destinatari specifici". Da questo concetto, è esclusa la semplice pubblicazione *on line* (di dati personali) quali i registri pubblici o i mezzi di comunicazione di massa (giornali elettronici e televisione).

Agli albori di internet, nella sentenza *Bodil Lindqvist*, la Corte di giustizia ha statuito che "l'operazione consistente nel fare riferimento, in una pagina Internet, a

---

[7] Sentenza della Corte di giustizia del 6 novembre 2003, *Bodil Lindqvist c Svezia*, causa C-101/01, in *Racc*., p. I-12971, par. 24.

[8] Sentenza del maggio 2009, *College van burgemeester en wethouders van Rotterdam c. M. E. E. Rijkeboer*, causa C-553/07, in *Racc*., p. I-3889, paragrafi 42 e 62.

[9] Sentenza del 30 maggio 2013, *Worten*, causa C-342/12, non ancora in *Racc*, paragrafi 19 e 22.

[10]Sentenza 20 maggio 2003, *Österreichischer Rundfunk e a.*, cause riunite C-465/00, C-138/01 e C-139/01, in *Racc.*, p. I-4989, par. 64.

[11] V. *Satakunnan Markkinapörssi e Satamedia*, cit., paragrafi 35 e 37.

[12] V. sentenza del 16 dicembre 2008, *Huber*, causa C-524/06, in *Racc.,* p. I-09705, paragrafi 20 e 43.

[13]V. sentenza del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, causa C-92/09 e C-93/09, in *Racc*., p. I-11063, par. 59; v. altresì conclusioni dell'Avvocato generale Jääskinen nella causa C-131/12, *Google Spain* e *Google*, cit., par. 118.

diverse persone e nell'identificarle vuoi con il loro nome, vuoi con altri mezzi, ad esempio indicando il loro numero di telefono o informazioni relative alla loro situazione lavorativa e ai loro passatempo, costituisce "un trattamento di dati personali interamente o parzialmente automatizzato (…)". Tuttavia, la Corte ha poi sottolineato che vi sono norme specifiche che mirano a garantire un controllo da parte degli Stati membri sui trasferimenti di dati personali verso paesi terzi. Tenuto conto, da una parte, dello sviluppo iniziale di Internet all'epoca della redazione della direttiva 95/46/CE e, dall'altra, della mancanza nella stessa direttiva di criteri applicabili all'uso di Internet, la Corte concludeva che "non si può presumere che il legislatore comunitario avesse l'intenzione di includere prospettivamente nella nozione di trasferimenti verso un paese terzo di dati personali l'inserimento (...) di dati in una pagina Internet, anche se questi sono così resi accessibili alle persone di paesi terzi in possesso dei mezzi tecnici per consultarli"[15].

3. In un primo periodo della sua giurisprudenza sulla Carta, la Corte di giustizia si riferisce alla protezione della privacy con un riferimento spesso cumulativo agli articoli 7 e 8 senza riconoscere l'autonomia del "diritto alla protezione dei dati personali" rispetto al "diritto al rispetto della vita privata". Inoltre, sino al momento in cui è emersa la questione delle limitazioni consentite ai diritti previsti dagli articoli 7 e 8, con riferimento all'applicazione dell'art. 52 Carta, la Corte non ha distinto il profilo relativo all'applicazione del principio di proporzionalità, da quello riguardante la violazione dei "contenuti essenziali" dei diritti in gioco.

In questo senso particolarmente significativo è il ragionamento della Corte nella sentenza *Volker* del 2010[16]. Infatti si deve ritenere che, da un lato, il rispetto del diritto alla vita privata con riguardo al trattamento dei dati personali sia riferito ad ogni informazione relativa ad una persona fisica identificata o identificabile; dall'altro, che le limitazioni che possono essere legittimamente apportate al diritto alla protezione dei dati personali corrispondano a quelle tollerate nell'ambito dell'art. 8 della CEDU. .Il riferimento all'art. 8 della CEDU sottolinea come il diritto alla protezione dati sia considerato semplicemente quale accessorio rispetto al diritto al rispetto alla vita privata previsto dall'art. 7 della Carta.

La conservazione dei dati può costituire una limitazione del diritto al rispetto della vita privata e del diritto alla protezione dei dati personali. In parallelo con l'art. 8, par. 2, della CEDU, la Carta riconosce che l'ingerenza di un'autorità pubblica nell'esercizio del diritto al rispetto della vita privata può essere giustificata se

[15] Altrimenti, qualora la direttiva "venisse interpretata nel senso che si configura un trasferimento verso un paese terzo di dati personali ogni volta che dati personali vengono caricati su una pagina Internet, tale trasferimento sarebbe necessariamente un trasferimento verso tutti i paesi terzi in cui esistono i mezzi tecnici necessari per accedere ad Internet. Il regime speciale previsto [dalla direttiva] diverrebbe quindi necessariamente, per quanto riguarda le operazioni su Internet, un regime di applicazione generale. Infatti, non appena la Commissione constatasse (...) che un solo paese terzo non garantisce un livello di protezione adeguato, gli Stati membri sarebbero tenuti ad impedire qualsiasi immissione su Internet di dati personali".
[16] V. *Volker*, cit., par. 52.

necessaria alla sicurezza nazionale, alla pubblica sicurezza e alla prevenzione dei reati.

In particolare, ai sensi dell'art. 52, par. 1 della Carta, tali limitazioni devono "essere previste dalla legge e rispettare il contenuto essenziale di detti diritti […] nel rispetto del principio di proporzionalità", ed essere necessarie e rispondere a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui. In pratica, ciò significa che le eventuali limitazioni devono essere: formulate con precisione e prevedibilità; necessarie per realizzare una finalità di interesse generale o per proteggere i diritti e le libertà altrui; proporzionate alla finalità perseguita; conformi al contenuto essenziale dei diritti fondamentali in questione.

Pertanto, la protezione dei dati personali prevista dall'obbligo prescritto dall'art. 8, par. 1 della Carta risulta particolarmente importante per il diritto al rispetto della vita privata di cui all'art. 7 della stessa Carta.

4. La Convenzione di Roma per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (CEDU) stabilisce un elevato livello di protezione dei dati personali. Secondo l'art. 8, ogni persona è titolare del diritto al rispetto della sua vita privata e familiare, del suo domicilio e della sua corrispondenza. Sulla base di un'interpretazione estensiva della nozione di "vita privata", sono stati individuati dalla Corte europea principi o diritti propri della materia.

In base alla giurisprudenza della Corte EDU, la protezione dei dati ex art. 8 CEDU ha ad oggetto il loro trattamento, che può comprendere diverse operazioni (raccolta, registrazione, conservazione, impiego, trasferimento, divulgazione, rettifica o cancellazione). Il trattamento deve essere compiuto nel rispetto dei principi di legalità, legittimità, temporaneità e proporzionalità. Per ciò che attiene alle limitazioni ammissibili, il requisito fondamentale è la "prevedibilità" e "accessibilità" della legge.

L'accertamento di una violazione può dipendere da fattori, quali la qualità, la modalità e la tipologia dei dati e dal diritto di esercitare il diritto di accesso e dalla possibilità di richiesta, di rettifica e cancellazione da parte del soggetto interessato. Sono ammissibili deroghe relative alla sicurezza nazionale o alla prevenzione o alla repressione del crimine. Una particolare categoria è costituita dai dati sensibili (ad esempio stato di salute ed origini etniche) che richiedono specifiche garanzie per evitare qualsiasi forma di discriminazione.

Per quanto riguarda la possibilità di interpretare estensivamente la nozione di vita privata la Corte ha più volte ribadito che "Private life is a broad term not susceptible to exhaustive definition"[17]. La Corte ha più volte statuito che elementi quali il sesso, il nome, l'orientamento sessuale e la vita sessuale sono elementi importanti della

[17] *Peck v. the United Kingdom*, no. 44647/98 (Sect. 4), ECHR 2003-I- (28.1.03), § 57.

sfera personale (ex art. 8 CEDU). Vi è però anche una zona di interazione di una persona con gli altri, anche in un contesto pubblico, che può rientrare nell'ambito dell'applicazione della "vita privata". Il diritto di identità e sviluppo personale e il diritto di stabilire e sviluppare relazioni con altri esseri umani può persino consentire di estendere l'ambito di applicazione alle attività di natura professionale o commerciale. Nella nozione di "vita privata" non possono neanche essere escluse le attività di natura professionale o commerciale.

Tra le prime sentenze della Corte in materia vanno ricordate le sentenze *Leander*[18] e *Amann*[19]. La Corte ha ivi riconosciuto che le operazioni di registrazione e trasferimento dei dati relativi alla vita del ricorrente unitamente al diniego della possibilità di accedervi integrano un'interferenza nella sua vita privata. Tale interferenza è da considerarsi ammissibile in quanto "prevista dalla legge" e "necessaria in una società democratica nell'interesse della sicurezza nazionale" (art. 8, par. 2). La memorizzazione di dati da parte di una pubblica autorità determina un'ingerenza nella vita privata di un individuo e il successivo utilizzo delle informazioni è irrilevante.

5. Il controllo effettuato dalla Corte di giustizia sul rispetto dei diritti fondamentali ha per oggetto le attività delle istituzioni, l'attuazione del diritto dell'Unione europea da parte degli Stati membri e l'analisi delle giustificazioni delle possibili deroghe.

Il bilanciamento della Corte di giustizia tra libertà fondamentali del mercato e diritti fondamentali è stato oggetto di numerose sentenze tra le quali si segnalano *Schmidberger*, *Omega*, *Viking e Laval*[20].

La questione di maggior interesse attuale riguarda il bilanciamento tra diritti fondamentali. Il diritto alla privacy rappresenta il contesto ideale per esplorare la tensione e il conflitto tra i diritti fondamentali, perché si scontra abitualmente con altri diritti, come il diritto di proprietà o la libertà di espressione. Come vedremo, nella ricerca di un giusto equilibrio tra i diritti fondamentali (ad esempio *Promusicae* e *Satamedia*)[21], la Corte ha preferito indicare solo alcuni principi di

[18] *Leander v. Sweden*, 26 March 1987, cit.

[19] *Amann v. Switzerland* [GC], no. 27798/95, cit.

[20]Sentenze della Corte di giustizia: del 12 giugno 2003, *Schmidberger c. Austria*, causa C-112/00, in *Racc*., p. I-05659; del 14 ottobre 2004, *Omega Spielhallenm und Automatenaufstellungs-GmbH c. Oberbürgermeisterin der Bundesstadt Bonn*, causa C-36/02, in *Racc*., p. I-09609; dell'11 dicembre 2007, *International Transport Workers' Federation e Finnish Seamen's Union c. Viking Line ABP e OÜ Viking Line Eesti,* causa C-438/05. in *Rac*c., p. I-10779; del 18 dicembre 2007, *Laval un Partneri Ltd c. Svenska Byggnadsarbetareförbundet, Svenska Byggnadsarbetareförbundets avdelning 1, Byggettan e Svenska Elektrikerförbundet*, causa C-341/05, in *Racc*., p. I-11767.

[21]Sentenze della Corte: del 29 gennaio 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, causa C-275/06, in *Racc*., p. I-00271 e del 16 dicembre 2008, *Tietosuojavaltuutettu contro Satakunnan Markkinapörssi Oy e Satamedia Oy*, causa C-73/07, in *Racc*., p. I-09831.

valutazione e rimettere la soluzione delle questioni principali ai giudici nazionali nell'ambito della dinamica dell'interpretazione pregiudiziale.

Com'è noto, tale dialogo costituisce il punto di intersezione tra il livello di tutela nazionale e quello dell'Unione europea. Il confronto tra le corti nazionali e la Corte di giustizia, attraverso il rinvio pregiudiziale, costituisce un passaggio fondamentale del coordinamento dei due livelli di tutela. Il bilanciamento si realizza proprio nel rinvio pregiudiziale, che permette di realizzare continuamente la coesione e l'uniformità dell'ordinamento. In proposito, occorre tuttavia ricordare che la competenza della Corte di giustizia trova un limite invalicabile, nel senso che essa non può essere adita laddove sia in gioco una prerogativa derivante dal diritto nazionale o per una questione prettamente di diritto interno.

La Corte di giustizia è chiamata a svolgere tale opera di bilanciamento, risolvendo i conflitti nei casi concreti che vengono posti alla sua attenzione. Sulla base delle scelte del legislatore europeo, suo obiettivo è la ricerca del giusto equilibrio e della corretta ponderazione tra le diverse esigenze nel caso di specie. La Corte esamina il bilanciamento legislativo tra gli interessi contrapposti (ad esempio, prevenzione, investigazione e perseguimento dei reati da una parte e riservatezza e protezione dei dati personali dall'altra). In alcuni casi, critica la mancata considerazione degli aspetti relativi ai diritti fondamentali all'interno del processo di armonizzazione dell'UE che si concentra esclusivamente sugli aspetti tecnici della conservazione dei dati.

Nella sentenza c.d. *data retention*[22], la Corte di giustizia conferma la tendenza a valorizzare il suo ruolo di controllo sulla normativa europea e su quella nazionale, nei limiti, non ancora precisamente delineati dall'art. 51, par. 1, della Carta, affermando il proprio ruolo di garante costituzionale mediante il sindacato sul rispetto dei diritti fondamentali, in dialogo con la Corte EDU e le Corti costituzionali nazionali.

Nella più recente sentenza *Google Spain*[23], la Corte di giustizia ha utilizzato una lettura manipolativa della disciplina di diritto derivato alla luce dei parametri costituzionali che, agli artt. 7 e 8 della Carta, configurano lo statuto della c.d. "privacy digitale".

6. Com'è noto, lo scarno catalogo originale del testo della CEDU (con annessi allegati) si è trasformato nell'attuale ricco e articolato "diritto vivente" proprio per

[22] Sentenza della Corte dell'8 aprile 2014, *Digital Rights Ireland Ltd c. Minister for Communications, Marine and Natural Resources e altri e Kärntner Landesregierung e altri*, cause riunite C-293/12 e C-594/12, non ancora in *Racc*.

[23] Sentenza della Corte del 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, non ancora pubblicata in *Racc.*

effetto dell'attività della Corte di Strasburgo[24]. Infatti quest'ultima opera un continuo consolidamento dei diritti legati ai cambiamenti della società e della tecnologia, in materia familiare, ambientale e genetico–riproduttiva, argomentando tra gli opposti criteri del "consenso europeo" e del margine di apprezzamento lasciato agli Stati.

Nel caso della privacy e della telematica è l'impatto della tecnologia ad essere oggetto di valutazione. La Corte fa progressivamente emergere da una disposizione quale l'art. 8 della CEDU, che tutela il rispetto della vita privata e familiare nell'accezione di una libertà negativa (obbligo di non interferenza da parte della autorità), una tutela positiva e dinamica come quella che connota il diritto al controllo dei propri dati personali. Infatti, la Corte interpreta il testo convenzionale applicando un'interpretazione teleologica "parametrata" sul consenso europeo. Lo *standard* europeo applicabile è, per lo più, il risultato di un'indagine della Corte sull'esistenza di una base comune nel diritto e nella prassi degli Stati contraenti, soprattutto al fine di restringere il margine di apprezzamento dei singoli Stati contraenti. Tale metodo non è esente da critiche nella misura in cui tende a trascurare le posizioni minoritarie di alcuni Stati contraenti o non sia suffragato da una profonda e dettagliata ricerca comparativa; di sicuro consente però una convergenza progressiva tra i diritti protetti negli ordinamenti nazionali verso un comune *standard* europeo, quale fine ultimo del sistema convenzionale.

Nella giurisprudenza della Corte europea dei diritti umani, la sussidiarietà tra tutela nazionale e garanzia sovranazionale non deriva soltanto dalla regola del "previo esaurimento delle vie di ricorso interno", ma anche dal controllo della Corte sull'esistenza di idonei rimedi giurisdizionali per la protezione dei diritti negli ordinamenti nazionali (sussidiarietà)[25].

Infatti, nel valutare se un'ingerenza sia proporzionata alla finalità perseguita, riconosce un margine di discrezionalità ai comportamenti legislativi ed operativi degli Stati contraenti, in ragione della loro prossimità alla situazione da valutare e controllare.

Il giudizio così condotto deve portare al rilevamento di un "*pressing social need*". L'assenza di espressi criteri di riferimento ha indotto la Corte a riconoscere un ampio margine di discrezionalità (*wide margin of appreciation*) agli Stati, vale a dire l'esistenza di un "livello minimo" di rispetto del diritto alla privacy. Il margine di apprezzamento viene riconosciuto alle autorità nazionali competenti al fine di trovare un giusto equilibrio tra i contrapposti interessi pubblici e privati. Tale

[24] M. O'BOYLE, *The future of the European Court of Human Rights*, in *German Law Journal*, 2011, p. 1862 ss. Sulle caratteristiche delle sentenze della Corte europea dei diritti umani, v. R.C.A. WHITE, *Judgments in the Strasbourg Court: some reflections*, disponibile *on line*.

[25] Sulle questioni legate all'aborto, v. *Evans v. the United Kingdom* [GC], no. 6339/05, § 77- 87, ECHR 2007-I; in materia di adozione, *Moretti and Benedetti v. Italy*, no. 16318/07, § 63, 27 April 2010.

margine statale è sottoposto alla vigilanza della Corte che esercita un secondo margine di apprezzamento europeo in relazione alla natura e alla gravità degli interessi in gioco.

Tuttavia, occorre precisare che l'esame della giurisprudenza della Corte sul contenuto e sulla portata degli obblighi convenzionali richiede particolare cautela, perché le argomentazioni utilizzate sono collegate alle concrete vicende del ricorso ed agli specifici atti nazionali in discussione (funzione di "giudice del caso concreto"). Tuttavia, occorre sottolineare l'evidente tendenza ad un'attività interpretativa a più ampio spettro, che la porta a sollevare d'ufficio questioni non proposte dal ricorrente. Il valore delle sentenze della Corte non può essere limitato al mero accertamento dell'esistenza di violazioni nei singoli casi in esame.

Occorre inoltre ricordare che, per la definizione delle nozioni convenzionali, un particolare rilievo possono assumere gli strumenti internazionali e la prassi degli Stati contraenti, in quanto espressioni di "*common values*"[26]. Quanto al valore delle sentenze della Corte di Strasburgo, nonostante le pronunce abbiano efficacia giuridico–formale limitata al singolo caso (art. 46, par. 1), con effetti giuridici esclusivamente tra le parti, si ritiene producano il cosiddetto effetto della *res interpretata*[27]. In sostanza, la Corte afferma, secondo il principio della sentenza *Goodwin*[28], di non essere formalmente vincolata a seguire i propri precedenti, ma di ritenere prioritario non discostarsene nell'interesse della certezza giuridica, della prevedibilità e dell'uguaglianza di fronte al diritto, almeno in assenza di valida giustificazione.

Il bilanciamento degli interessi generali e individuali da parte della Corte EDU è realizzato tramite criteri, quali la proporzionalità degli obiettivi perseguiti e la necessità delle deroghe in una società democratica. L'azione giurisdizionale della Corte resta nei limiti di ingerenza nella sfera sovrana degli Stati contraenti, se si considera, da un lato, l'applicazione del principio di proporzionalità; dall'altro, la dottrina pretoria del "margine di apprezzamento", che consente uno spazio di flessibilità allo Stato contraente, specie nella concreta applicazione delle deroghe alla tutela di alcuni diritti. La Corte di Strasburgo ha introdotto il giudizio sulla proporzionalità nella sentenza *Handyside*[29] quale corollario della formula "necessità in una società democratica" (nel par. 2 delle norme convenzionali degli articoli da 8 a 11 CEDU). Tale valutazione, finalizzata al contemperamento di due diritti fondamentali in conflitto, si esprime nel "margine di apprezzamento" riconosciuto allo Stato contraente e sottoposto a livello europeo al giudizio della Corte.

La Corte EDU valuta l'esistenza di un'interferenza dello Stato convenuto

[26] *Demir and Baykara v. Turkey* [GC], no. 34503/97, § 85, ECHR 2008.
[27] U. VILLANI, *Dalla Dichiarazione universale alla Convenzione europea dei diritti dell'uomo*, Bari, 2012, p. 89 ss.
[28] *Goodwin v. the United Kingdom*, 27 March 1996, *Reports of Judgments and Decisions* 1996-II.
[29] *Handyside v. the United Kingdom*, 7 December 1976, Series A no. 24.

(obbligo negativo) o di una violazione di un obbligo negativo[30]. Le parti contraenti sono tenute ad impegnarsi al fine di garantire un effettivo godimento del diritto protetto. Gli Stati, oltre ad essere destinatari di un obbligo negativo di astensione dal porre in essere interferenze non giustificabili, sono destinatari di obblighi positivi per garantire l'effettività del rispetto del diritto alla privacy. Se il comportamento attivo o omissivo dallo Stato convenuto costituisce un'interferenza con il diritto del ricorrente deve essere giustificabile o ammissibile in base alle condizioni previste dal secondo paragrafo del medesimo art. 8 CEDU. L'interferenza deve essere prevista da una disposizione normativa che abbia i caratteri di prevedibilità e accessibilità; perseguire uno o più degli scopi legittimi ivi previsti (sicurezza nazionale, pubblica sicurezza, benessere economico del paese, ecc.); "necessaria" a soddisfare un "bisogno sociale imperativo" nonché "proporzionata" al perseguimento degli scopi legittimi. Rispetto a quest'ultimo principio, l'interferenza non deve essere eccessiva, irragionevole o discriminatoria, anche in considerazione dell'intensità o della gravità dell'interferenza e delle garanzie giurisdizionali a tutela dell'individuo.

Per quanto riguarda la categoria degli obblighi positivi, gli Stati contraenti sono tenuti a compiere determinate attività volte a garantire l'effettivo rispetto del diritto alla privacy. Tale categoria consente di espandere la tutela a situazioni in cui il godimento dei diritti è ostacolato da atti dei privati (cd. "effetto nei confronti dei terzi").

II riferimento al principio di sussidiarietà e alla dottrina del margine di apprezzamento trovano ora posto nel preambolo del Protocollo n. 15[31]. In ogni caso, l'interpretazione della Corte non può essere "imbrigliata" dalle preoccupazioni degli Stati contraenti[32], se resta nella corretta applicazione del principio di proporzionalità. Il "margine di apprezzamento" consente uno spazio di flessibilità allo Stato contraente da bilanciare però con l'effettività della tutela dei diritti convenzionali e le esigenze di interpretazione evolutiva.

Infine, occorre ricordare che la CEDU è immediatamente applicabile e i giudici nazionali sono chiamati all'interpretazione conforme delle norme interne.

---

[30] B. CONFORTI, *Reflections on State Responsibility for the Breach of Positive Obligations: the Case-law of the European Court of Human Rights*, in *IYIL*, 2003, p. 3 ss.; M. HAKIMI, *State Bystander Responsibility*, in *EJIL*, 2010, p. 341 ss.

[31] M. L. PADELLETTI, *Il Protocollo n. 15 alla Convenzione europea dei diritti dell'uomo: quali prospettive per i ricorsi individuali alla Corte europea?*, in *Diritti umani e diritto internazionale*, 2013, p. 761 ss.; C. ZANGHÌ, *I progetti di Protocolli 15 e 16 alla Convenzione europea dei diritti dell'uomo*, in *Rivista della cooperazione giuridica internazionale*, 2013, n. 43, p. 24 ss.

[32] B. CONFORTI, *Osservazioni sulla dichiarazione di Brighton*, in *Diritti umani e diritto internazionale*, 2012, p. 649 ss., in specie p. 650 ss. Sulla dichiarazione di Brighton e sui negoziati per la conclusione dei due ultimi protocolli alla CEDU adottati, v. E. NALIN, *I Protocolli n. 15 e 16 alla Convenzione europea dei diritti dell'uomo*, in *Studi sull'integrazione europea*, 2014, p. 117 ss.

Parte I
Il bilanciamento degli interessi da parte del legislatore dell'Unione

Cap. I
Definizioni e inquadramento giuridico

– 1. La Convenzione 108 del Consiglio d'Europa. – 2. Le basi giuridiche nel Trattato di Lisbona. – 3. La direttiva 95/46/CE. – 4. Il ruolo della direttiva 95/46/CE a partire dalla sentenza *Lindqvist*. – 5. La direttiva 2002/58 relativa alla vita privata e alle comunicazioni elettroniche, modificata dalla direttiva 2009/136/CE. – 6. La direttiva *data retention*. – 7. La decisione quadro 2008/977/GAI. – 8. La direttiva 2013/40/UE relativa agli attacchi contro i sistemi di informazione.

1. La tutela garantita dalla Carta è il punto di arrivo di un percorso intrapreso con l'adozione della Convenzione 108 del Consiglio d'Europa nel 1980.

La tutela dei dati personali si collega nel contesto del Consiglio d'Europa alla questione della promozione dei diritti umani, della democrazia e dello stato di diritto. In tale ambito, un particolare rilievo occupa la disciplina della Convenzione n.108, che ha ispirato gli standard della giurisprudenza della CEDU e della Corte di giustizia dell'Unione europea.

Nel Preambolo è sancito il principio secondo cui la libera circolazione delle informazioni non può prescindere dalla tutela dei diritti e delle libertà fondamentali di ciascuno e in particolare dal diritto al rispetto della vita privata. La finalità della Convenzione 108 è quella di garantire la protezione degli individui senza considerazione di frontiere, a prescindere dalla loro cittadinanza o residenza, nei confronti dell'elaborazione automatica dei dati che li riguardano (art. 1). La sua applicazione è espressamente indirizzata alle persone fisiche e all'elaborazione automatica di dati (in ambito pubblico o privato) e impegna gli Stati ad adottare provvedimenti in materia idonei a rendere operativi i principi fondamentali. La Convenzione non è uno strumento "self–executing", immediatamente esecutivo, ma vincola le Parti a conformare ad essa le normative nazionali.

In particolare, in base al criterio di "legalità" gli scopi del trattamento devono essere legittimi e i dati, esatti e aggiornati, devono essere trattati secondo le prescrizioni di legge. Altro principio fondamentale è quello che vieta l'elaborazione automatica di alcuni tipi di dati sensibili ex art 6 (informazioni capaci di rivelare l'origine razziale, le opinioni politiche, le convinzioni religiose, lo stato di salute, la vita sessuale o relative alle condanne penali). Il divieto generale di sottoporre tali dati a trattamento può venir meno a condizione che "il diritto interno preveda garanzie appropriate", vale a dire che i trattamenti di dati sensibili siano contenuti e controllati mediante strumenti appositi. Un altro principio (art. 7) che non sembra essere in alcun modo derogabile è quello relativo alle "misure di sicurezza" che devono essere adottate per evitare la distruzione, la perdita o l'accesso non autorizzati dei dati. Si tratta di un dovere degli Stati di sancire un obbligo per i responsabili del trattamento che dovranno adottare delle garanzie adeguate al tipo di trattamento, al livello del rischio e dello stato delle conoscenze informatiche. All'interessato, cui si riferiscono i dati, è riconosciuta una serie di diritti (art. 8), tra cui il diritto di accesso ai propri dati, il diritto di rettifica e aggiornamento di dati inesatti, quello di cancellazione dei dati elaborati in violazione di legge. Tra questi ultimi devono farsi rientrare anche i dati non più utili ai fini dell'elaborazione, a tutela del diritto all'oblio dell'interessato.

Per rendere questi diritti effettivamente attuabili si riconosce agli interessati la possibilità di esperire un'azione amministrativa o giudiziaria, ad esempio nel caso di

inerzia del responsabile del trattamento di fronte a una richiesta dell'interessato.

La Convenzione prevede una serie di deroghe ai principi che consentono agli Stati di attenuare alcuni obblighi o di limitare i diritti, purché sia necessario in una società democratica a tutelare interessi rilevanti dello Stato (sicurezza dello Stato, sicurezza pubblica, repressione dei reati, interessi monetari statali) o del soggetto cui i dati si riferiscono o ancora di diritti e libertà altrui; le deroghe devono essere contenute in atti di rango legislativo.

Le parti Contraenti possono riconoscere agli interessati una protezione più ampia di quella prevista in quanto la Convenzione costituisce un "denominatore comune minimo".

Uno specifico valore interpretativo va peraltro ricercato anche ad atti non vincolanti (*soft law*) dell'Assemblea consultiva parlamentare, del Comitato Consultativo della Convenzione n. 108 e del relativo Commissario del Consiglio d'Europa[33].

2. Il Trattato di Lisbona ha creato per la prima volta una nuova base giuridica per la protezione dei dati personali nello Spazio di libertà, sicurezza e giustizia, utilizzabile sia per l'armonizzazione legislativa del mercato, che per la cooperazione giudiziaria civile e penale (ex terzo pilastro). Tuttavia, la base giuridica dell'art. 16 TFUE consente all'Unione europea di adottare direttive e regolamenti per la cooperazione di polizia solo dopo la fine del periodo transitorio di cinque anni, vale a dire alla fine del 2014.

La competenza prevista dall'art. 16 del TFUE è una competenza concorrente dell'Unione con gli Stati membri come per tutto lo Spazio di libertà, sicurezza e giustizia (cooperazione in materia di immigrazione, cooperazione civile e penale). In quest'ultimo settore potranno comunque essere previste norme specifiche (v. Dichiarazione 21 allegata al Trattato di Lisbona)[34]. Infatti, le informazioni nel settore della libertà, della sicurezza e della giustizia vengono scambiate anche per

[33] L. PRATCHETT, *Developing democracy in Europe: an analytical summary of the Council of Europe's acquis*, Strasbourg, 2004; M.FUMAGALLI MERAVIGLIA, *Compliance review nel Consiglio d'Europa*, Milano, 2004; G. RAIMONDI, *Il Consiglio d'Europa e la Convenzione europea dei diritti dell'uomo*, Napoli, 2005; R. BODY, *A democratic Europe: the alternative to the European Union*, London, 2006; A. ROYER, *The Council of Europe*, Strasbourg, 2010; R. PISILLO MAZZESCHI, *Esaurimento dei ricorsi interni e diritti umani*, Torino, 2004; U. VILLANI, *Il protocollo n. 14 alla Convenzione europea dei Diritti dell'Uomo*, in *La Comunità internazionale*, 2004, p. 487 ss.; F. SALERNO, *Le modifiche strutturali apportate dal Protocollo n. 14 alla procedura della Corte Europea dei Diritti dell'Uomo*, in *RDIPP*, 2006, p. 377 ss.; D. HARRIS (AND OTHERS), *Law of the European Convention on Human Rights*, Oxford, 2009, 2nd ed.; P. PIRRONE, *L'obbligo di conformarsi alle sentenze della Corte europea per i diritti umani*, Milano, 2004.

[34] Dichiarazione relativa alla protezione dei dati personali nel settore della cooperazione giudiziaria in materia penale e della cooperazione di polizia. In considerazione della specificità dei settori in questione, potrebbero rivelarsi necessarie norme specifiche sulla protezione dei dati personali e sulla libera circolazione di tali dati nei settori della cooperazione giudiziaria in materia penale e della cooperazione di polizia, in base all'art. 16 del TFUE.

analizzare le minacce alla sicurezza, identificare i trend delle attività criminali o valutare i rischi nei settori correlati.

La seconda base giuridica riguarda il settore della politica estera e di sicurezza comune, in cui il TFUE prevede invece solo l'adozione di una decisione *ad hoc* del Consiglio[35].

3. La direttiva 95/46/CE[36] costituisce la parte principale della normativa secondaria sulla protezione dei dati personali nel mercato che contiene gli elementi principali della tutela, concretizzando e ampliando il contenuto della Convenzione 108.

La direttiva rappresenta un quadro generale completato da strumenti normativi specifici quali il regolamento (CE) n. 45/2001/CE del Parlamento europeo e del Consiglio, del 18 dicembre 2000[37], concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari e la direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche nonchè la libera circolazione di tali dati (in particolare art. 41)[38].

La direttiva 95/46/CE prevede di promuovere la libera circolazione delle informazioni nel mercato interno; l'armonizzazione di disposizioni essenziali del diritto nazionale; esprime la fiducia reciproca degli Stati membri nei rispettivi sistemi giuridici nazionali. Le sue disposizioni della direttiva non si applicano ai trattamenti di dati personali effettuati per l'esercizio di attività che non rientravano nel campo di applicazione del diritto comunitario e, comunque, ai trattamenti aventi come oggetto la pubblica sicurezza, la difesa, la sicurezza dello Stato e in materia di diritto penale.

Per quanto riguarda le finalità di raccolta (art. 6), gli Stati membri dispongono che i dati personali debbano essere trattati lealmente e lecitamente; rilevati per finalità determinate, esplicite e legittime, e successivamente trattati in modo non incompatibile con tali finalità. Il trattamento successivo dei dati per scopi storici, statistici o scientifici non è ritenuto incompatibile, purché gli Stati membri

[35] V. art. 39 TUE: "Conformemente all'art. 16 del trattato sul funzionamento dell'Unione europea e in deroga al par. 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti".

[36] Direttiva 95/46/CE del Parlamento europeo e del Consiglio relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati, in *GU* L 281 del 23 novembre 1995.

[37] in *GU CE* 238 del 13 agosto 2011, p. 14-14.

[38] V. direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche e il regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio, del 18 dicembre 2000, concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari.

forniscano garanzie appropriate.

Secondo il principio generale del consenso, la persona interessata deve esprimersi esplicitamente a favore del trattamento dei dati personali che la riguardano. Gli Stati membri dispongono che il trattamento di dati personali può essere effettuato soltanto quando la persona interessata ha manifestato il proprio consenso in maniera inequivocabile, oppure se è necessario all'esecuzione del contratto concluso con la persona interessata o all'esecuzione di misure precontrattuali prese su richiesta di tale persona; oppure se è necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento (art. 7). Inoltre il trattamento può essere svolto quando risulta necessario per la salvaguardia dell'interesse vitale della persona interessata, oppure è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento o il terzo a cui vengono comunicati i dati; quando è necessario per il perseguimento dell'interesse legittimo del responsabile del trattamento oppure dei terzi cui vengono comunicati i dati, a condizione che non prevalgano l'interesse o i diritti e le libertà fondamentali della persona (art. 1, par. 1). Tuttavia, gli Stati membri riconoscono alla persona interessata il diritto di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale (art. 14).

Quanto all'esclusione di specifiche categorie di dati, specie di carattere sensibile, è vietato il trattamento di dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché il trattamento di dati relativi alla salute e alla vita sessuale. Gli Stati membri prevedono per il trattamento di dati personali effettuato esclusivamente a scopi giornalistici o di espressione artistica o letteraria, deroghe ad alcune disposizioni della direttiva solo quando risultino necessarie per conciliare il diritto alla vita privata con le norme sulla libertà d'espressione. Inoltre, gli Stati membri possono adottare disposizioni legislative intese a limitare la portata degli obblighi e dei diritti previsti dalle disposizioni della direttiva, qualora tale restrizione costituisca una misura necessaria alla salvaguardia della sicurezza dello Stato, della difesa e della pubblica sicurezza.

Per quanto riguarda i ricorsi giurisdizionali, gli Stati membri stabiliscono che chiunque può disporne in caso di violazione dei diritti garantiti dalle disposizioni nazionali applicabili al trattamento (art. 22).

In materia di responsabilità, chiunque subisca un danno cagionato da un trattamento illecito o da qualsiasi altro atto incompatibile con le disposizioni nazionali di attuazione della direttiva ha il diritto di ottenere il risarcimento del pregiudizio subito dal responsabile del trattamento (art. 23). Il responsabile del trattamento può essere esonerato in tutto o in parte da tale responsabilità se prova

che l'evento dannoso non gli è imputabile.

Per quanto riguarda l'obbligo di informazione sui dati raccolti, gli Stati membri dispongono che il responsabile del trattamento, o il suo rappresentante, debba informare gli interessati sulla raccolta dei dati che la riguardano, a meno che tale persona ne sia già informata (art. 10). Infatti, gli Stati membri prevedono un obbligo di notifica a carico del responsabile del trattamento, od eventualmente del suo rappresentante, presso l'autorità di controllo, prima di procedere alla realizzazione di un trattamento, o di un insieme di trattamenti, interamente o parzialmente automatizzato, destinato al conseguimento di una o più finalità correlate.

Per i trattamenti dei dati che potenzialmente presentano rischi specifici per i diritti e le libertà delle persone, gli Stati membri precisano e provvedono a che tali trattamenti siano esaminati prima della loro messa in opera (art. 20). Tali esami preliminari sono effettuati dall'autorità di controllo, una volta ricevuta la notificazione del responsabile del trattamento, oppure dalla persona incaricata della protezione dei dati che, nei casi dubbi, deve consultare l'autorità di controllo medesima. Gli Stati membri possono effettuare tale esame anche durante il processo di elaborazione di un provvedimento del Parlamento nazionale, o in base ad un provvedimento fondato su siffatto provvedimento legislativo, in cui si definisce il tipo di trattamento e si stabiliscono appropriate garanzie.

In relazione ai poteri investigativi, ogni autorità di controllo dispone del diritto di accesso ai dati oggetto di trattamento e di raccolta di qualsiasi informazione necessaria all'esercizio della sua funzione di controllo; di poteri effettivi d'intervento, come quello di formulare pareri prima dell'avvio di trattamenti (art. 20) e di dar loro adeguata pubblicità o quello di ordinare il congelamento, la cancellazione o la distruzione dei dati, oppure di vietare a titolo provvisorio o definitivo un trattamento, ovvero quello di rivolgere un avvertimento o un monito al responsabile del trattamento o quello di adire i Parlamenti o altre istituzioni politiche nazionali e del potere di promuovere azioni giudiziarie in caso di violazione delle disposizioni nazionali di attuazione della presente direttiva nonché di adire per dette violazioni le autorità giudiziarie. È possibile un ricorso giurisdizionale contro le decisioni dell'autorità di controllo eventualmente recanti pregiudizio. Qualsiasi persona, o associazione che la rappresenti, può presentare ad un'autorità di controllo una domanda relativa alla tutela dei suoi diritti e libertà con riguardo al trattamento di dati personali.

4. Nella sentenza *Lindqvist*, la protezione dei dati personali viene posta a confronto con la libertà di espressione[39]. La Corte ritiene, innanzitutto, applicabile la

[39] V. sentenza *Lindqvist*, cit. Il rinvio pregiudiziale veniva attivato nell'ambito di un procedimento penale svoltosi dinanzi ad una Corte d'appello svedese contro la sig.ra *Lindqvist*. Quest'ultima era perseguita per aver violato la normativa relativa alla protezione dei dati personali pubblicando nel

direttiva al caso di specie, considerando che le definizioni di "dati personali" e "trattamento" erano tali da ricomprendere l'attività dell'imputata del giudizio principale. La Corte si sofferma sul conflitto tra il diritto alla libertà di espressione della sig. ra Lindqvist a pubblicare i dati in oggetto sul proprio sito ed il diritto alla riservatezza dei titolari di tali dati, richiamando, innanzitutto, gli obiettivi della direttiva, ovvero garantire l'armonizzazione dei regimi nazionali applicabili al trattamento dei dati e salvaguardare al tempo stesso i diritti fondamentali. Tali obiettivi non possono essere confliggenti e devono essere perseguiti contemporaneamente. Le disposizioni della direttiva sono necessariamente generiche, dovendo questa applicarsi ad un certo numero di situazioni diverse: essa lascia, infatti, agli Stati il compito di decidere i dettagli o scegliere le diverse opzioni di tutela. La Corte sottolinea (par. 84) che gli Stati membri dispongono, sotto molti aspetti di un margine di manovra al fine di trasporre la direttiva 95/46/CE, ma niente lascia presumere che questa manchi di prevedibilità o sia in contrasto con i principi generali del diritto dell'Unione europea o i diritti fondamentali. Dopo aver eliminato ogni dubbio circa la compatibilità dello strumento dell'Unione europea con i diritti fondamentali, in verità con un'affermazione alquanto apodittica, la Corte rinvia il bilanciamento alla fase di attuazione sul piano nazionale. Essa, infatti, specifica che è in tale fase che "deve essere trovato un giusto equilibrio tra i diritti e gli interessi di cui trattasi". La Corte indica che è necessario soppesare la libertà di espressione e la tutela della vita privata: tale bilanciamento deve essere fatto interpretando il diritto nazionale in modo conforme alla direttiva e ai diritti fondamentali tutelati nell'ordinamento giuridico dell'Unione europea. La Corte impone, però, il rispetto del principio di proporzionalità, in quanto, sebbene gli Stati siano chiamati ad elaborare sanzioni efficaci per il mancato rispetto della direttiva, non devono però in alcun modo violare tale principio.

In tale pronuncia, dunque, la Corte non effettua direttamente un bilanciamento tra i diritti in causa, ma rinvia al giudice nazionale confermando la conformità ai diritti fondamentali della normativa comunitaria e la necessità di perseguire la tutela degli stessi. Appare, dunque, che se la direttiva viene elaborata inizialmente per finalità di realizzazione del mercato, diventa poi strumento per l'equiparazione dei livelli di tutela dei diritti fondamentali nei vari ordinamenti degli Stati membri. Essa assume, in tal modo, un ambito di applicazione molto vasto, che prescinde dal collegamento

---

proprio sito internet informazioni riguardanti un certo numero di persone che lavoravano con lei in qualità di volontari in una parrocchia della Chiesa protestante di Svezia. Le questioni sollevate dal giudice riguardano, innanzitutto, l'applicabilità della direttiva 95/46/CE alla fattispecie, in particolare se la realizzazione da parte di un singolo di una pagina internet, inserendovi il nome di un certo numero di persone unitamente a dichiarazioni e informazioni sugli stessi, costituisca un trattamento dei dati. In caso di risposta affermativa, il giudice richiedeva se in un'ipotesi come quella di specie la direttiva ponesse dei limiti incompatibili con i principi generali in materia di libertà di espressione o con altre libertà e diritti vigenti all'interno dell'Unione europea e che trovano corrispondenza con l'art. 10 CEDU.

con l'esercizio di una libertà comunitaria o con un elemento transfrontaliero e supera lo standard di tutela proprio di ciascuno Stato, imponendo il livello dell'Unione europea.

5. A livello del diritto comunitario, la conservazione e l'uso di dati a fini di contrasto dei reati sono stati affrontati per la prima volta dalla direttiva 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni[40]. Detta direttiva ha stabilito, per la prima volta, che gli Stati membri possono adottare le disposizioni legislative che considerano necessarie per la salvaguardia della pubblica sicurezza, della difesa o dell'ordine pubblico (compreso il benessere economico dello Stato ove le attività siano connesse a questioni di sicurezza dello Stato) e per l'applicazione del diritto penale[41].

La direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche[42] riguarda principalmente il trattamento dei dati personali nel quadro della fornitura dei servizi di telecomunicazione. La direttiva contiene norme fondamentali destinate a garantire la fiducia degli utilizzatori nei servizi e nelle tecnologie delle comunicazioni elettroniche. Esse riguardano in particolare il divieto di "spam", il sistema di consenso preventivo dell'utilizzatore ("opt-in") e l'installazione di marcatori ("cookies").

Si accresce la tutela contro i trattamenti invisibili di dati che si attivano ogni qualvolta si accede ad un sito internet. Le norme in materia di privacy *on line* si rafforzano, quindi, in merito all'uso dei *cookies* (stringhe di testo che possono anche memorizzare le scelte di navigazione degli utenti) e simili sistemi. Gli utenti di internet dovranno essere maggiormente informati sull'esistenza di tali sistemi e su ciò che accade ai loro dati, potendo così controllarli più facilmente. Anche per i "cookies" devono valere i concetti di informativa e consenso. Ai fini dell'espressione del consenso possono essere utilizzate specifiche configurazioni di programmi informatici o di dispositivi che siano di facile e chiara utilizzabilità per il contraente o l'utente.

---

[40] Nell'ambito delle loro attività, i fornitori di reti e servizi (di seguito "operatori") trattano dati personali ai fini della trasmissione di una comunicazione, della fatturazione, dei pagamenti di interconnessione, della commercializzazione e della fornitura di altri servizi a valore aggiunto. Tale trattamento riguarda dati che indicano la fonte, la destinazione, la data, l'ora, la durata e il tipo di una comunicazione, nonché le attrezzature di comunicazione degli utenti e, nel caso della telefonia mobile, dati sull'ubicazione delle attrezzature.

[41] Art. 14, par. 1, della direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni, in *GU* L 24 del 30 gennaio 1998, pp. 1-8).

[42] Il "Pacchetto Telecom 2002" comprende quattro altre direttive concernenti il quadro generale, l'accesso e l'interconnessione, le autorizzazioni e le licenze, il servizio universale.

La direttiva stabilisce come principio di base, che gli Stati membri devono garantire, tramite la legislazione nazionale, la riservatezza delle comunicazioni effettuate tramite una rete pubblica di comunicazioni elettroniche. In particolare, devono proibire ad ogni altra persona di ascoltare, intercettare, memorizzare le comunicazioni senza il consenso degli utenti interessati.

Per quanto riguarda la sicurezza dei servizi, il fornitore di un servizio di comunicazione elettronica deve garantire che i dati personali siano accessibili soltanto al personale autorizzato; tutelati dalla distruzione, perdita o alterazione accidentale. Eventuali violazioni devono essere comunicate alla persona interessata, nonché all'autorità nazionale di regolamentazione (ANR).

Per garantire la disponibilità dei dati di comunicazione per la ricerca, l'accertamento e il perseguimento di reati, la direttiva stabilisce un regime di conservazione dei dati. La direttiva adotta l'approccio di libera scelta ("opt–in") in relazione alle comunicazioni elettroniche commerciali indesiderate, cioè gli utenti devono dare il loro accordo preliminare prima di ricevere queste comunicazioni. Questo sistema di "opt–in" copre anche i messaggi sms e altri messaggi elettronici ricevuti su qualsiasi terminale fisso o mobile. Sono tuttavia previste deroghe.

A norma della direttiva 2002/58/CE relativa alla vita privata e alle comunicazioni elettroniche[43], in linea di principio tali dati relativi al traffico, generati dall'uso dei servizi di comunicazione elettronica, devono essere cancellati o resi anonimi quando non sono più necessari ai fini della trasmissione di una comunicazione, salvo i casi in cui risultino necessari per la fatturazione, e solo per il periodo necessario a tal fine, o in cui sia stato ottenuto il consenso dell'abbonato o utente. I dati relativi all'ubicazione possono essere trattati soltanto se sono resi anonimi o con il consenso dell'utente interessato, nella misura e per il periodo necessari alla fornitura di un servizio a valore aggiunto.

Le modifiche introdotte dalla direttiva 2009/136/CE, in materia di trattamento dei dati personali e tutela della vita privata nel settore delle comunicazioni elettroniche sono finalizzate a promuovere una maggiore tutela dei consumatori contro le violazioni dei dati personali, le comunicazioni indesiderate e il c.d. "spam". A questo proposito, il soggetto tutelato dalle comunicazioni indesiderate e dallo spam viene definito in modo nuovo, vale a dire "contraente" o "utente" (in sostituzione del concetto di interessato o abbonato).

[43] Direttiva del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), in *GU* L 201 del 31 luglio 2002, pp. 37-47.

6. La direttiva *data retention*[44] ha modificato l'art. 15, par. 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche, inserendo un paragrafo che esclude che tale normativa si applichi ai dati conservati in base alla direttiva *data retention*[45]. Secondo tale direttiva (art. 11), gli Stati membri possono adottare disposizioni legislative in deroga al principio della riservatezza delle comunicazioni, tra cui, a talune condizioni, la conservazione, l'accesso e il ricorso ai dati a fini di contrasto. L'art. 15, paragrafo 1, permette agli Stati membri di limitare i diritti e gli obblighi attinenti alla vita privata, anche mediante la conservazione di dati per un periodo di tempo limitato, qualora la misura sia "necessaria, opportuna e proporzionata all'interno di una società democratica per la salvaguardia della sicurezza nazionale (cioè della sicurezza dello Stato), della difesa, della sicurezza pubblica; e la prevenzione, ricerca, accertamento e perseguimento dei reati, ovvero dell'uso non autorizzato del sistema di comunicazione elettronica".

Quanto all'origine della direttiva *data retention*, occorre ricordare che l'Irlanda e altri Stati membri avevano presentato al Consiglio un progetto di decisione quadro per la conservazione dei dati trattati e memorizzati nell'ambito della fornitura di servizi di comunicazioni elettroniche accessibili al pubblico per la prevenzione, l'accertamento e il perseguimento dei reati, compreso il terrorismo[46]. Tale progetto

---

[44] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio del 15 marzo 2006 riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE, in *GU* C 175 del 10 giugno 2014, pp. 6-7. La conservazione dei dati è diversa dalla conservazione per ordine giudiziario (il cosiddetto "congelamento rapido"), in base al quale gli operatori sono tenuti a conservare soltanto i dati riguardanti specifici indiziati a partire dalla data dell'ordine. Questo tipo di conservazione dei dati è uno strumento investigativo previsto e utilizzato dagli Stati firmatari della convenzione del Consiglio d'Europa sulla criminalità informatica[44]. Quasi tutti gli Stati firmatari hanno istituito un punto di contatto, il cui ruolo è garantire assistenza immediata nelle indagini o nei procedimenti riguardanti la criminalità informatica. Tuttavia non tutte le parti della convenzione sembrano aver previsto questo tipo di conservazione, e finora non è ancora stata valutata l'efficacia di tale strumento nell'affrontare la criminalità informatica. I sostenitori della conservazione per ordine giudiziario ritengono che questo strumento comporti una minore ingerenza nella vita privata rispetto alla conservazione dei dati. Tuttavia, secondo la maggior parte degli Stati membri, qualsiasi modalità di conservazione per ordine giudiziario non può sostituire adeguatamente la conservazione dei dati, in quanto quest'ultima rende disponibili dati storici, mentre la conservazione per ordine giudiziario non garantisce la possibilità di individuare tracce anteriormente all'ordine di conservazione, né consente di condurre indagini quando un soggetto è ignoto o di raccogliere prove, per esempio, sugli spostamenti delle vittime o dei testimoni di reato.

[45] L'art. 11 della direttiva dispone: "All'art. 15 della direttiva 2002/58/CE è inserito il seguente paragrafo: 1 bis. Il par. 1 non si applica ai dati la cui conservazione è specificamente prevista dalla direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione, ai fini di cui all' art. 1, par. 1, di tale direttiva".

[46] Il 28 aprile 2004 la Repubblica francese, l'Irlanda, il Regno di Svezia e il Regno Unito di Gran Bretagna e Irlanda del Nord hanno presentato al Consiglio un'iniziativa ai fini dell'adozione di una decisione quadro fondata sugli artt. 31, n. 1, lett. c), UE e 34, n. 2, lett. b), UE. Tale progetto riguardava la conservazione dei dati trattati e memorizzati nel quadro della fornitura di servizi di comunicazione elettronica accessibili al pubblico o dei dati sulle reti pubbliche di comunicazione a

di decisione quadro prevedeva sia l'obbligo per gli operatori di conservare per un periodo i dati di traffico riguardanti gli utenti di loro servizi e sia obblighi relativi all'accesso e allo scambio da parte delle autorità competenti in materia penale.

La Commissione si pronunciava a favore del fondamento normativo utilizzato in tale progetto di decisione quadro solo per quanto riguarda una parte di quest'ultimo. In particolare, ricordava che l'art. 47 TUE (vecchio) non consentiva che un atto fondato sul Trattato UE modificasse l'*acquis communautaire* (vale a dire le direttive 95/46/CE e 2002/58/CE). In conclusione, ritenendo che la determinazione delle categorie di dati da conservare e del relativo periodo di conservazione rientrasse nella competenza del legislatore comunitario, la Commissione si è riservata il diritto di presentare una proposta di direttiva.

La direttiva *data retention* (ora annullata dalla Corte di giustizia) imponeva agli Stati membri di prevedere l'obbligo, per i fornitori di servizi di comunicazione elettronica accessibili al pubblico o di una rete pubblica di comunicazione, di conservare i dati relativi alle "comunicazioni a fini di indagine, accertamento e perseguimento di reati gravi, quali definiti da ciascuno Stato membro nella propria legislazione nazionale, e ha tentato di armonizzare alcune questioni correlate a livello dell'Unione".

La direttiva si applicava ai settori della telefonia di rete fissa, della telefonia mobile, dell'accesso internet, della posta elettronica su internet e della telefonia via internet[47]. Essa specificava (all'art. 5) le categorie di dati da conservare, vale a dire i dati necessari per identificare: la fonte di una comunicazione; la destinazione di una comunicazione; la data, l'ora e la durata di una comunicazione; il tipo di comunicazione; le attrezzature di comunicazione degli utenti o quello che si presume essere le loro attrezzature; l'ubicazione delle apparecchiature di comunicazione mobile. Comprendeva inoltre (art. 3, par. 2) i tentativi di chiamata non riusciti, ossia le chiamate telefoniche che sono state collegate con successo ma che non hanno ottenuto risposta, oppure in cui vi è stato un intervento del gestore della rete, ove i dati relativi a tali tentativi siano generati o trattati e immagazzinati oppure trasmessi dagli operatori. A norma della direttiva *data retention* non poteva essere conservato alcun dato relativo al contenuto della comunicazione.

Gli Stati membri erano tenuti a garantire che le categorie di dati di cui all'art. 5 fossero conservate per periodi non inferiori a sei mesi e non superiori a due anni[48]. Il periodo massimo di conservazione può essere prolungato da uno Stato membro che "si trovi ad affrontare circostanze particolari che giustificano una proroga per un periodo limitato"; tale proroga doveva essere notificata alla Commissione, la quale

fini di prevenzione, ricerca, accertamento e perseguimento della criminalità e dei reati, compreso il terrorismo (documento del Consiglio n. 8958/04).

[47] Campo d'applicazione della conservazione dei dati e categorie di dati da conservare (art. 1, par. 2; art. 3, par. 2, e art. 5).

[48] Periodi di conservazione (articoli 6-12).

decideva, entro sei mesi dalla notifica, se approvarla o respingerla. Mentre il periodo massimo di conservazione poteva essere prolungato, non erano previste disposizioni per ridurre la conservazione a meno di sei mesi.

La direttiva imponeva agli Stati membri di provvedere a che gli operatori rispettassero, come minimo, quattro principi di sicurezza dei dati, cioè che i dati conservati siano: della stessa qualità e soggetti alla stessa sicurezza e tutela dei dati in rete; soggetti ad adeguate misure tecniche e organizzative intese a tutelarli da una distruzione accidentale o illecita, da un'alterazione o perdita accidentale, da immagazzinamento, trattamento, accesso o divulgazione non autorizzati o illeciti; soggetti ad adeguate misure tecniche e organizzative intese a garantire che gli stessi possono essere consultati soltanto da persone appositamente autorizzate; e distrutti alla fine del periodo di conservazione, fatta eccezione per quelli consultati e conservati [ai fini previsti dalla direttiva].

Gli operatori non potevano trattare i dati conservati a norma della direttiva per scopi diversi da quelli per cui sono stati raccolti. Gli Stati membri dovevano designare un'autorità pubblica responsabile di esercitare, "in totale indipendenza", il controllo dell'applicazione dei suddetti principi. Tale autorità poteva essere la stessa autorità prevista dalla direttiva 95/46/CE sulla protezione dei dati.

Gli Stati membri (come indicato al considerando 12 della direttiva) potevano pertanto continuare a derogare al principio della riservatezza delle comunicazioni. La direttiva (sulla conservazione dei dati) disciplina soltanto la conservazione dei dati ai fini più limitati dell'indagine, dell'accertamento e del perseguimento di reati gravi.

Questo complesso rapporto giuridico tra la direttiva sulla conservazione dei dati e la direttiva relativa alla vita privata e alle comunicazioni elettroniche, associato all'assenza di una definizione di "reato grave" in entrambi gli strumenti, rende difficile distinguere, da un lato, le misure adottate dagli Stati membri per attuare gli obblighi in materia di conservazione dei dati previsti dalla direttiva e, dall'altro lato, la prassi più generale di conservazione dei dati negli Stati membri, consentita dall'art. 15, par. 1, della direttiva relativa alla vita privata e alle comunicazioni elettroniche[49].

7. La decisione-quadro 2008/977/GAI[50] è finalizzata alla protezione dei diritti e delle libertà fondamentali delle persone fisiche nell'eventualità che i loro dati

[49] Il Gruppo di lavoro "art. 29" si chiede se "l'intento della direttiva [sulla conservazione dei dati] sia quello di derogare all'obbligo generale di cancellare i dati relativi al traffico una volta conclusa la comunicazione elettronica, o di rendere obbligatoria la conservazione di tutti i dati che i fornitori sono già autorizzati a memorizzare ai fini delle loro attività commerciali".

[50] Decisione quadro 2008/977/GAI del Consiglio, del 27 novembre 2008, sulla protezione dei dati personali trattati nell'ambito della cooperazione giudiziaria e di polizia in materia penale, *GU* L 350 del 30.12.2008, p. 60.

personali siano trattati per scopi preventivi ed investigativi volti all'accertamento e al perseguimento dei reati o all'esecuzione delle sanzioni penali. Diversi strumenti che prevedono disposizioni specifiche per la protezione dei dati personali nei settori della cooperazione giudiziaria e di polizia in materia penale (ex terzo pilastro)[51].

La decisione-quadro riguarda il trattamento di dati personali interamente o parzialmente automatizzato, nonché il trattamento non automatizzato di dati personali presenti negli archivi. La decisione-quadro rispetta i principi di protezione dei dati stabiliti nella direttiva 95/46/CE e definisce una serie di regole supplementari in relazione alla particolarità del contesto peculiare della protezione dei dati nel settore di applicazione della legge.

La decisione-quadro è applicabile a tutte le situazioni rientranti nel terzo pilastro. Attualmente l'Europol e l'Eurojust hanno a loro disposizione sistemi di protezione dei dati ben definiti, compreso un sistema di sorveglianza, pertanto non vi è una immediata necessità di adeguare le disposizioni applicabili al testo della proposta di cui trattasi. Nel lungo periodo le norme sulla protezione dei dati applicabili all'Europol e all'Eurojust dovranno essere conformi pienamente alla decisione-quadro, considerando che la decisione quadro deve essere applicata alla raccolta e al trattamento dei dati personali trasmessi dagli Stati membri all'Europol e all'Eurojust.

La raccolta dei dati personali da parte dalle autorità competenti degli Stati membri può essere effettuata esclusivamente per finalità specifiche, esplicite e legittime; i dati devono essere trattati solo per la finalità per la quale sono stati raccolti, salvo che il trattamento per un fine diverso sia consentito in determinate circostanze e in presenza di adeguate garanzie. Il loro trattamento è ammesso soltanto se strettamente necessario e in presenza di adeguate garanzie assicurate dalla legislazione nazionale. Non è, invece, ammesso il trattamento di dati personali riguardanti la salute, la vita sessuale, l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche e l'appartenenza sindacale. Laddove risulti possibile e necessario i dati vengono rettificati, completati e aggiornati. Qualora non sussista più la finalità per cui i dati sono stati inizialmente raccolti, essi devono essere cancellati, anonimizzati e, in alcuni casi, possono essere "bloccati". Sono previsti adeguati termini per la cancellazione dei dati personali o per un esame periodico della necessità della memorizzazione dei dati.

Spetta alle autorità competenti degli Stati membri la verifica dell' esattezza e della completezza dei dati personali da trasmettere. Tutte le trasmissioni di dati personali devono essere registrate o documentate in modo tale che possa essere verificata la legalità del trattamento dei dati e assicurata l'integrità e la sicurezza degli stessi. Misure di sicurezza necessarie devono essere adottate dalle autorità

[51] V. l'elenco integrale di tali strumenti nell'allegato 3 della valutazione d'impatto (v. documento SEC(2012)72).

competenti per evitare che i dati personali siano soggetti a trattamento illegittimo, perdita accidentale, alterazione e a divulgazione o accesso non autorizzati. Misure specifiche devono essere disposte per il trattamento automatizzato dei dati.

Le autorità nazionali di controllo negli Stati membri sorvegliano e forniscono consulenza sull'applicazione della presente decisione quadro: ogni autorità di controllo dispone di poteri investigativi, di poteri effettivi d'intervento, nonché del potere di promuovere azioni giudiziarie. Inoltre gli Stati membri devono sanzionare in maniera efficace, proporzionata e dissuasiva le violazioni delle disposizioni della decisione quadro.

Tutti i dati personali raccolti, archiviati, trattati o analizzati ai fini dell'applicazione della legge possono formare oggetto di scambio in base al principio di disponibilità con le autorità competenti di un altro Stato membro. La disponibilità a scambiare i dati con le autorità di altri Stati membri (livello transnazionale) è garantito in misura proporzionale al livello di protezione dei diversi Stati membri. L'armonizzazione delle norme nazionali riguardanti i dati personali nel settore della polizia e della giustizia, compresa la garanzia della protezione dei dati suddetti, accresce la fiducia reciproca e l'efficacia degli scambi transnazionali.

Il trattamento dei dati personali ricevuti da un altro Stato membro è consentito soltanto per le stesse finalità della loro trasmissione. In alcuni casi, possono essere trattati per scopi diversi, quali la prevenzione, l'indagine, l'accertamento o il perseguimento di altri reati, l'esecuzione di altre sanzioni penali o la prevenzione di gravi minacce alla sicurezza pubblica. Lo Stato membro che trasmette i dati, in base a quanto previsto dalla propria legge interna, può imporre allo Stato ricevente l'osservanza di eventuali restrizioni relative allo scambio dei dati.

In determinate circostanze, lo Stato membro ricevente può trasferire i dati personali a paesi terzi o ad organismi internazionali. In questo caso, salvo i casi urgenti, il trasferimento necessita del consenso preliminare dello Stato che per primo ha trasmesso i dati. I dati personali possono anche essere trasmessi a privati negli Stati membri per finalità esclusive e a condizione che l'autorità competente dello Stato membro presso cui i dati sono stati ottenuti abbia acconsentito.

La persona interessata deve essere informata della raccolta o del trattamento di dati personali che la riguardano. Qualora siano stati trasmessi dati personali tra Stati, ciascuno Stato membro può chiedere che l'altro non informi la persona interessata. Ogni persona interessata ha il diritto di richiedere una conferma del fatto che dati che la riguardano siano stati trasmessi, nonché informazioni sui destinatari e sui dati che sono oggetto di trattamento e una conferma che sono state effettuate tutte le verifiche necessarie dei dati. L'accesso alle informazioni da parte della persona interessata può essere limitato dagli Stati membri soltanto in determinate circostanze. La persona interessata deve essere informata di qualsiasi decisione

restrittiva dell'accesso mediante comunicazione per iscritto, nonché dei motivi di fatto e di diritto sui quali la decisione è fondata. Alla persona interessata deve anche essere comunicata la possibilità di ricorrere contro tale decisione. É consentito alla persona coinvolta la richiesta di rettifica, cancellazione o blocco dei dati personali che la riguardano. Qualsiasi rifiuto di dar seguito a tali azioni deve essere comunicato per iscritto alla persona interessata. Nella comunicazione devono essere specificati i mezzi con cui la persona interessata può presentare ricorso o reclamo.

8. Il legislatore europeo ha esercitato la competenza in materia penale (art. 83, par. 1, TFUE) adottando una direttiva[52] volta a ravvicinare il diritto penale degli Stati membri nel settore degli attacchi contro i sistemi di informazione, stabilendo norme minime per la definizione dei reati e delle sanzioni rilevanti, per facilitare la prevenzione di tali reati e migliorare la cooperazione tra autorità giudiziarie e altre autorità competenti (art. 1).

A favore della sussistenza dei requisiti richiesti dall'art. 83, par. 1, TFUE (la particolare gravità ed il carattere transnazionale delle forme di criminalità) richiesti per l'intervento armonizzatore si afferma la pericolosità di attacchi ai sistemi d'informazione che fanno parte dell'infrastruttura critica degli Stati membri[53], che rappresenta una minaccia per la creazione di una società dell'informazione più sicura e di uno spazio di libertà, sicurezza e giustizia; la particolare dannosità di attacchi condotti su larga scala e con metodi sempre più sofisticati (come ad esempio le c.d. *botnet*), che possono comportare perturbazioni dei servizi di sistema di rilevante interesse pubblico, costi finanziari esorbitanti o perdita di dati personali o di informazioni sensibili, o ancora l'interruzione dei sistemi di informazione e delle comunicazioni sia attraverso la perdita o l'alterazione di informazioni riservate commercialmente importanti o di altri dati (anche se la determinazione della nozione di "danno grave" viene delegata ai legislatori nazionali).

La selezione delle condotte più gravi da sottoporre a sanzione penale viene poi operata mediante una previsione restrittiva con riguardo al criterio d'imputazione soggettiva, in quanto ricadono nell'ambito di operatività della direttiva i soli comportamenti connotati dal dolo (considerando n. 17) e con l'esclusione dei casi di minore gravità.

---

[52] Direttiva 2013/40/UE del Parlamento europeo e del Consiglio del 12 agosto 2013, relativa agli attacchi contro i sistemi di informazione e che sostituisce la decisione quadro 2005/222/GAI del Consiglio, pubblicata in *GUUE* L 218, 14 agosto 2013, p. 8.

[53] Il considerando 4 precisa cosa debba intendersi per infrastruttura critica di uno Stato, riferendosi ad "un elemento, un sistema o parte di questo […] che è essenziale per il mantenimento delle funzioni vitali della società, della salute, della sicurezza e del benessere economico o sociale delle persone, come gli impianti energetici, le reti di trasporto o le reti governative, e il cui danneggiamento o la cui distruzione avrebbe un impatto significativo in uno Stato membro a causa dell'impossibilità di mantenere tali funzioni".

Infine, il carattere transnazionale delle condotte oggetto degli obblighi di penalizzazione imposti dalla direttiva viene evidenziato nel considerando 27, sul rilievo del carattere transnazionale e senza frontiere dei moderni sistemi di informazione, che fa sì che gli attacchi contro tali sistemi abbiano una dimensione transfrontaliera, che rende evidente la necessità del ravvicinamento del diritto penale in questo settore.

Per quanto specificamente attiene alle condotte, gli obblighi di penalizzazione concernono in primo luogo le ipotesi di accesso intenzionale e senza diritto, vale a dire non autorizzato da parte del proprietario o da un altro titolare di diritti sul sistema o su una sua parte, ovvero non consentito a norma del diritto nazionale, ad un sistema di informazione o a una parte dello stesso, qualora sia commesso in violazione di una misura di sicurezza, prevedendo come soglia minima del massimo edittale una pena detentiva non inferiore a due anni (art. 3-Accesso illecito a sistemi di informazione).

Vengono poi previste le condotte di interferenza illecita relativamente ai sistemi e ai dati (artt. 4 e 5), che puniscono gli atti, compiuti intenzionalmente e senza diritto, rispettivamente "di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione di dati informatici, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di tali dati o rendendo tali dati inaccessibili" e "di cancellare, danneggiare, deteriorare, alterare, sopprimere dati informatici in un sistema di informazione, o di rendere tali dati inaccessibili". In questi casi, viene prevista come soglia minima del massimo edittale della pena base, una pena detentiva non inferiore a due anni, che viene aumentata a tre anni, se un numero significativo di sistemi di informazione è stato colpito avvalendosi di programmi, password, codici di accesso utilizzati per commettere una delle altre ipotesi previste dalla direttiva.

L'art. 6 della direttiva richiede invece che gli Stati configurino come reato l'interferenza illecita, consistente nel comportamento di chi intercetta intenzionalmente e senza diritto, tramite strumenti tecnici, trasmissioni non pubbliche di dati informatici verso, da o all'interno di un sistema di informazione, incluse le emissioni elettromagnetiche da un sistema di informazione che trasmette tali dati informatici, prevedendo come soglia minima del massimo edittale una pena detentiva non inferiore a due anni. Infine, lo stesso trattamento sanzionatorio viene stabilito per le condotte di fabbricazione, vendita, approvvigionamento per l'uso, importazione, distribuzione o messa a disposizione in altro modo intenzionali di un programma per computer, destinato o modificato principalmente al fine di commettere uno dei reati indicati dalla direttiva stessa ovvero di una password di un computer, di un codice d'accesso, o di dati simili che permettono di accedere in tutto o in parte a un sistema di informazione, qualora siano compiute senza diritto e con l'intenzione di utilizzarli al fine di commettere uno dei reati descritti dalla direttiva.

Il legislatore richiede altresì che risultino punibili le condotte di istigazione, favoreggiamento e più in generale di partecipazione concorsuale nei reati indicati ed il tentativo di questi ultimi, sottolineando anche la necessità di prevedere la responsabilità delle persone giuridiche per questi ultimi.

La direttiva in esame sembra porsi tendenzialmente nell'alveo del rispetto sia del principio di sussidiarietà, avendo essa stessa evidenziato l'indispensabilità di un intervento sovrannazionale con riguardo a forme di criminalità, quali sono gli attacchi informatici, caratterizzate dalla transnazionalità degli strumenti usati e delle implicazioni da esse derivanti; sia dei principi – inerenti a considerazioni di politica criminale proprie delle scelte di criminalizzazione – di necessità e proporzionalità di un intervento punitivo posto a tutela di un bene giuridico, quale l'integrità, il buon funzionamento e la sicurezza dei sistemi di informazione strettamente connesso tra l'altro alla tutela della riservatezza e alla protezione dei dati personali custoditi all'interno dei sistemi d'informazione, limitato alle sole condotte dolose connotate, come evidenziato, da una certa gravità.

In quanto all'obiettivo di armonizzazione delle legislazioni penali degli Stati perseguito dalla direttiva, la mancanza di nozioni comuni a livello sovrannazionale relative ai concetti di "casi di minore gravità", di "danno grave", nonché di norme della parte generale del diritto penale, concernenti il tentativo, la partecipazione, il regime delle circostanze, la determinazione ed esecuzione della pena, può di fatto frustrare tale obiettivo soprattutto con riguardo ai regimi sanzionatori concretamente applicabili nei diversi Stati membri.

Cap. II
La riforma della normativa generale in materia di protezione dei dati personali nel mercato interno

1. La riforma secondo l'impostazione della Commissione. – 2. Sussidiarietà, destinatari e beneficiari e poteri esecutivi. – 3. Lo status del responsabile del trattamento. – 4. Le deroghe ammissibili. – 5. Ricorsi e risarcimento danni. – 6. Proporzionalità e rischi con particolare riferimento alle PMI. – 7. La manifestazione del consenso del soggetto interessato. – 8. La specifica situazione del consenso per alcune categorie di dati (*opt–out*). – 9. Conservazione e informativa sui dati. – 10. Rettifica e oblio. – 11. Principali emendamenti del Parlamento europeo in prima lettura sulla proposta di regolamento in materia.

1. Il programma di Stoccolma (2009-14) evidenzia la necessità di istituire un "regime completo di protezione" e "rafforzare la posizione dell'UE in relazione alla protezione dei dati personali in tutte le politiche europee, anche nel contrastare e prevenire la criminalità".

L'*approccio globale* adottato in materia dall'Unione europea (2010)[54] stabiliva alcuni obiettivi prioritari di riforma, quali: il rafforzamento dei diritti delle persone (trasparenza e accesso/controllo dei dati personali da parte dell'individuo) e della dimensione del "mercato interno" (riduzione oneri amministrativi e condizioni eque per merce e servizio "informazioni"); la regolamentazione delle competenze delle autorità nazionali indipendenti per la protezione dei dati; una disciplina della cooperazione di polizia e giudiziaria in materia penale, in particolare la questione del trasferimento dei dati al di fuori dell'Unione.

Nella proposta di riforma[55], la Commissione si è concentrata su alcuni obiettivi prioritari: migliorare il mercato interno; garantire l'efficacia dell'esercizio del diritto da parte dei privati; istituire un quadro completo ed omogeneo in tutti i settori di competenza dell'Unione. Tra le istituzioni che hanno contribuito all'iter formativo: in particolare il Gruppo dell'Art. 29 (organo consultivo composto dai rappresentanti dell'autorità di protezione dei dati di ciascuno Stato membro, dal Garante europeo della protezione dei dati e dalla Commissione)[56].

La riforma della normativa in materia di protezione dei dati personali, presentata dalla Commissione europea il 25 gennaio 2012 comprende: una proposta di regolamento concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla

[54] COM(2010) 492 def., del 21 settembre 2010 sull'approccio globale al trasferimento dei dati del codice di prenotazione (Passenger Name Record, PNR) verso paesi terzi.

[55] La riforma della normativa in materia di dati personali è il risultato anche di due fasi di consultazione pubblica. Per i contributi della prima consultazione dal 9 luglio al 31 dicembre 2009. Per quelli della seconda dal 4 novembre 2010 al 15 gennaio 2011. I lavori di riforma hanno avuto come base la Risoluzione del Parlamento europeo del 6 luglio 2011 su un approccio globale in materia di protezione dei dati personali nell'Unione europea (2011/2025 (INI)).

[56] V. in particolare il parere n. 1/2013 adottato il 26 febbraio 2013 (doc. web n. 2980389) e i pareri n. 1/2012 e 8/2012 (doc. web nn. 2572831 e 2133818; v. Relazione 2012, p. 273), nei quali il Gruppo si è soffermato sulla proposta di direttiva della Commissione e sulla necessità di: rafforzare la tutela dei dati relativi a persone non sospette, vittime di reati e terze parti; ampliare l'esercizio dei diritti dell'interessato che non deve essere oggetto di deroghe ingiustificate; applicare il principio della verifica dell'impatto della privacy; rafforzare e specificare i poteri delle autorità di protezione dati in questo particolare ambito. Con il documento del 27 febbraio 2013 (doc. web n. 2980331), il Gruppo ha preso posizione su sei specifici settori del pacchetto di riforma ed in particolare sulla necessità di: mantenere un approccio omogeneo sul trattamento di dati effettuati in ambito privato e pubblico; considerare i "dati pseudonimi" come dati personali (applicando quindi anche ad essi i principi di protezione dati); specificare che il consenso dell'interessato deve essere "esplicito"; irrobustire il ruolo delle autorità nazionali di protezione dei dati e del Comitato europeo della protezione dati; rafforzare la tutela dei dati che siano oggetto di trasferimento verso Paesi terzi; mantenere l'approccio fondato sulla valutazione del rischio da parte dei titolari del trattamento.

protezione dei dati)[57]; una proposta di direttiva (Consiglio concernente la tutela della persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati)[58].

Nella proposta di riforma non rientrano le questioni relative allo specifico contesto delle comunicazioni elettroniche e relative all'uso del PNR, che saranno oggetto di successivi negoziati. Inoltre resta esclusa la materia di politica estera e di sicurezza comune che ha un diverso fondamento giuridico nell'art. 39 TUE[59].

La Commissione ricomprende nella proposta anche il settore pubblico per il crescente aumento dello scambio transfrontaliero in settori quali fiscalità, sicurezza sociale, sanità, banche e vigilanza sui mercati finanziari.

Le principali novità della disciplina proposta riguardano: la previsione che il consenso dell'interessato per l'utilizzo dei propri dati personali debba essere manifesto ed esplicito, escludendo in tal modo l'eventualità di un consenso tacito[60]; l'introduzione di garanzie per i dati relativi ai minori[61]; il rafforzamento del diritto alla cancellazione dei dati personali, quando siano venute meno le ragioni che ne consentivano l'utilizzo[62]; l'introduzione del diritto alla portabilità dei dati (vale a dire il diritto di trasferire i propri dati tra diversi sistemi elettronici senza che il responsabile del trattamento possa impedirlo)[63]; l'introduzione di disposizioni volte

---

[57] COM(2012)11 def., Proposta di regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati) che abroga la direttiva 95/46/CE

[58] COM(2012)10 def., Proposta di direttiva del Parlamento europeo e del Consiglio concernente la tutela della persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini della prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, che abroga la decisione quadro 2008/977/GAI

[59] Conformemente all'art. 16 del trattato sul funzionamento dell'Unione europea e in deroga al par. 2 di detto articolo, il Consiglio adotta una decisione che stabilisce le norme relative alla protezione delle persone fisiche con riguardo al trattamento dei dati di carattere personale da parte degli Stati membri nell'esercizio di attività che rientrano nel campo di applicazione del presente capo, e le norme relative alla libera circolazione di tali dati. Il rispetto di tali norme è soggetto al controllo di autorità indipendenti.

[60] V. art. 7 proposta di regolamento, cit. Per quanto riguarda il responsabile che effettua un trattamento di dati personali fondato sul consenso dell'interessato deve essere in grado di dimostrare il consenso di quest' ultimo. Specificamente nell'ambito di una dichiarazione scritta in riferimento ad un'altra materia, l'interessato deve essere informato del diritto e della misura con cui può esprimere il consenso. Il consenso è libero solamente nel caso in cui l'interessato può ritirarlo senza subire pregiudizio alcuno: infatti il consenso non costituisce una valida base giuridica per il trattamento dei dati personali qualora sia evidente uno squilibrio tra l'interessato e il responsabile del trattamento. Se il responsabile del trattamento è un'autorità pubblica, vi è squilibrio soltanto nelle specifiche operazioni di trattamento in cui l'autorità pubblica può imporre un obbligo in forza dei suoi pubblici poteri; in tal caso, il consenso non può essere considerato libero, tenuto conto degli interessi dell'interessato.

[61] V. art. 8 proposta di regolamento, cit.

[62] *Ivi*, articoli 16 e 17.

[63] *Ivi*, art. 18.

a dettagliare i limiti della tecnica di profilazione[64] utilizzata nelle attività di marketing per via informatica; la sostituzione dell'obbligo generalizzato di notifica alle autorità di controllo attualmente in vigore con un obbligo di notifica mirata alle operazioni che presentino rischi particolari (approccio basato sul rischio[65]); la previsione dell'obbligo di notificare e comunicare, entro termini prestabiliti, le eventuali violazioni dei dati personali che siano state evidenziate[66].

Un aspetto del tutto nuovo della proposta è il principio del cd. *one stop shop* (sportello unico) che individua un'unica autorità di controllo competente a controllare le attività del titolare del trattamento in tutta l'Unione, in modo da garantire la certezza giuridica e ridurre gli oneri amministrativi per i titolari del trattamento.

2. La proposta di regolamento mira ad ottenere un'uniforme applicazione delle disposizioni generali sulla protezione dei dati in tutto il territorio dell'UE. In relazione alla giustificazione della proposta di regolamento, il principio della sussidiarietà[67] giustifica l'intervento dell'Unione. Per quanto riguarda il requisito della dimensione trasfrontaliera, insito nel principio di sussidiarietà, è evidente la necessità di armonizzazione dal momento che norme diversificate a livello nazionale potrebbero apportare un grave pregiudizio in occasione del trasferimento di dati. In ogni caso, risulta di fondamentale importanza la cooperazione tra Stati e autorità nazionali a livello dell'Unione. La proposta è stata elaborata anche nel rispetto del principio di proporzionalità[68].

I beneficiari della tutela prevista dalla proposta di regolamento sono esclusivamente le persone fisiche a prescindere dalla nazionalità o dal luogo di residenza[69], ad esclusione cioè delle persone giuridiche. I destinatari degli obblighi sono invece gli operatori economici, siano micro, piccole e medie imprese[70].

---

[64] *Ivi*, art. 20.
[65] *Ivi*, articoli 35.
[66] *Ivi*, articoli 31 e 32.
[67] In virtù del principio di sussidiarietà, nei settori che non sono di sua competenza esclusiva, l'Unione interviene soltanto se e in quanto gli obiettivi dell'azione prevista non possono essere conseguiti in misura sufficiente dagli Stati membri, né a livello centrale né a livello regionale e locale, ma possono, a motivo della portata o degli effetti dell'azione in questione, essere conseguiti meglio a livello di Unione (art. 5 par. 3).
[68] In virtù del principio di proporzionalità, il contenuto e la forma dell'azione dell'Unione si limitano a quanto necessario per il conseguimento degli obiettivi dei Trattati (art. 5 par.4).
[69] Sono escluse dall'ambito di applicazione del presente regolamento le persone giuridiche ed in particolare le imprese dotate di personalità giuridica, compreso il nome, la forma giuridica e i contatti. Ciò vale anche quando il nome della persona giuridica contiene il nome di una o più persone fisiche.
[70]Per tener conto della specifica situazione delle micro, piccole e medie imprese, il regolamento prevede una serie di deroghe. Inoltre, le istituzioni e gli organi dell'Unione, gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese nell'applicare il presente regolamento. Il concetto di micro, piccola e media impresa deve ispirarsi alla raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla

La "pseudonimizzazione" dei dati personali è un'operazione frequente nel mondo digitale e uno dei mezzi più importanti per garantire la protezione dei dati nell'ambito di un approccio fondato sul rischio[71]. Il dibattito a livello tecnico ha portato all'inserimento della "pseudonimizzazione" nella proposta di regolamento al fine di limitare l'impatto sui diritti individuali e rafforzare la sicurezza dei dati. Contribuirà a stabilire il giusto equilibrio tra la tutela dei diritti e delle libertà fondamentali delle persone fisiche interessate e l'esigenza del settore pubblico e privato di trattare grandi quantità di dati.

Una questione di grande rilievo giuridico è poi quella del campo di applicazione territoriale. Qualsiasi trattamento di dati personali effettuato nell'ambito delle attività di uno stabilimento di un responsabile del trattamento (o incaricato del trattamento) nel territorio dell'Unione deve essere conforme al regolamento, sia che il trattamento avvenga all'interno dell'Unione che al di fuori. Lo stabilimento implica l'effettivo e reale svolgimento di attività nel quadro di un'organizzazione stabile. A tale riguardo, non è determinante la forma giuridica assunta, sia essa una succursale o una filiale dotata di personalità giuridica. Onde evitare che una persona fisica venga privata della tutela cui ha diritto in base al presente regolamento, è necessario che questo disciplini anche il trattamento dei dati personali di residenti nell'Unione effettuato da un responsabile del trattamento non ivi stabilito, quando le attività di trattamento sono legate all'offerta di beni o servizi a dette persone indipendentemente dal fatto che vi sia un pagamento[72].

Alcune perplessità nei confronti della disciplina della proposta di regolamento si hanno anche in relazione al potere riconosciuto alla Commissione di adottare atti delegati per colmare eventuali vuoti legislativi[73] e sul sistema sanzionatorio[74].

Il continuo riferimento a norme di attuazione può ridurre l'efficacia diretta della misura legislativa prescelta e mina la stabilità giuridica della stessa. Pertanto per i settori essenziali della disciplina sarebbe preferibile non ricorrere alla legislazione delegata. Le sanzioni amministrative applicabili risultano sproporzionate in relazione agli illeciti amministrativi contemplati[75] ed è pertanto auspicabile una

---

definizione delle microimprese, piccole e medie imprese (in *GU* L 124 del 20 maggio 2003).

[71] Un esempio di pseudonimizzazione potrebbe essere rappresentato dal caso in cui i dati medici di pazienti malati di cancro siano sottoposti ad un processo di eliminazione degli elementi identificativi diretti, quali il nome, e di attribuzione casuale di numeri di serie a ciascun paziente, in modo che le informazioni così ottenute possano essere utilizzate a fini di ricerca medica o di salute pubblica.

[72] Sulla questione, v. G. CAGGIANO, *L'interpretazione del "contesto delle attività di stabilimento" dei responsabili del trattamento dei dati personali*, in *Dir. Inf. e informatica*, 2014, p. 615 ss.

[73] V. ad esempio gli articoli 9, par. 3; 14, par. 7); 17, par. 9; 22, par. 4). Il progetto di relazione del PE nonostante alcune modifiche ai profili di intervento della Commissione (Emendamenti nn. 104, 144, 186,191), ne lascia sostanzialmente impregiudicato l'ambito di azione.

[74] L'art. 79 della proposta di regolamento, confermato anche dal progetto di Relazione parlamentare, prevede sanzioni amministrative pecuniarie particolarmente elevate (fino al 2% del fatturato mondiale annuo).

[75] L'applicazione di una sanzione amministrativa deve essere specificata la natura, la gravità, la

revisione dei massimi edittali.

Il diritto alla portabilità dei dati mira a permettere alle persone fisiche di trasferire i loro dati personali da un prestatore all'altro quando decidono di optare per un altro prestatore (ad es. trasmissione dei dati di una persona fisica relativi alla sua esperienza professionale da una rete sociale a finalità generale ad una rete orientata alla carriera professionale). Le discussioni hanno mostrato l'importanza che il diritto alla portabilità dei dati riveste per consentire alle persone fisiche di avere il controllo sui loro dati, specie su Internet e per modernizzare il quadro attuale.

Sulla profilazione[76] l'attuale compromesso non introduce un regime specifico. Esso assoggetta tali attività alle norme generali che disciplinano il trattamento dei dati personali (basi giuridiche del trattamento, principi di protezione dei dati) con specifiche garanzie (ad esempio, obbligo di effettuare una valutazione d'impatto in alcuni casi, v. articoli 33 e 34) o disposizioni relative alle informazioni specifiche da fornire alla persona fisica interessata. Il comitato europeo per la protezione dei dati avrebbe la possibilità di emanare orientamenti in tale contesto.

L'automazione della decisione dovrebbe essere consentita solo se necessaria per la conclusione o l'esecuzione di un contratto, sulla base di un esplicito consenso dell'interessato o qualora esplicitamente autorizzata dal diritto dell'Unione o di uno Stato membro, incluso per la prevenzione delle frodi e dell'evasione fiscale e a fini di monitoraggio. La profilazione e l'automazione della decisione basate su categorie particolari di dati personali dovrebbero essere consentite solo a determinate condizioni.

3. La proposta di regolamento ha precisato la responsabilità generale del responsabile del trattamento. Quest'ultimo infatti ha l'obbligo di fornire ai soggetti interessati informazioni trasparenti, comprensibili e facilmente accessibili (art. 11 della proposta)[77]. Il responsabile del trattamento deve specificare per quanto tempo

---

durata, il carattere doloso o colposo della violazione, il grado di responsabilità, comportamenti precedenti del titolare, adozione delle misure di prevenzione e grado di cooperazione con l'autorità di controllo per rimediare alla violazione.

[76] Nell'era digitale molte attività economiche si basano sulla creazione e utilizzazione di taluni profili. Perciò la pubblicità via internet, che rappresenta in se stessa un importante fondamento economico di Internet, è spesso basata sulla creazione e l'utilizzazione di taluni profili per finalità di marketing. La creazione e l'utilizzazione di profili degli utenti può essere anche impiegata per tutelare questi ultimi, ad es. da frodi legate alle carte di credito o da altri tipi di frode in un ambiente digitale. Tuttavia, il trattamento inteso a valutare (ossia, analizzare e prevedere) taluni aspetti relativi al rendimento professionale, alla situazione economica, allo stato di salute, alle preferenze personali o agli interessi, all'affidabilità o al comportamento, all'ubicazione o agli spostamenti (profilazione) possono comportare gravi rischi per i diritti e le libertà delle persone fisiche. In virtù della direttiva del 1995 (art. 15), già esiste una disposizione sul diritto di una persona di non essere sottoposta ad una decisione fondata esclusivamente su un trattamento automatizzato e che produca effetti giuridici o abbia effetti significativi nei suoi confronti in considerazione di alcuni dei suddetti aspetti.

[77] Tale disposizione si ispira in particolare alla risoluzione di Madrid sulle norme internazionali sulla protezione dei dati personali e della vita privata, adottata il 5 novembre 2009 dalla Conferenza

devono essere conservati i dati e se saranno oggetto di trasferimenti internazionali[78] D'altro canto il soggetto interessato dal trattamento dei dati deve essere messo in condizione di presentare un eventuale reclamo e di usufruire delle misure idonee[79] per l'esercizio dei propri diritti.

Nella proposta di regolamento è sancito il diritto all'oblio (art. 17)[80]. Il responsabile del trattamento è obbligato ad informare i terzi della richiesta di cancellazione di copie, riproduzioni di dati e link che consentono il collegamento ai dati del soggetto interessato. Il trattamento inoltre deve essere limitato a casi specifici senza ricorrere al c.d. "blocco dei dati".

Una nuova possibilità consentita è la predisposizione di certificazioni, marchi e sigilli per la tutela dei dati (art. 39 della proposta).

4. Sulla base dell'art. 9 della direttiva 95/46/CE e della giurisprudenza della Corte di giustizia[81], i dati trattati per finalità giornalistiche o di espressione artistica o letteraria possono essere soggetti a deroghe previste dagli Stati membri nel rispetto sia del diritto fondamentale alla protezione dei dati e sia del diritto alla libertà di espressione[82]: ogni deroga presuppone un operazione di bilanciamento tra diritti fondamentali in conflitto.

I dati sanitari devono essere trattati in base a disposizioni specifiche dell'UE o degli Stati membri nel rispetto degli interessi legittimi dell'interessato[83]. Un professionista della sanità o altra persona equiparata che effettui un trattamento di dati è vincolato dall'obbligo di segretezza ai sensi della legislazione degli Stati membri o delle regole degli organismi nazionali competenti.

Il trattamento di dati personali riguardante la salute necessari a scopi storici,

---

internazionale dei commissari in materia di protezione dei dati e della vita privata. V. anche l'art. 13, par. 3, della proposta di regolamento relativo a un diritto comune europeo della vendita (COM(2011)635 def.).

[78] Sono mantenute le deroghe previste dalla direttiva 95/46/CE, per cui l'obbligo di informazione non si applica se la registrazione o la divulgazione dei dati sono espressamente previste per legge. Ciò può avvenire, ad esempio, nei procedimenti avviati dalle autorità per la concorrenza, da un'amministrazione fiscale o doganale o dai servizi di sicurezza sociale

[79] Ai sensi dell'art.12 il soggetto interessato può introdurre le richieste per via elettronica/telematica e il responsabile del trattamento ha l'obbligo di rispondere entro un termine determinato e di motivare un eventuale rifiuto.

[80] Tale disposizione specifica il diritto alla cancellazione di cui all'art. 12, lett. b), della direttiva 95/46/CE.

[81] Per l'interpretazione, si veda ad esempio la sentenza della Corte del 16 dicembre 2008, causa C-73/07, *Tietosuojavaltuutettu/Satakunnan Markkinapörssi Oy, Satamedia Oy*, in *Racc.*, p. I-9831.

[82] Le esenzioni o le deroghe possono riguardare le disposizioni concernenti i principi generali di cui al capo II, i diritti dell'interessato di cui al capo III, il responsabile del trattamento e l'incaricato del trattamento di cui al capo IV, il trasferimento di dati personali verso paesi terzi ed organizzazioni internazionali di cui al capo V, le autorità di controllo indipendenti di cui al capo VI e la cooperazione e la coerenza di cui al capo VII.

[83] Ai sensi dell'art. 81 le finalità che giustificano il trattamento dei dati sanitari possono variare dalla prevenzione medica, alla diagnosi, all'assistenza sanitaria, alla terapia, alla gestione dei servizi sanitari.

statici o di ricerca scientifica è soggetto alle condizioni e alle garanzie previste (art. 83 della proposta)[84]. L'accesso da parte delle autorità di controllo ai dati personali e agli edifici è regolato dagli Stati membri dispongano norme specifiche a tal fine (art. 84).

5. La disciplina dei ricorsi giurisdizionali proponibili nei confronti di un'autorità di controllo, del responsabile o dell'incaricato del trattamento[85] da parte dell'interessato, di associazioni e organismi per la tutela dei dati non si discosta dalla direttiva vigente (articoli 22 e 28)[86].

L'autorità di controllo, avverso la quale è stato presentato un ricorso, agisce nel rispetto delle competenza giurisdizionale che è attribuita ai giudici dello Stato membro in cui ha sede l'autorità di controllo. Possono agire legalmente in nome dell'interessato, nello Stato membro in cui si trova l'autorità di controllo competente, anche le autorità di controllo dello Stato membro di residenza dell' interessato in caso di violazioni delle disposizioni del regolamento in parola.

La disciplina introdotta dagli articoli 77 e 78 prescrive l'obbligo al risarcimento del danno anche per gli incaricati del trattamento, chiarisce la responsabilità dei corresponsabili e coincaricati del trattamento e definisce le sanzioni applicabili per le violazioni del regolamento.

6. Nella sua proposta, la Commissione prevede di alleviare alcuni degli oneri amministrativi, prevedendo che le piccole e medie imprese (con meno di 250 dipendenti) beneficino di una deroga ad alcuni degli obblighi previsti (per es. art. 28 sugli obblighi in materia di documentazione) e, d'altra parte, collegando determinati obblighi al carattere rischioso del trattamento (per es. art. 33 relativo alla valutazione d'impatto sulla protezione dei dati). In alcuni altri casi, questo approccio è combinato (per es. per quanto riguarda la designazione del responsabile della protezione dei dati all'art. 35).

Vi è un consenso generale a favore di un'impostazione basata maggiormente sui rischi. Questa impostazione dovrà creare un equilibrio tra due elementi distinti ossia, da un lato, l'eventuale pregiudizio all'interessato in relazione ai suoi diritti e libertà

[84] Secondo la proposta di regolamento, i dati personali possono essere trattati per finalità storiche, statistiche e di ricerca scientifica solo se: a) tali finalità non possono essere altrimenti conseguite trattando dati che non consentono o non consentono più di identificare l'interessato; b) i dati che permettono di associare informazioni a un interessato identificato o identificabile sono conservati separatamente dalle altre informazioni, nella misura in cui tali finalità possano essere conseguite in questo modo.

[85] Ai sensi dell'art. 75 è consentita la scelta tra il ricorso al giudice dello Stato membro in cui è stabilito il ricorrente e quello in cui risiede l'interessato. Se più procedimenti riguardanti la stessa misura sono in corso nell'ambito del meccanismo di coerenza, il giudice può sospendere il procedimento, salvo casi d'urgenza.

[86] V. art. 73 e seguenti.

individuali (per es. danno alla reputazione, discriminazione, perdite finanziarie, furto di identità) e, dall'altro, i fattori che possono influire sulla probabilità che un pericolo possa effettivamente concretizzarsi.

Si tratta di un importante aspetto della proporzionalità ma, all'atto di decidere sull'esatta definizione degli obblighi in materia di protezione dei dati nel progetto di regolamento, occorrerà evidentemente soppesare il rischio in relazione alla libertà imprenditoriale (settore privato) e le funzioni svolte dalle autorità pubbliche (settore pubblico). Sembra esservi un consenso generale tra gli Stati membri sul fatto che il regolamento generale sulla protezione dei dati proposto dovrebbe seguire un approccio basato sui rischi, secondo il quale gli obblighi dei responsabili del trattamento e degli incaricati del trattamento devono essere ponderati, in particolare in relazione alla natura del trattamento e dei dati trattati nonché all'impatto su diritti e libertà delle persone.

La proposta di regolamento offre già un esempio di valutazione dei rischi e contestualizzazione degli obblighi giuridici, in particolare per quanto riguarda l'obbligo di effettuare valutazioni d'impatto sulla protezione dei dati (progetto di art. 33).

Un approccio basato sul rischio può anche essere descritto come uno sforzo volto a ridurre le violazioni dei dati. Nel contesto di questo approccio alla definizione delle norme sulla protezione dei dati è importante determinare chi debba valutare e sostenere l'onere di ridurre il rischio di violazioni dei dati. Alcune delegazioni sostengono che gli interessati hanno l'obbligo preciso di comportarsi in modo responsabile per evitare o ridurre al minimo alcuni dei rischi connessi a determinati tipi di trattamento dei dati, per esempio nell'uso dei social media.

La proposta della Commissione contiene già alcuni elementi riguardanti la responsabilità dei responsabili del trattamento dei dati (in particolare l'obbligo di effettuare una valutazione d'impatto sulla protezione dei dati ex art. 33), ma alcune delegazioni sostengono che occorrerebbe porre maggiormente l'accento sulla responsabilità dei responsabili del trattamento in quanto essi sono nella posizione migliore per valutare il rischio connesso a determinate operazioni di trattamento dei dati.

E' stato espresso il parere che un approccio in base al quale i responsabili del trattamento sono incoraggiati a intraprendere azioni basate sui rischi, mirate e proporzionate per proteggere i dati personali (art. 22, par. 3) e sono ritenuti responsabili per eventuali violazioni dei dati, può produrre risultati migliori rispetto a una serie di prescrizioni che possono tradursi nell'atteggiamento di chi si limita a "riempire caselle" con uno scarso aumento in termini di protezione dei dati.

Perplessità sorgono in merito all'esclusione delle imprese dall'ambito di applicazione del regolamento[87]. L'esclusione sembra riferirsi solamente alle imprese

[87] Il Considerando n. 12 della proposta di regolamento (confermato anche dalla proposta di

dotate di personalità giuridica e non generalmente ai soggetti che esercitano un'attività economica a prescindere dalla forma giuridica rivestita o dal riconoscimento della personalità[88]. Di conseguenza sarebbero escluse dall'ambito di applicazione del regolamento le imprese con personalità giuridica ed inclusi gli imprenditori individuali. La scelta del requisito della personalità giuridica come unico fondamento di distinzione ed esclusione di un soggetto economico al quale si riferiscono i dati sembra non essere giustificato da specifiche esigenze di protezione. Un soggetto economico tratta dati personali a prescindere dalla personalità giuridica con la probabilità di incorrere negli stessi rischi[89].

7. Troppo rigido risulta l'approccio alle modalità di manifestazione del consenso[90]. Infatti nel regolamento le disposizioni in materia sono circoscritte esclusivamente ai trattamenti di dati sensibili[91]. Il prerequisito del consenso esplicito potrebbe avere come conseguenza da parte dei titolari del trattamento l'uso del sistema preventivo dell'*opt–in*, vale a dire del consenso esplicito preventivo senza distinguere la categoria di dati trattati e gli obiettivi da raggiungere e senza la possibilità di beneficiare del sistema più flessibile dell'*opt–out* che prevede l'esonero dal consenso. Sarebbe opportuno a tale riguardo ricorrere a sistemi più versatili al passo con la continua evoluzione dell'economia digitale[92].

La semplificazione degli adempimenti in tema di privacy relativi alla manifestazione del consenso può avvenire attraverso l'adeguamento degli stessi ai rischi collegati ai diversi tipi di trattamento e alle relative finalità. Ad esempio, potrebbero essere esonerate dalla manifestazione del consenso le comunicazioni di dati personali svolte nell'ambito di gruppi o di altre forme organizzate di attività di

---

regolamento del Parlamento europeo e del Consiglio concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) precisa che la tutela offerta dal regolamento non può essere invocata per il trattamento dei dati delle persone giuridiche, "in particolare delle imprese dotate di personalità giuridica, compreso il nome, la forma giuridica e i contatti", anche quando il nome della persona giuridica contiene il nome di una o più persone fisiche.

[88] V. art. 4, n. 15 della proposta di regolamento, cit.

[89] "Pertanto, al fine di semplificare e uniformare gli adempimenti privacy connessi allo svolgimento delle attività economiche, sarebbe necessario estendere l'esclusione dal campo di applicazione del regolamento al concetto più ampio di impresa e sopprimere dal testo del considerando n. 12 le parole e, in particolare e dotate di personalità giuridica", v. Documento di Confindustria "Osservazioni al progetto di Relazione del Parlamento Europeo sulla proposta di Regolamento in materia di protezione dei dati personali" dell'11 marzo 2013.

[90] Il Considerando n. 25 e l'art. 4, n. 8 della proposta di regolamento, confermati anche dal progetto di Relazione parlamentare prevedono che il consenso al trattamento deve essere manifestato in maniera esplicita. Inoltre, il considerando n. 25 precisa che non costituisce consenso quello manifestato tacitamente ovvero passivamente.

[91] V. art. 8, par. 2, lett. a) della direttiva 45/96/CE.

[92] Si auspica l'eliminazione del riferimento al consenso esplicito dal Considerando n. 25 e dall'art. 4, n. 8, al fine di rendere le modalità di autorizzazione al trattamento più flessibili e applicabili nella pratica, v. Confindustria "Osservazioni al progetto di Relazione del Parlamento Europeo, cit.

impresa[93] per agevolare la circolazione di informazioni sensibili. In aggiunta i dati trattati per la gestione accentrata dei servizi di tesoreria o di amministrazione nei gruppi o per lo svolgimento di progetti formativi per tutti i dipendenti di un'azienda non necessitano della comunicazione del consenso[94]. Per rendere le procedure più snelle si possono eliminare gli obblighi di informativa e consenso preventivo per il trattamento dei dati inseriti volontariamente nei *curricula vitae*[95].

Un'ulteriore considerazione merita la non chiara espressione "notevole squilibrio" tra la posizione del titolare e l'interessato: in tal caso, nonostante la manifestazione del consenso[96], il trattamento sarebbe illegittimo. L'espressione riguarda i rapporti di lavoro dove l'interessato è in posizione di dipendenza rispetto al titolare. A tale riguardo il notevole squilibrio esclude ogni possibilità di trattamento dei dati poiché in presenza di tale condizione sarebbero nulli anche gli esoneri dal consenso per l'adempimento di obblighi contrattuali o previsti dalla legge[97]. Se così fosse la disciplina del consenso risulterebbe d'ostacolo all'esecuzione di un elevato numero di rapporti contrattuali e ne bloccherebbe lo svolgimento[98].

8. Ai trattamenti riguardanti attività promozionali effettuate mediante posta cartacea o porta a porta si applica il sistema dell'*opt–in*[99] che prevede l'adempimento di diversi oneri. In tale settore contrattuale per agevolare il *direct marketing*, nel caso di trattamenti che non necessitano del consenso dell'interessato, è preferibile l'applicazione di un regime meno oneroso come quello dell'*opt–out*[100] che consentirebbe di ridurre gli oneri connessi alla privacy a carico delle imprese. A tal proposito, va sottolineato che il *direct marketing* costituisce un mezzo fondamentale di comunicazione per la promozione di beni e servizi a costi contenuti

[93] V. ad esempio per le reti d'impresa, come attualmente previsto in Italia dal Codice privacy ai sensi dell'art. 24, par. 1, lett. i-ter) del d.Lgs n. 196/2003.

[94]Analoga conclusione per quelli trattati per finalità di partecipazione o esecuzione di attività imprenditoriali in forma congiunta (è il caso delle attività svolte da consorzi, reti di imprese, RTI o ATI aggiudicatrici di appalti).

[95] Un soggetto che riceve un CV "spontaneo"si trova nell'impossibilità di fornire l'informativa preventiva all'interessato e il soggetto che lo invia manifesterebbe un consenso non informato.

[96] V. considerando n. 34 e l'art. 7, par. 4 della proposta di regolamento, cit.

[97] V. art. 6, par. 1, lettere b) e c).

[98] Si pensi, infatti, ai rapporti lavorativi e ai rapporti con i consumatori che, per effetto della nuova previsione, risulterebbero sostanzialmente bloccati.

[99] Il considerando n. 57 e l'art. 19, par. 2 della proposta di regolamento estendevano il regime di *opt-out* ai trattamenti effettuati per finalità di *marketing* diretto. Tale principio era da considerarsi limitato al *marketing* mediante posta cartacea e al *marketing door-to-door*, in quanto alle attività promozionali effettuate tramite comunicazione elettronica (es. telefonate con o senza l'intervento di un operatore, email, fax) continuavano ad applicarsi le disposizioni della direttiva *E-privacy* (2002/58/CE), fatte salve dallo stesso regolamento (considerando n. 135 e art. 89). Tuttavia, il progetto di Relazione parlamentare ha eliminato da tali disposizioni il riferimento al *marketing* diretto (emendamenti n. 37 e n. 156).

[100] Emendamento n. 101 del progetto di relazione sulla proposta di regolamento (gennaio 2013).

rispetto a quelli necessari per l'acquisto di spazi pubblicitari su giornali, TV e radio. Pertanto un regime di *opt–out* è in grado di soddisfare le aspettative di protezione dell'interessato che deve ricevere le informazioni relative alle caratteristiche del trattamento e alla possibilità di opposizione allo svolgimento di *direct marketing* nei suoi confronti[101].

La proposta di regolamento privilegia l'*opt–in* per tutte le attività di *profiling* e anche in questo caso sarebbe opportuno diversificare i trattamenti a secondo delle finalità e della natura dei dati trattati[102] in riferimento alle diverse tipologie di attività di profilazione e dei rischi connessi. Alle attività meno rischiose è auspicabile l'applicazione di un regime più flessibile, come l'*opt–out*, e proporzionato con gli interessi del titolare e del soggetto coinvolto dal trattamento dei dati. Le imprese che forniscono beni e servizi sul web o tramite posta possono ricorrere alla profilazione per il soddisfacimento dei reali bisogni dei consumatori. Infatti l'offerta da parte di un'impresa va ponderata in relazione ai reali bisogni dei soggetti interessati. La semplificazione degli adempimenti di privacy attraverso il regime di *opt–out* può risultare più vantaggiosa per i consumatori sul presupposto che vengano rispettati gli obblighi di informativa e garantito il diritto di opposizione.

9. Ai sensi dell'art. 13 della proposta di regolamento[103], il titolare deve comunicare all'interessato i soggetti che si occuperanno della rettifica e cancellazione dei dati. Tale tipo di adempimento potrebbe rivelarsi eccessivamente oneroso per il titolare e inutile per la protezione dei dati.

Il titolare del trattamento dei dati è già soggetto all'obbligo generale di specificare i destinatari dei dati all'interno dell'informativa sulla privacy (art. 14, par. 1, lett. f)[104].

Il diritto di ricevere comunicazioni da parte del soggetto interessato dal trattamento dei dati è ampiamente tutelato dall'intero regolamento.

Le misure predisposte per assicurare la liceità dei trattamenti da parte del titolare

---

[101] Al fine di ridurre gli oneri derivanti dallo svolgimento di attività di *marketing* diretto, sarebbe opportuno ripristinare l'originaria formulazione del considerando n. 57 e dell'art. 19, par. 2, v. documento di Confindustria, Osservazioni al progetto di Relazione del Parlamento Europeo sulla proposta di Regolamento in materia di protezione dei dati personali.

[102] Ai sensi del considerando n. 58 e dell'art. 20 della proposta di regolamento è vietato lo svolgimento delle attività di *profiling*, a meno che: non avvenga nel contesto della conclusione ovvero dell'esecuzione di un contratto; non sia espressamente autorizzato da un atto normativo europeo o nazionale; l'interessato abbia manifestato il proprio consenso (*opt-in*). La prima ipotesi di liceità è stata limitata a livello dall'intervento del progetto di Relazione parlamentare. L'emendamento n. 160 dispone che in un rapporto contrattuale la profilazione è lecita solo se è necessaria per la conclusione o l'esecuzione del contratto. Pertanto, in riferimento alla profilazione "contrattuale", i margini di intervento del titolare risultano notevolmente ridimensionati.

[103] Versione modificata dall'emendamento n. 124 del progetto di relazione del Parlamento europeo.

[104] L'interessato ha diritto ad essere informato anche della trasmissione dei dati a soggetti terzi (art. 15, par. 1, lett. c)).

sono analizzate da revisori interni ed esterni che ne garantiscono l'efficacia e la conformità con il regolamento[105]. Con tale tipo di previsione il titolare del trattamento rischia di essere soggetto ad un onere amministrativo eccessivo poiché è costretto a ricorrere a soggetti indipendenti per esaminare l'adeguatezza degli strumenti adottati. Il titolare deve essere libero di scegliere di determinare i meccanismi di audit e in caso di violazione anche la relativa responsabilità al fine di poter dimostrare l'adeguatezza delle misure[106]. Inoltre, in base a quanto disposto dal regolamento, il titolare del trattamento dei dati deve essere in grado di dimostrare di aver fatto ricorso a tutti gli strumenti possibili per evitare il danno e che non sia dipeso dalla sua negligenza[107].

Il titolare del trattamento è soggetto ad un ulteriore obbligo che consiste nella conservazione dei documenti di ogni trattamento effettuato[108] e che sostituisce quello di notifica all'autorità di controllo con l'intento di semplificazione della procedura a carico dei titolari[109]. In realtà la previsione normativa appena descritta rischia di introdurre nuovi adempimenti burocratici che gravano su coloro che trattano i dati. La disciplina attuale limita l'obbligo di notificazione esclusivamente ai trattamenti rischiosi[110]; al contrario, la proposta di regolamento prevede l'obbligo di conservazione e compilazione dei documenti di tutti i trattamenti effettuati. Pertanto le imprese sarebbero obbligate inutilmente in termini di protezione dei dati a compilare giornalmente centinaia di documenti in quanto sono già soggette all'obbligo generale di conformità[111] con il regolamento di ogni trattamento che svolgono. Di conseguenza, tutti coloro che trattano i dati devono rispettare gli obblighi generali di informativa e consenso a prescindere dal nuovo obbligo di conservazione introdotto dalla proposta di regolamento.

L'attuale fattispecie della violazione dei dati, disciplinata dalla direttiva 2002/58/CE e dalla direttiva n. 136/2009/CE, è circoscritta ai soli trattamenti effettuati nell'ambito delle comunicazioni elettroniche. Al contrario, ai sensi dell'art. 31 della proposta di regolamento, ogni tipologia di trattamento dei dati può essere causa di violazione di dati[112]. Pertanto, qualsiasi violazione che si verifichi

---

[105] V. art. 22, par. 3 del regolamento confermato anche dall'Emendamento n. 173 del progetto di relazione del Parlamento europeo che specifica che le attività di *audit* devono essere svolte da soggetti indipendenti.

[106] Quanto descritto si verifica anche attualmente in riferimento agli adempimenti previsti dalle norme nazionali.

[107] V. art. 77 della proposta di regolamento, cit.

[108] V. art. 28 della proposta di regolamento, cit., confermato dal progetto di Relazione del Parlamento europeo. Specificamente in base a quanto previsto dall'art. 14, i documenti devono contenere le stesse informazioni oggetto dell'informativa.

[109] V. a tal proposito la relazione di accompagnamento allo schema di regolamento.

[110] V. artt. 18 e 19 della direttiva 95/46/CE.

[111] V. art. 22, par. 1.

[112] La previsione è confermata anche dal progetto di Relazione parlamentare, che sul tema non prevede modifiche di natura sostanziale.

durante il trattamento deve essere notificata all'autorità di controllo e comunicata all'interessato da parte del titolare che in tal modo è costretto all'adempimento di ulteriori oneri informativi[113]. La nozione di violazione dei dati così generalizzata è sicuramente sproporzionata per i trattamenti che non presentano particolari rischi.

È chiaramente deducibile dalle considerazioni precedenti che la proposta di regolamento amplia gli obblighi a carico del titolare del trattamento rispetto all'attuale disciplina: infatti è stata introdotta per i trattamenti rischiosi la cosiddetta "valutazione d'impatto privacy"[114].

La proposta di regolamento ha classificato i sistemi di videosorveglianza come trattamenti rischiosi che richiedono la valutazione d'impatto della privacy. Considerata l'ampia diffusione dei sistemi di videosorveglianza sia in contesti pubblici che privati appare alquanto anacronistica l'inclusione degli stessi nella categoria dei trattamenti pericolosi.

È fatto obbligo per il titolare di nominare un *privacy officer* vale a dire un responsabile della protezione quando i dati sono trattati da persona giuridica, riguardano annualmente molti interessati e il trattamento dei dati in parola richiede un controllo regolare e sistematico[115].

Il responsabile controlla il rispetto degli obblighi previsti dal regolamento e si relaziona con l'autorità di controllo[116]. Sono altresì regolamentati dettagliatamente sia gli aspetti meramente organizzativi che i rapporti tra titolare e responsabile con una conseguente compressione dell'autonomia privata a scapito delle parti[117]. Nel rapporto tra titolare e responsabile è necessario che ci sia un giusto equilibrio tra le diverse funzioni del titolare e del *privacy officer* in considerazione delle esigenze di semplificazione e dell'autonomia negoziale[118].

10. Il concetto di "diritto all'oblio" si riferisce al diritto alla cancellazione, al blocco, al congelamento dei dati o all'opposizione al trattamento dei dati previsti

---

[113] V. art. 32 della proposta di regolamento, cit.

[114] Ai sensi dell'art. 33, la valutazione deve avere per oggetto il trattamento previsto, i rischi connessi e la definizione delle misure adottate al fine di evitare i rischi e assicurare la tutela dei dati. Inoltre il progetto di Relazione parlamentare introduce gli emendamenti nn. 205, 206, 207, 208 e 209 che modificano il testo della norma con la specifica dei trattamenti che possono definirsi rischiosi.

[115] V. art. 35, par. 1 della proposta di regolamento, nel testo emendato dal progetto di relazione del Parlamento europeo (emendamento n. 223).

[116] V. art. 37 della proposta di regolamento, cit.

[117] I paragrafi 7, 8 e 9 dell'art. 37 prevedono per il titolare limiti e condizioni obbligatorie per la nomina del *privacy officer*, ad esempio la durata di almeno quattro anni del mandato; i casi di revoca qualora non siano soddisfatte le condizioni richieste; le modalità di affidamento dell'incarico e gli obblighi informativi nei confronti dell'autorità di controllo e del pubblico. Tali disposizioni andrebbero ridimensionate alla luce della libertà di impresa economica.

[118] A titolo esemplificativo, si richiama la previsione secondo cui il *privacy officer* è un subalterno diretto dei superiori gerarchici del titolare e non già di quest'ultimo (art. 36, par. 2, v. emendamento n. 229). Non si comprende la *ratio* di tale previsione, che andrebbe eliminata, specie se si considera che il rapporto tra i citati soggetti è riconducibile al contratto di mandato.

dalla direttiva 95/46/CE. Vi si dispone, con riguardo al diritto di accesso ai dati da parte della persona interessata che "gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: a) liberamente e senza costrizione, ad intervalli ragionevoli e senza ritardi o spese eccessivi (…) b) a seconda dei casi, la rettifica, la cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati" (art. 12).

La medesima direttiva disciplina il diritto di opposizione della persona interessata e dispone che "gli Stati membri riconoscono alla persona interessata il diritto: a) almeno nei casi di cui all'articolo 7, lettere e) e f), di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale. In caso di opposizione giustificata il trattamento effettuato dal responsabile non può più riguardare tali dati" (art. 14).

Il quadro non muta nella proposta di regolamento del Parlamento europeo e del Consiglio "concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali e la libera circolazione di tali dati (regolamento generale sulla protezione dei dati)" del 25 gennaio 2012 ove si disciplinano il diritto all'oblio e il diritto alla cancellazione dei dati, benché nei commenti la previsione concernente il diritto all'oblio sia stata molto evidenziata ed enfatizzata (art. 17).

I presupposti per richiedere la cancellazione dei dati sono che i dati non siano più necessari rispetto alle finalità per le quali sono stati raccolti o altrimenti trattati; che l'interessato revochi il consenso su cui si fonda il trattamento, di cui all'art. 6, par. 1, lett. a); oppure che il periodo di conservazione dei dati autorizzato sia scaduto e non sussista altro motivo legittimo per trattare i dati; che l'interessato si opponga al trattamento di dati personali; che il trattamento dei dati non sia conforme al regolamento per altri motivi (art. 17, par. 1).

L'innovazione è laddove si configura una nuova responsabilità del titolare del trattamento, prevedendo che quest'ultimo debba informare i terzi che stanno trattando i dati della richiesta dell'interessato di cancellare qualsiasi link, copia o riproduzione dei suoi dati personali e che, se il titolare ha autorizzato un terzo a pubblicare dati personali, è ritenuto responsabile di tale pubblicazione (art. 17, par. 2).

Volendo meglio delineare i confini di termini, quali "cancellazione dei dati" e "oblio", si può definire la cancellazione come un'operazione sui dati che esclude ogni ulteriore conservazione degli stessi, mentre l'oblio sembra piuttosto essere una finalità, che si può raggiungere con la cancellazione, ma anche con il blocco.

11. Il Parlamento in prima lettura[119] ha mantenuto l'impostazione originale secondo cui le due proposte fanno parte di un "pacchetto" di norme da gestire in modo unitario. Per tale ragione molti emendamenti alla proposta di direttiva sui trattamenti di dati personali nelle attività giudiziarie e di polizia tendono a garantire uniformità con le disposizioni della proposta di regolamento, ad esempio, rispetto alle definizioni, ai poteri delle autorità di controllo ed alla loro previa consultazione o ad alcuni meccanismi (quali la valutazione di impatto–privacy).

Per quanto riguarda gli emendamenti approvati relativi alla proposta di regolamento, il testo mantiene in larga parte l'impostazione dell'originaria proposta della Commissione, ad esempio in materia di consenso della persona interessata (che deve essere "esplicito" anziché solo "inequivocabile" come nell'attuale direttiva 95/46/CE) o in tema di diritto alla portabilità dei dati. Sono state inoltre mantenute, sia nel testo del regolamento che in quello della direttiva, alcune proposte innovative, quali: la nomina (obbligatoria) di un "data protection officer" da parte di alcune categorie di titolari di trattamento (secondo criteri però diversi rispetto a quelli indicati dalla Commissione); l'introduzione di un obbligo generale per tutti i titolari di notificare eventuali violazioni di dati personali (anche agli interessati, in determinati casi); per altro verso, l'eliminazione dell'obbligo, oggi vigente, di notificare i trattamenti all'autorità di controllo.

Gli emendamenti introducono anche versioni "semplificate" di alcune disposizioni del futuro regolamento. Ad esempio, il diritto all'oblio è stato trasformato in un diritto alla rettifica o al "congelamento" dei dati.

La posizione della LIBE è stata influenzata anche dalla necessità di fornire risposte "forti" alle attività di sorveglianza di massa legate al cd. *data-gate* a partire dal giugno 2013. Così si spiega, ad esempio, la scelta di vincolare all'autorizzazione dell'autorità di protezione dei dati competente nonché alla preventiva informativa all'interessato, l'invio di dati su richiesta di autorità giudiziarie o amministrative di Paesi terzi.

Il voto LIBE ha fornito una spinta al rafforzamento dei diritti degli interessati, nonché alla previsione di forti sanzioni per le imprese che violino i principi di protezione dei dati personali. Nel testo approvato è stato infatti modificato il sistema delle sanzioni amministrative, che tutte le autorità nazionali di controllo devono poter comminare, ma che sono libere di definire entro una soglia pecuniaria massima e nel rispetto di una griglia di criteri fissati nel testo, cui si aggiunge l'intervento chiarificatore e di indirizzo del Comitato europeo della protezione dati composto dai responsabili delle autorità di controllo dei diversi Stati membri. Ulteriori modifiche significative riguardano il cd. "sportello unico" e la

[119] La Commissione competente del Parlamento europeo (LIBE-Libertà civili, giustizia e affari interni) ha approvato gli emendamenti ai testi delle due proposte (21 ottobre 2013) e successivamente si è avuto in prima sessione il voto della Plenaria (12 marzo 2014).

collaborazione fra autorità di controllo attraverso il cd. "meccanismo di coerenza": secondo il Parlamento, lo sportello unico deve permettere alle imprese multinazionali di dialogare con un unico interlocutore nell'UE (l'autorità di controllo del Paese dove hanno lo "stabilimento principale"), ma il ruolo di questa autorità capofila (cd. *lead authority*) deve consistere nel coordinamento di un processo di co-decisione cui tutte le autorità degli Stati membri interessati da un trattamento devono partecipare.

Gli aspetti che hanno suscitato perplessità in entrambi gli strumenti così come emendati nelle proposte della LIBE riguardano invece l'introduzione della definizione di "dato pseudonimo", locuzione suscettibile di generare incertezze interpretative; le norme sulla profilazione e la definizione stessa di profilazione; l'introduzione, chiesta dal Parlamento (ma solo nel regolamento), di un "certificato europeo" della protezione dati, che costituisce una sorta di "bollino-qualità" in grado di consentire ai titolari di trattamenti di beneficiare di varie deroghe ed esenzioni e la cui vigilanza sarebbe affidata a soggetti terzi, diversi dalle autorità di controllo.

Parte II
La giurisprudenza della Corte di Strasburgo

Cap. I
Il bilanciamento con l'interesse pubblico alla sicurezza

1. I dati personali conservati dai servizi di *intelligence*: a) *Rotaru v. Romania*, b) *Haralambie v. Romania*, c) *Turek v. Slovakia*, d) *Segerstedt-Wiberg and O. v. Sweden*, e) *Shimovolos v. Russia*. – 2. La conservazione del DNA: a) *S. and Marper v. United Kingdom*, b) *Peruzzo and Martens v. Germany*. – 3. La conservazione dei dati in speciali banche dati: a) *Bouchacourt, Gardel e M.B. v. France*, b) *Khelili v. Switzerland*, c) *M.K. v. France*, d) *Dalea v. France*, e) *E.B v. Austria*, f) *Bernh Larsen v. Norway*. – 4. Controlli e videosorveglianza: a) *Peck v. the United Kingdom*, b) *Vetter v. France*, c) *Kopke v. Germany*, d) *Van Vondel v. Netherlands*.

1. a) Nella sentenza *Rotaru v. Romania*[120], la Corte ha stabilito che la raccolta, la conservazione e l'utilizzo sistematici da parte di pubbliche autorità di notizie riguardanti la vita di un individuo costituiscono un'ingerenza nel diritto al rispetto della vita privata (art. 8, par. 1 CEDU), malgrado le informazioni si riferiscano al passato di una persona. Costituiscono altresì una violazione il diniego della possibilità di accesso alle informazioni raccolte e di presentazione di domanda di cancellazione.

Per quanto riguarda il concetto di "vita privata", comprende vari tipi di informazioni personali, tra le quali gli studi conseguiti; lo svolgimento di attività politica; le condanne penali subite. Non ha rilievo la circostanza che tali informazioni si riferiscano al passato, siano a carattere riservato o di pubblico dominio. La conservazione delle notizie sulla vita privata di un individuo in un registro segreto e la relativa comunicazione rientrano pertanto nel campo di applicazione dell'art. 8, par. 1 CEDU; la medesima norma prevede altresì eccezioni al principio del rispetto della vita privata, le quali tuttavia vanno interpretate in maniera restrittiva (par. 2). Sebbene la Corte riconosca la legittimità dei servizi di *intelligence* in una società democratica, ribadisce che, ai sensi della CEDU, i poteri di sorveglianza segreta nei confronti dei cittadini sono consentiti soltanto se "previsti dalla legge" e nei limiti strettamente necessari per la salvaguardia delle istituzioni democratiche.

Tuttavia, nel caso di specie, la legislazione nazionale non stabiliva limiti precisi all'esercizio dei poteri di sorveglianza da parte delle autorità pubbliche. La detenzione e l'uso, da parte dei servizi segreti, di notizie relative alla vita privata del ricorrente non risultavano regolati da una normativa interna; pertanto non era possibile stabilire se i provvedimenti adottati dalle autorità fossero compatibili con i criteri della "conformità alla legge" e della "necessità" in una società democratica. Infatti, l'ordinamento interno non definiva con chiarezza la portata e le modalità di esercizio del potere discrezionale riconosciuto alle autorità pubbliche nell'attuazione di misure di sorveglianza segreta. In ogni caso, la discrezionalità in parola deve avere dei limiti e non può costituire un potere assoluto, altrimenti risulta incompatibile con lo stato di diritto.

Per quanto riguarda il criterio della "conformità alla legge", la Corte ribadisce la sua precedente giurisprudenza, secondo cui tale concetto giuridico richiede non solo che il provvedimento impugnato debba essere fondato su una normativa nazionale con determinate caratteristiche, bensì deve risultare accessibile alla persona interessata e prevedibile per quanto riguarda i suoi effetti.

Per quanto riguarda il riconoscimento di misure di tutela adeguate ed efficaci

[120] *Rotaru v. Romania* [GC], no. 28341/95, ECHR 2000-V.

contro possibili abusi, la Corte deve procedere ad una valutazione comparativa degli interessi coinvolti, poiché un sistema di sorveglianza segreta finalizzato a proteggere la sicurezza nazionale comporta il rischio di indebolire o anche distruggere la medesima democrazia, con il pretesto di rafforzarla.

Le procedure di controllo devono rispettare i valori di una società democratica, in particolare lo stato di diritto, espressamente citato nel preambolo della CEDU. Lo stato di diritto implica, *inter alia*, che l'ingerenza da parte del potere esecutivo nei diritti dell'individuo sia soggetta ad un controllo efficace. Tale controllo di norma deve essere garantito, almeno in ultima istanza, dal potere giudiziario, in quanto il controllo giurisdizionale garantisce indipendenza ed imparzialità.

Per quanto riguarda il secondo motivo di impugnazione, vale a dire la presunta violazione del diritto ad un ricorso effettivo (art. 13), com'è noto, la CEDU garantisce l'esperibilità di una procedura di impugnazione a livello nazionale in caso di violazione dei diritti e delle libertà in essa previsti. Tale norma richiede la disponibilità di un ricorso interno che consenta "all'autorità nazionale competente" di decidere in merito alla presunta violazione dei diritti convenzionali. Malgrado gli Stati contraenti godano di un certo margine discrezionale nel dare attuazione alla norma in parola, il rimedio giurisdizionale deve rispettare il requisito dell'efficacia[121]. La previsione di un ricorso nell'ordinamento interno può riguardare solo i motivi di ricorso attivabili sulla base della Convenzione[122]. Pertanto, nel caso di specie, la Corte accoglie anche il secondo motivo di impugnazione, visto che a livello nazionale non era previsto alcuno strumento di ricorso per la modifica o la distruzione dei file di interesse per il ricorrente.

Nelle sue conclusioni concordanti, il giudice Wildhaber sostiene che la Corte avrebbe dovuto sottolineare che la misura controversa nel caso di specie non persegue uno scopo legittimo (ex art. 8, par. 2). Pertanto, pur in presenza di una base giuridica prevedibile, era riscontrabile una violazione della CEDU, sia perché non vi era alcuna finalità legittima per continuare a detenere un sistema abusivo di file segreti, sia perché ciò non risultava necessario in una società democratica. L'esistenza di una finalità legittima di sicurezza nazionale deve essere accompagnata dall'affermazione che gli Stati non godono di potere assoluto nei confronti delle persone sottoposte alla sorveglianza segreta. Tale ingerenza non risulta necessaria in una società democratica allo scopo di garantire la sicurezza nazionale.

Nella sua Opinione parzialmente dissenziente, il giudice Bonello sottolinea che le notizie "false" sul ricorrente, conservate dai servizi segreti romeni, avrebbero potuto compromettere in modo grave la sua reputazione. Pertanto la Corte avrebbe dovuto considerare tale questione in maniera esplicita e non incidentalmente, come se fosse

[121] *Wille v. Liechtenstein* [GC], no. 28396/95, § 75, ECHR 1999-VII.
[122] V. ad esempio, *Çakıcı v. Turkey* [GC], no. 23657/94, § 112, ECHR 1999-IV.

un aspetto marginale del diritto alla privacy. Infatti, come vedremo, quest'ultimo aspetto costituirà oggetto di interessanti sviluppi della sua giurisprudenza negli anni successivi. Infatti la giurisprudenza più recente sembra orientarsi verso la tesi che anche il concetto di "reputazione" rientri nel suo ambito di applicazione (art. 8, par. 1).

1. b) Nello stesso filone giurisprudenziale si inserisce la sentenza *Haralambie v. Romania*[123]*, in cui* la Corte ha accertato la violazione del diritto al rispetto della vita privata per la difficoltà da parte del ricorrente di accesso ad un dossier che lo riguardava e che era stato redatto dai servizi segreti durante il regime comunista. Secondo la Corte, la quantità di fascicoli da trasferire e le carenze del sistema di archiviazione non possono giustificare un ritardo di molti anni per il soddisfacimento della richiesta del ricorrente. Le autorità nazionali avrebbero dovuto predisporre una "procedura effettiva ed accessibile" tale da consentire agli interessati l'accesso al "complesso delle informazioni" che li riguardavano.

La Corte afferma che lo Stato contraente non ha soddisfatto l'obbligo positivo di stabilire per il ricorrente una procedura efficace per consultare in un termine ragionevole il suo fascicolo personale. Al riguardo, ricorda che agli obblighi negativi a tutela dell'individuo contro le ingerenze arbitrarie del pubblico potere possono aggiungersi altresì obblighi positivi. Il confine tra obblighi positivi e negativi ai sensi dell'art. 8 non si presta ad una definizione precisa, ma i principi applicabili sono comparabili[124].

1. c) Nella sentenza *Turek v. Slovakia*[125], la Corte riconosce, specie nell'ambito di procedimenti relativi ad operazioni condotte dalle agenzie di sicurezza statali, l'illegittimità di normative nazionali che pongano limiti di accesso a documenti e materiali riservati.

Dinanzi alla Corte, il ricorrente aveva sostenuto che l'esistenza di un file dell'ex agenzia di sicurezza comunista cecoslovacca nel quale egli era stato registrato come un agente (insieme al rilascio di un nulla osta negativo e al rigetto del suo ricorso contro tale iscrizione) costituiva una grave violazione del suo diritto al rispetto della vita privata[126]. Secondo la sua tesi, il pregiudizio al buon nome e alla reputazione

[123] *Haralambie v. Romania*, no. 21737/03, 27 October 2009.

[124] A tal proposito si veda la sentenza *Odièvre v. France* [GC], no. 42326/98, § 40, ECHR 2003-III: "The boundaries between the State's positive and negative obligations under Article 8 do not lend themselves to precise definition. The applicable principles are nonetheless similar. In particular, in both instances regard must be had to the fair balance which has to be struck between the competing interests; and in both contexts the State enjoys a certain margin of appreciation".

[125] *Turek v. Slovakia*, no. 57986/00, ECHR 2006-II (extracts).

[126] Il ricorrente aveva ricoperto un incarico pubblico di alto livello nel settore dell'istruzione scolastica. In risposta ad una richiesta formulata dal datore di lavoro ai sensi del "Lustration Act"(una legge del 1991 che ha definito i requisiti per lo svolgimento di alcune attività nel settore pubblico), il

individuale derivava proprio dalla infondatezza della sua registrazione nei file dell'agenzia di sicurezza statale. Era quindi fondamentale riuscire a dimostrare che la registrazione in parola fosse avvenuta in modo illegittimo all'epoca dei fatti. E' particolarmente interessante che la Corte puntualizzi i confini logico–giuridici fra analisi di merito e controllo sovranazionale. Non rientra nei suoi compiti agire come una Corte di appello ed esaminare gli errori di fatto o di diritto commessi da un giudice nazionale, se non nella misura dell'accertamento di eventuali violazioni dei diritti convenzionali[127]. Infatti, spetta ai giudici nazionali valutare gli elementi di prova nonché la loro rilevanza; mentre compito della Corte è soltanto accertare se il procedimento, ivi compresa l'analisi delle prove, sia stato svolto correttamente ai sensi dell'art. 8.

La Corte ha pertanto esaminato se la procedura nazionale di cui ha beneficiato il ricorrente fosse stata efficace. In particolare, riconosce che, nei procedimenti relativi alle operazioni delle agenzie di sicurezza statali, possono esserci legittimi motivi per limitare l'accesso a documenti riservati. Nel procedimento interno, al ricorrente era stato negato un pieno accesso ai documenti che lo riguardavano per contestarne la veridicità; al contrario, allo Stato contraente, mediante i suoi servizi segreti, era stata riconosciuta tale possibilità. Ciò in violazione del principio di uguaglianza processuale.

La conclusione è che i procedimenti giurisdizionali di cui ha usufruito il ricorrente non hanno assicurato una protezione efficace del diritto al rispetto della vita privata. La condotta dello Stato contraente costituisce un'interferenza illegittima per la mancata previsione di una procedura di accesso ai documenti da parte del ricorrente in un contesto così specifico come quello del *Lustration Act*[128]. Infatti, a seguito della caduta dei regimi comunisti nell'Est europeo, i procedimenti di *lustration*[129] sono orientati alla ricostruzione di fatti risalenti al periodo comunista e

---

Ministero degli Interni aveva emesso nei suoi confronti un certificato negativo. Il certificato affermava che egli era stato registrato dall'ex Agenzia di sicurezza statale ("STB") come collaboratore e che pertanto era interdetto da alcuni ruoli pubblici. Il ricorrente riconosceva di aver involontariamente incontrato gli agenti del "STB"prima e dopo i viaggi che aveva fatto all'estero, durante gli anni delle dittatura comunista, ma non aveva mai rivelato informazioni riservate e che pertanto non era una spia. Il ricorrente aveva avviato un'azione civile per la tutela della sua reputazione, per ottenere una sentenza che dichiarasse che la sua registrazione come collaboratore del "STB" risultasse illegittima. A seguito di una richiesta di accesso da parte di un tribunale regionale, il servizio di intelligence slovacco ("SIS"), in possesso degli archivi segreti, aveva rifiutato di consegnare i documenti dell'ex "STB" che riguardavano il ricorrente, sostenendo che fossero coperti da segretezza sulla base di una normativa che ne tutelava la riservatezza. I ricorsi avanzati dal ricorrente negli anni successivi erano stati respinti, anche dalla Corte costituzionale.

[127] *Turek v. Slovakia*, cit., par. 114.

[128] *Ivi*, par. 116: "The applicant's proceedings therefore cannot be considered as offering him effective protection of his right to respect for his private life. The Court arrives at this conclusion without embarking on an examination of the assessment of evidence in this case, which, in its view, is also open to criticism".

[129] La definizione del procedimento in parola è la seguente: "Lustration is the government process regulating the participation of former communists, especially informants of the communist secret

non sono direttamente collegati alle funzioni e alle operazioni dei servizi di sicurezza. Pertanto, a meno che non venga fornita prova contraria in ciascun caso specifico, non vi può essere un interesse pubblico a restrizioni nell'accesso di materiali considerati riservati nel corso di regimi politici precedenti. Tali procedimenti di *lustration* dipendono in maniera inevitabile dall'esame dei documenti relativi alle operazioni delle ex agenzie di sicurezza comuniste. Sulla base della normativa interna, è l'agenzia di sicurezza che ha il potere di decidere quali documenti debbano rimanere riservati e per quanto tempo. Tuttavia, l'esistenza di questo potere discrezionale non rispetta il principio di equità del procedimento, compreso il principio della parità dei mezzi. Lo Stato che adotta tali misure deve assicurare che agli interessati vengano riconosciute tutte le garanzie procedurali previste dalla CEDU, in relazione a qualsiasi controversia.

Pertanto, la Corte ha riconosciuto la mancanza di una procedura nazioanle con la quale richiedere una protezione efficace del diritto al rispetto della vita privata. Infatti, a causa della sua qualificazione come "agente", al ricorrente era stato rilasciato un certificato che aveva avuto un notevole impatto sulla sua reputazione e pertanto sulla sua vita privata (art. 8 CEDU)[130].

1. d) Nel caso *Segerstedt–Wiberg*[131], i ricorrenti avevano richiesto senza successo alla polizia di sicurezza svedese di visualizzare integralmente i dati che li riguardavano. Secondo la polizia, la diffusione di tali dati avrebbe potuto compromettere la prevenzione della criminalità e la sicurezza nazionale[132].

La Corte ammette che la raccolta delle informazioni perseguiva obiettivi legittimi, quali nel caso della prima ricorrente la prevenzione dei reati e per gli altri la tutela della sicurezza nazionale. Se l'esistenza dei servizi di intelligence appare legittima in una società democratica, i poteri di sorveglianza segreta sono tollerabili solo nella misura strettamente necessaria alla salvaguardia delle istituzioni democratiche. Tali interferenze devono essere supportate da motivi pertinenti e sufficienti e devono essere proporzionate allo scopo legittimo e agli obiettivi

---

police, in the successor political appointee positions or in civil service positions in the period after the fall of the various European Communist states in 1989 – 1991. It also applies more broadly to the process of nations dealing with past human rights abuses or injustices that have occurred".

[130] *Turek v. Slovakia*, cit., par. 116.

[131] *Segerstedt-Wiberg and Others v. Sweden*, no. 62332/00, ECHR 2006-VII.

[132] La Corte ha ritenuto che la registrazione delle informazioni trovasse un fondamento giuridico nella legge svedese sui dati di polizia del 1998. In particolare, tale normativa riconosceva il diritto della polizia alla registrazione di informazioni personali in caso di sospetto reato contro la sicurezza nazionale o di terrorismo, o in caso di persona sottoposta ad un controllo di sicurezza o per altri motivi particolari (art. 33). La polizia godeva di un potere discrezionale nell'applicazione di tali misure, tuttavia non illimitato. Infatti, la normativa in materia pone un divieto generale di registrazione in un registro pubblico sulla base dell'opinione politica (art. 5) e la Costituzione svedese ha escluso che siffatta registrazione, basata sulla sola opinione politica, possa avere luogo in mancanza del consenso della persona interessata.

perseguiti. A questo proposito, la Corte ricorda che le autorità nazionali godono di un margine di apprezzamento, la cui portata dipende non solo dalla natura dello scopo legittimo perseguito, ma anche dalla particolare natura dell'ingerenza in parola.

Nel caso di specie, l'interesse dello Stato convenuto di tutela della sicurezza nazionale e della lotta contro il terrorismo doveva essere bilanciato con la gravità del pregiudizio arrecato al diritto dei ricorrenti al rispetto della vita privata. La portata del potere discrezionale conferito alle autorità statali e le modalità del suo esercizio erano stati indicati con sufficiente chiarezza, così da offrire all'individuo una protezione adeguata contro ingerenze arbitrarie. Pertanto, l'interferenza con la vita privata dei ricorrenti risultava conforme alla legge (ex art. 8). La Corte ha anche riconosciuto che la memorizzazione delle informazioni in questione perseguiva obiettivi legittimi, vale a dire la prevenzione dei reati e la tutela della sicurezza nazionale.

Malgrado la Corte abbia riconosciuto la legittimità di un sistema di servizi segreti in una società democratica, ha sottolineato che la sorveglianza segreta dei cittadini risulta compatibile con la CEDU nella misura strettamente necessaria alla salvaguardia delle istituzioni democratiche. Tale interferenza deve essere supportata da motivi pertinenti e sufficienti ed essere proporzionata allo scopo legittimo o agli obiettivi perseguiti

La Corte riconosce che la conservazione delle informazioni relative alla ricorrente risultavano pertinenti e sufficienti rispetto all'obiettivo di prevenzione dei reati. Infatti la misura era stata adottata proprio allo scopo di proteggerla. Pertanto non costituiva un'interferenza sproporzionata con il suo diritto al rispetto della vita privata.

Considerazioni di diverso tenore venivano svolte sulle informazioni relative ad altri due ricorrenti[133]. La Corte non ha ritenuto che la conservazione delle informazioni si basasse su ragioni pertinenti e sufficienti di salvaguardia della sicurezza nazionale. La conservazione dei dati, anche se rilevante, non poteva essere comunque considerata proporzionata se protratta per più di trent'anni anni. Pertanto, la Corte rilevava un'interferenza sproporzionata con il loro diritto al rispetto della vita privata.

Per quanto riguarda il terzo e il quarto ricorrente sull'appartenenza ad un partito politico che avrebbe fatto uso di violenza per sovvertire l'ordine sociale, la Corte ha ritenuto che il programma di un partito politico non potesse essere considerato come unico criterio per la determinazione della violenza, bensì che dovessero essere valutate anche le azioni dei relativi leader.

[133] In un caso l'iscrizione nel pubblico registro era stata decisa a seguito della partecipazione del ricorrente ad una riunione politica; nell'altro caso, a seguito della resistenza violenta da parte del ricorrente nei confronti della polizia durante una manifestazione.

In ogni caso, la Corte ha ribadito la legittimità del rifiuto di accesso ad un registro nazionale di polizia segreta quando lo Stato poteva legittimamente temere che le informazioni ivi contenute compromettesse l'efficacia di un sistema di sorveglianza per la sicurezza nazionale e per lotta al terrorismo. In questo senso, la Corte ritiene di non poter contraddire la valutazione delle autorità amministrative e giudiziarie nazionali.

Per quanto riguarda il diritto dei ricorrenti ad un ricorso effettivo (art. 13 CEDU), la Corte osserva che, nel sistema interno, alcuni organi istituzionali (mediatore parlamentare e cancelliere di giustizia) risultavano competenti alla ricezione di denunce individuali e allo svolgimento delle relative indagini. I pareri espressi da tali figure godono di grande considerazione nella società svedese e di norma sono rispettati malgrado non abbiano carattere vincolante. La competenza degli organi in parola riguardava peraltro una supervisione dell'intero procedimento.

Tuttavia, la Corte afferma l'assenza all'epoca dei fatti di un sistema di impugnazione efficace nel diritto interno (ex art. 13). Riconosce che, nel frattempo, erano stati introdotti alcuni miglioramenti normativi, i quali tuttavia non rispettavano il requisito dell'"efficacia", in mancanza della possibilità per i ricorrenti di chiedere un risarcimento.

Per tali ragioni, la Corte ha riconosciuto all'unanimità i motivi di ricorso avanzati dai ricorrenti[134].

1. e) La sentenza *Shimovolos v. Russia*[135] riguarda la registrazione del ricorrente come attivista a sostegno dei diritti umani in un c.d "database di sorveglianza". Infatti, nel corso di un summit Russia–Unione europea, le autorità russe, informate circa l'organizzazione di proteste, decisero l'arresto di tutti gli organizzatori al fine di prevenire atti illeciti ed estremisti. In particolare, le autorità avevano ricevuto informazioni sull'arrivo del ricorrente presso la località del summit ed avevano proceduto al suo arresto preventivo[136].

Visto l'uso della coercizione e malgrado la breve durata dell'arresto, la Corte ha ritenuto che il ricorrente fosse stato "privato della libertà"in modo illegittimo. Infatti il ricorrente, senza aver commesso alcun reato, era stato arrestato per evitare che

[134] In particolare, per quattro ricorrenti su cinque la Corte ha riconosciuto la violazione dell'art. 8 (diritto al rispetto della vita privata e familiare); dell'art. 10 (libertà di espressione); dell'art. 11 (libertà di riunione e di associazione). Per quanto riguarda tutti i cinque ricorrenti, la Corte ha riconosciuto altresì la violazione dell'art. 13 (diritto ad un ricorso effettivo).

[135] *Shimovolos v. Russia*, no. 30194/09, 21 June 2011.

[136] Il ricorrente era stato fermato dalla polizia e condotto con la forza alla stazione di polizia. Alla stazione di polizia gli agenti hanno redatto un rapporto di partecipazione utilizzando un modello prestampato dal titolo "Relazione (di partecipazione) nei confronti di una persona che ha commesso un illecito amministrativo". Tuttavia, essi avevano provveduto a cancellare la frase "che ha commesso un illecito amministrativo". Il richiedente fu rilasciato dopo circa 45 minuti. L'ufficiale di polizia che lo aveva scortato dichiarò in seguito di aver agito così per impedire che il ricorrente commettesse altri illeciti amministrativi e penali.

commettesse eventuali reati di natura estremista. Secondo la Corte, le autorità non erano state in grado di menzionare tali potenziali reati specifici e il vago riferimento a "reati di natura estremista" non era sufficiente a soddisfare i requisiti ex art. 5 CEDU.

L'unico sospetto concreto nei confronti del ricorrente era che potesse divulgare concetti di propaganda estremista, malgrado non avesse con sé alcun bagaglio al suo arrivo. In realtà, l'arresto era stato eseguito soltanto sulla base dell'inserimento del suo nome nel "database di sorveglianza". La registrazione in parola era avvenuta per la sua appartenenza ad un'organizzazione in difesa dei diritti umani. La Corte ha sottolineato che essere un attivista dei diritti umani non può in alcun caso costituire ragione sufficiente per eseguire un arresto. In conclusione, l'arresto del ricorrente non poteva ragionevolmente essere considerato come necessario per impedire la commissione di un reato (ai sensi dell'art. 5 par. 1, lett. c) CEDU).

La Corte all'unanimità ha riconosciuto altresì la violazione del diritto al rispetto della vita privata del ricorrente. Il suo nome era stato inserito in un registro, che raccoglieva informazioni sui suoi movimenti in treno o in aereo sul territorio nazionale con grave ingerenza nella sua vita privata. La creazione e la gestione del database e la procedura per il suo funzionamento erano stati disciplinati da un decreto ministeriale mai pubblicato o reso accessibile. A tale riguardo, la Corte ha rilevato che il diritto interno non indicasse con sufficiente chiarezza la portata e le modalità di esercizio del potere discrezionale delle autorità nazionali nella raccolta e memorizzazione nel database delle informazioni relative alla vita privata degli individui. In particolare, non indicava in una forma accessibile al pubblico alcun tipo di garanzia minima contro gli abusi.

La Corte ha già rilevato che la raccolta sistematica e la memorizzazione di dati da parte dei servizi di sicurezza costituisce un'ingerenza nella vita privata, malgrado i dati fossero stati raccolti in un luogo pubblico o riguardassero esclusivamente le attività professionali e pubbliche delle persone interessate.

Secondo la Corte, l'espressione "prevista dalla legge"(art. 8 par. 2) richiede non solo che l'ingerenza della vita privata trovi un fondamento giuridico nel diritto interno, ma che abbia altresì determinate caratteristiche, vale a dire che sia impugnabile da parte degli interessati e che siano prevedibili le sue conseguenze. A tale riguardo, la Corte sottolinea che una persona non dovrebbe essere in grado di prevedere l'applicazione nei suoi confronti di attività di sorveglianza in quanto ciò potrebbe vanificare il loro effetto. Tuttavia, specie se il potere esecutivo viene esercitato in segreto, restano alti i rischi di arbitrarietà. Pertanto, visto che la tecnologia è sempre più sofisticata, è indispensabile che le norme in materia di sorveglianza segreta siano chiare così come le loro modalità di applicazione. In questo modo il ricorso a tali misure di sorveglianza segreta e la relativa raccolta dati avrebbero luogo in modo più trasparente.

Inoltre, visto che il rischio di abusi è connaturato a qualsiasi sistema di sorveglianza segreta, specie in mancanza di un controllo pubblico, ogni ordinamento dovrebbe prevedere alcune garanzie minime per evitare tali distorsioni, con l'indicazione della natura, dello scopo e della durata delle misure, la motivazione per l'adozione delle stesse, le autorità competenti alla relativa esecuzione e al controllo, nonché il tipo di ricorso previsto dal diritto interno.

Nel caso di specie, secondo la Corte, la creazione e il mantenimento del c.d. "database di sorveglianza" e la procedura per il suo funzionamento erano disciplinati da un ordine ministeriale. L'ordine di sorveglianza non risultava pubblicato e non era accessibile al pubblico. Pertanto restavano ignoti i motivi della registrazione di un nome nella banca dati; le autorità competenti all'ordine di registrazione; la durata della misura; l'esatta natura dei dati raccolti; le modalità di conservazione e l'utilizzo dei dati raccolti; i controlli esistenti e le garanzie contro gli abusi.

Per questi motivi, la Corte ha condannato lo Stato convenuto sul presupposto che il diritto interno non indicasse con sufficiente chiarezza la portata e le modalità di esercizio del potere discrezionale conferito alle autorità nazionali nella raccolta e conservazione delle informazioni sulla vita privata delle persone nel database. Pertanto, l'ingerenza con i diritti del ricorrente non risultava conforme alla CEDU, né ai requisiti previsti in materia dalla giurisprudenza della Corte di giustizia.

LA CONSERVAZIONE DEL DNA

2. Negli ultimi anni, i registri del DNA hanno indubbiamente fornito un fondamentale contributo alle autorità giudiziarie per la lotta alla criminalità; tuttavia, la protezione dei dati personali riveste un'importanza fondamentale per il godimento del diritto al rispetto della vita privata (art. 8, par. 1 CEDU).

Secondo la Corte, la lotta contro la criminalità, specie contro il crimine organizzato ed il terrorismo, costituisce una delle sfide più importanti cui devono far fronte le società moderne. Il successo di tale lotta dipende in larga misura dall'uso delle più moderne tecniche scientifiche di indagine e di identificazione. Il Consiglio d'Europa ha riconosciuto oramai da più di quindici anni che le tecniche di analisi del DNA presentano enormi vantaggi per il sistema giudiziario. Gli Stati membri hanno rapidamente realizzato notevoli progressi in materia di utilizzo dei dati del DNA ai fini dell'accertamento dell'innocenza o della colpevolezza degli imputati di reati penali.

Se da un lato la Corte non può non riconoscere l'importanza del ruolo giocato da tali nuove tecnologie nell'individuazione dei reati, dall'altro essa ha l'obbligo di delimitare la portata del loro utilizzo.

La conservazione delle informazioni riguardanti le impronte digitali e i dati

genetici persegue lo scopo legittimo di individuare e prevenire la commissione di reati. Il prelievo iniziale delle informazioni in parola collega una determinata persona ad un particolare reato del quale è sospettata e la successiva conservazione serve ad identificare eventuali futuri autori di reati. Pertanto, la conservazione dei campioni di cellule e dei loro profili di DNA costituisce un'interferenza nel diritto dei ricorrenti al rispetto della loro vita privata ai sensi della CEDU.

Tuttavia alle autorità nazionali competenti deve essere riconosciuto un certo margine di apprezzamento. L'ampiezza di siffatto margine può dipendere dalla natura dei diritti convenzionali oggetto della controversia, dalla loro importanza per gli individui, dalla natura dell'ingerenza nonché dagli obiettivi perseguiti con l'ingerenza. Il margine si riduce necessariamente quando il diritto in questione è indispensabile per il godimento effettivo di diritti fondamentali e intimi riconosciuti all'individuo. Pertanto nel caso in cui la posta in gioco riguardi un aspetto particolarmente importante dell'esistenza o dell'identità di un individuo, il margine di apprezzamento riconosciuto allo Stato contraente sarà necessariamente ridotto.

2. a) Nella sentenza *S. and Marper v. United Kingdom*[137], la Corte ha stabilito che, a seguito di un'assoluzione in un procedimento penale, il rifiuto dell'autorità statale di cancellazione dei dati personali del ricorrente relativi a impronte digitali, profili di DNA e campioni di cellule costituisse un'illegittima interferenza nella sua vita privata. Si tratta infatti di dati personali (sulla base della relativa Convenzione europea sulla protezione dei dati personali), visto che riguardano persone identificate o identificabili.

L'ampliamento del ricorso alla banche dati del DNA deve rispettare i limiti del bilanciamento con l'interesse concorrente della protezione della vita privata. Lo sviluppo di nuove tecnologie implica infatti una speciale responsabilità degli Stati contraenti di individuare il corretto bilanciamento degli interessi. La legislazione interna deve prevedere misure idonee ad impedire qualsiasi uso non conforme alla protezione dei diritti garantita dall'art. 8 CEDU. In particolare, la Corte ritiene che la conservazione dei dati personali può essere particolarmente pregiudizievole nel caso di minori, con riguardo sia alla loro peculiare situazione, sia all'importanza del loro sviluppo e della loro integrazione nella società. In conclusione, la Corte conclude che il carattere generale ed indifferenziato con cui opera il meccanismo di conservazione delle impronte digitali, dei campioni di cellule e dei profili di DNA di individui sospettati della commissione di determinati reati, che però non sono poi condannati, non garantisce un corretto bilanciamento dei concorrenti interessi pubblici e privati in gioco. Pertanto, nel caso di specie, lo Stato convenuto ha oltrepassato il margine di apprezzamento accettabile in proposito e la fattispecie in esame costituisce un'ingerenza sproporzionata nel diritto dei ricorrenti al rispetto

[137] *S. and Marper v. the United Kingdom* [GC], nos. 30562/04 and 30566/04, ECHR 2008.

della vita privata, che non può essere considerata come necessaria in una società democratica.

La Corte sottolinea in primo luogo che tutte e tre le categorie di dati personali del ricorrente conservati dalle autorità (vale a dire impronte digitali, profili di DNA e campioni di cellule) riguardano persone identificate o identificabili. Pertanto, ai sensi della relativa Convenzione europea sulla protezione, costituiscono dati personali.

Già in precedenza, la Corte aveva dovuto esaminare questioni attinenti alla conservazione di dati personali da parte delle autorità nel contesto di procedure penali. Per quanto riguarda la natura e la portata delle informazioni contenute in ciascuna delle tre categorie di dati, la Corte in passato ha provveduto ad operare una distinzione tra la conservazione delle impronte digitali da una parte e la conservazione dei campioni di cellule e dei profili di DNA dall'altra, viste le maggiori possibilità di uso delle informazioni presenti in queste ultime due categorie. Pertanto, la Corte ritiene che, anche nel caso di specie, essa debba procedere esaminando separatamente la questione dell'ingerenza nel diritto alla vita privata dei ricorrenti che deriva dalla conservazione dei campioni biologici e dei profili del DNA da un lato e quella derivante dalla conservazione delle loro impronte digitali dall'altro[138].

La questione non è quella di determinare se la conservazione di impronte digitali di campioni di cellule e di profili di DNA sia in generale legittima ai sensi della Convenzione. L'unica questione su cui la Corte si sofferma è quella di stabilire se la conservazione delle impronte digitali e dei dati del DNA dei ricorrenti, in quanto persone sospettate, ma non condannate, di certi reati, è da considerarsi legittima (ex art. 8, par. 2 CEDU)[139].

Malgrado i vantaggi di un maggiore utilizzo delle banche dati del DNA, alcuni Stati contraenti hanno introdotto limiti alla conservazione e all'utilizzo dei dati in parola in bilanciamento con l'opposto interesse alla protezione della vita privata. La Corte fa notare che la protezione riconosciuta dalla CEDU sarebbe indebolita in modo inaccettabile se si consentisse nel settore della giustizia penale l'utilizzo ad ogni costo di moderne tecniche scientifiche, senza operare un attento bilanciamento tra i vantaggi che possono derivare da un ricorso generalizzato a tali tecniche e i fondamentali interessi che sono collegati al rispetto della vita privata.

Secondo il punto di vista della Corte, il forte consenso in materia presente negli Stati contraenti ha ridotto inevitabilmente il margine di apprezzamento dello Stato convenuto nella determinazione dei limiti alle ingerenze nella vita privata dei sospettati di reati. La Corte ritiene che qualsiasi Stato che pretenda di svolgere un ruolo pionieristico nello sviluppo di nuove tecnologie debba accollarsi anche la

[138] *Ivi*, par. 69.
[139] *Ivi*, par. 106.

speciale responsabilità di individuare il corretto bilanciamento da applicare nel settore[140].

La Corte ritiene che l'allargamento della banca dati abbia contribuito all'individuazione e alla prevenzione delle infrazioni penali; tuttavia, non ritiene che l'identificazione e la punizione degli autori dei reati non sarebbe stata possibile senza la conservazione permanente ed indiscriminata delle impronte digitali e dei dati del DNA[141]. Resta, pertanto, da determinare se una tale conservazione sia proporzionata e rifletta il giusto bilanciamento tra interessi pubblici ed interessi individuali contrapposti[142].

Il livello di intensità dell'ingerenza nel diritto dei ricorrenti al rispetto della loro vita privata può variare a seconda di ciascuna delle tre categorie di dati personali oggetto della conservazione. Ad esempio, la conservazione di campioni di cellule costituisce un'ingerenza particolarmente invasiva, visto che contengono una grande quantità di informazioni genetiche, relative anche alla salute della persona interessata. Tuttavia, un regime di conservazione indifferenziato ed incondizionato come quello oggetto del ricorso, ha imposto un esame da parte della Corte senza distinzioni tra le tre categorie di dati[143].

La Corte ritiene, inoltre, che la conservazione dei dati personali riguardanti persone che non sono state condannate può essere particolarmente pregiudizievole nel caso di minori (come nel caso del primo ricorrente), in considerazione della loro peculiare situazione e dell'importanza del loro sviluppo e della loro integrazione nella società. A tale riguardo, ispirandosi alle disposizioni della Convenzione delle Nazioni Unite sui diritti del fanciullo del 1989 (art. 40), ha evidenziato la posizione di particolare fragilità dei minori nel sistema giudiziario penale e la particolare necessità di salvaguardare la loro vita privata nel corso delle procedure penali. I minori devono essere protetti dal pregiudizio derivante dalla conservazione dei dati personali specie in caso di assoluzione[144].

In conclusione, il carattere generale ed indifferenziato con cui opera il meccanismo di conservazione dei dati personali di individui sospettati ma non condannati per determinati reati non garantisce un corretto bilanciamento degli interessi (pubblici e privati) in gioco. Secondo la Corte, nel caso di specie, lo Stato convenuto ha oltrepassato un margine di apprezzamento accettabile. Ne segue che la conservazione dei dati personali costituisce un'ingerenza sproporzionata nel diritto dei ricorrenti al rispetto della vita privata, che non può in alcun modo essere considerata come necessaria in una società democratica. Siffatta conclusione elimina la necessità di esaminare l'adeguatezza di alcuni specifici aspetti, quale ad esempio

[140] *Ivi*, par. 112.
[141] *Ivi*, par. 117.
[142] *Ivi*, par. 118.
[143] *Ivi*, par. 120.
[144] *Ivi*, par. 124.

l'accesso ai dati o le insufficienti misure di garanzia contro l'utilizzo improprio o abusivo dei dati[145].

2. b) La decisione di irricevibilità del ricorso *Peruzzo and Martens v. Germany*[146] per manifesta infondatezza riguardava la raccolta e conservazione dei profili di DNA di criminali a fini di utilizzo in eventuali futuri procedimenti penali.

Nel caso di specie, il giudice nazionale aveva ordinato il prelievo di materiale cellulare dal primo ricorrente per stabilire il suo profilo del DNA ai fini della sua identificazione in futuri procedimenti penali. Tale decisione era stata raggiunta vista la gravità dei reati commessi (legati alla droga) e della prognosi criminale negativa[147]. Riguardo al secondo ricorrente, il giudice aveva ordinato il prelievo di campioni del DNA a causa della reiterazione dei reati violenti commessi[148].

La decisione in oggetto presenta profili giuridici diversi da quelli della sentenza *S. and Marper v. United Kingdom*, in cui la Corte aveva giudicato in senso negativo la conservazione illimitata indipendentemente dalla natura o gravità del reato o delle circostanze personali dell'individuo interessato.

Al contrario, nella fattispecie in oggetto, in caso di persone condannate per reati gravi e probabilmente soggette a procedimenti penali futuri, i profili di DNA avrebbero potuti essere prelevati e conservati. I giudici nazionali avevano basato le loro decisioni sulla circostanza che i reati commessi dai ricorrenti avessero raggiunto una particolare soglia di gravità. Pertanto, il prelievo dei campioni di DNA e la conservazione dei profili estratti risultavano giustificati e proporzionati.

Secondo la Corte, il diritto interno prevedeva idonee tutele a favore del diritto al rispetto della vita privata, nonché garanzie sufficienti circa l'effettiva protezione da usi abusivi dei dati personali conservati. La normativa nazionale garantiva il giusto equilibrio tra i confliggenti interessi pubblici e privati e rientrava nel margine di apprezzamento discrezionale lasciato allo Stato convenuto. Pertanto, la Corte ha dichiarato irricevibile il ricorso in quanto manifestamente infondato.

---

[145] *Ivi*, par. 125.

[146] *Peruzzo and Martens v. Germany*, appl. nos. 7841/08 e 57900/12, decision 4 June 2013.

[147] Il ricorrente era stato condannato per reati di droga.

[148] Secondo il diritto interno, il materiale cellulare ottenuto avrebbe dovuto essere utilizzato unicamente al fine di stabilire il profilo del DNA. L'identità dell'individuo da cui il campione era stato prelevato non poteva essere rivelata agli esperti incaricati di redigere il profilo; quest'ultimi inoltre avevano l'obbligo di adottare misure idonee a prevenire l'uso non autorizzato dei materiali esaminati. Successivamente, lo stesso materiale cellulare avrebbe dovuto essere immediatamente distrutto una volta che questo non fosse più necessario per stabilire il profilo del DNA. Solamente i profili del DNA estratti dal materiale cellulare potevano essere conservati nella banca dati dell'Ufficio di Polizia Criminale Federale e solamente per un massimo di dieci anni, sottoposti a regolare revisione.

3. a) Ai fini dell'iscrizione degli autori di crimini sessuali in un dossier giudiziario nazionale, nelle tre sentenze gemelle *Bouchacourt v. France*[149], *Gardel v. France*[150] e *M.B. v. France*[151], la Corte ha riaffermato la deroga della protezione dei dati personali per motivi di sicurezza. A seguito di una condanna per violenza sessuale a danno di un minorenne, i nominativi dei ricorrenti erano stati inseriti in un data–base di autori di reati sessuali. Secondo i ricorrenti, tale inclusione avrebbe violato il principio di non retroattività delle sanzioni penali (art. 7 CEDU) e il diritto al rispetto della vita privata (art. 8 CEDU).

Nell'analisi del caso, la Corte afferma che l'obbligo per i condannati per un reato sessuale di comunicare alla polizia il loro nome, la data di nascita, l'indirizzo e il relativo cambiamento rientra nell'ambito di applicazione della Convenzione. Infatti, il trattamento automatizzato dei dati personali, soprattutto per scopi di polizia, richiede adeguate garanzie. I dati devono essere pertinenti al fine per il quale vengono memorizzati e conservati in modo tale da permettere l'identificazione dell'interessato per un periodo necessario agli scopi della registrazione. Nel caso di specie, la creazione del data–base ha la funzione di evitare la recidiva e facilitare l'identificazione dei colpevoli in considerazione della natura spregevole dei reati in parola. In ogni caso i ricorrenti erano abilitati dalla normativa interna a presentare una petizione per la cancellazione dei dati dal momento in cui la decisione alla base dell'iscrizione fosse stata annullata.

Secondo la Corte, nel caso di specie la durata della conservazione dei dati risulta proporzionata alle finalità della memorizzazione delle informazioni. Infatti l'inclusione delle informazioni relative ai ricorrenti nella banca–dati bilancia gli interessi concorrenti pubblici e privati in gioco. A tale riguardo lo Stato convenuto non ha superato il margine di apprezzamento accettabile. L'entità di questo margine è variabile e dipende da una serie di fattori, compresa la natura delle attività interessate e gli obiettivi delle restrizioni. Così, quando risulta in gioco un aspetto particolarmente importante della vita o dell'identità di un individuo, il margine di apprezzamento lasciato allo Stato è generalmente limitato. La Corte non può mettere in discussione gli obiettivi di prevenzione di una banca–dati come quella in cui è inserito il nome del ricorrente, condannato a quindici anni di reclusione per aver violentato un minore. Sottolinea che lo scopo di tale banca–dati è quello di prevenire la criminalità, in particolare evitare la recidiva e facilitare l'identificazione dei colpevoli e che i bambini e le altre persone vulnerabili hanno diritto alla protezione da parte dello Stato nella forma di una effettiva protezione. Allo stesso tempo,

[149] *B.B. v. France*, no. 5335/06, 17 December 2009.
[150] *Gardel v. France*, no. 16428/05, ECHR 2009.
[151] *M.B. v. France*, no. 22115/06, 17 December 2009.

secondo la Corte, accanto alla pena, cresce l'importanza della riabilitazione dei detenuti, soprattutto al termine di una lunga pena detentiva.

Per quanto riguarda la conservazione delle informazioni, la Corte rileva che si tratta di venti o trenta anni, a seconda della gravità della pena comminata. La Corte rileva inoltre che la persona può presentare domanda di cancellazione se i dati conservati non sono più rilevanti per le finalità del data–base, in relazione alla natura del reato, all'età della persona, all'epoca della commissione del reato, e al comportamento della persona. Tale procedimento giudiziario in tal modo assicura un controllo indipendente delle ragioni della conservazione dei dati sulla base di criteri specifici, e offre sufficienti garanzie per il rispetto della vita privata in relazione alla gravità dei reati che hanno giustificato l'inclusione iniziale. Anche se la memorizzazione dei dati per un lungo periodo potrebbe comportare un problema in termini dell'art. 8 della Convenzione, la Corte constata che il ricorrente ha, in ogni caso, la possibilità concreta di presentare una petizione per la cancellazione dei dati archiviati da quando la decisione che ha condotto alla loro iscrizione cessa di avere ogni effetto. In queste circostanze, la Corte ritiene che la durata della conservazione dei dati non è sproporzionata rispetto allo scopo della memorizzazione delle informazioni.

Per quanto riguarda l'utilizzo da parte delle pubbliche autorità della banca–dati in parola, la Corte osserva che il relativo accesso è stato ampliato più volte e che è stato consentito non soltanto alle autorità giudiziarie e di polizia, bensì anche ad organi amministrativi. Tuttavia, la consultazione è consentita solamente ad autorità soggette all'obbligo di riservatezza e in circostanze determinate. Inoltre, il ricorso non si presta ad un esame relativo alla questione dell'accesso alla banca–dati per fini amministrativi.

In conclusione, la Corte stabilisce che la registrazione dei ricorrenti nella banca–dati costituisce un bilanciamento degli interessi concorrenti pubblici e privati in gioco e che lo Stato convenuto non ha superato il margine di apprezzamento accettabile. Pertanto, nega qualsiasi violazione della Convenzione.

3. b) Nella sentenza *Khelili v. Switzerland*[152], la Corte ha riconosciuto la violazione della CEDU in una vicenda riguardante la classificazione di una donna francese come "prostituta"nella banca–dati informatica della polizia per cinque anni[153]. La ricorrente, scoperto che la polizia aveva inserito il suo nome in tale registro con la qualifica di "prostituta", presentava ricorso sul presupposto che l'inserimento di presunti dati falsi violasse il suo diritto al rispetto della vita privata (art. 8 CEDU).

[152] *Khelili v. Switzerland*, no. 16188/07, 18 October 2011.

[153] Durante un controllo di polizia a Ginevra, la polizia aveva rinvenuto occasionalmente il portafoglio della ricorrente nel quale, insieme ad alcune carte telefoniche, vi era un biglietto con una frase allusiva ad una disponibilità a svolgere il ruolo di escort.

La polizia affermava che l'inserimento del nominativo nella banca–dati era avvenuto sulla base di una legge sulla protezione dei dati, che autorizzava la gestione dei dati personali per il tempo necessario alla persecuzione e prevenzione dei reati. La richiesta di cancellazione era stata respinta con la motivazione che le informazioni in parola dovessero essere conservate in via preventiva. La ricorrente sosteneva invece che il mantenimento di tale qualificazione nel suo fascicolo la danneggiava gravemente, in quanto avrebbe potuto essere comunicata ai suoi potenziali e futuri datori di lavoro.

Secondo la Corte, malgrado l'ingerenza nei confronti della ricorrente trovava una base giuridica nel diritto interno, la sua qualificazione come "prostituta" avrebbe potuto nuocere molto alla sua reputazione. A tale riguardo, l'accusa di prostituzione illegale risultava generica e non sufficientemente provata (infatti non era mai stata condannata per esercizio illegale della prostituzione). Inoltre, la condanna della ricorrente per diffamazione e la qualificazione della medesima come "prostituta" non sembravano sufficientemente collegate. Il comportamento delle autorità pubbliche risultava pertanto contraddittorio.

La Corte concludeva che l'archiviazione nei registri della polizia di dati probabilmente falsi riguardanti la vita privata costituisce una violazione della vita privata e che il mantenimento per un periodo così lungo della qualificazione in parola non risultava giustificata, né necessaria in una società democratica.

La Corte ha constatato che la ricorrente avesse un interesse rilevante all'eliminazione della parola "prostituta" dai registri della polizia; ha ritenuto che il termine in questione avrebbe potuto danneggiare la sua reputazione, visto che le informazioni contenute negli archivi della polizia avrebbero potuto essere trasmesse e diffuse.

Vista la mancanza di condanna per prostituzione e alla luce della presunzione di innocenza in una società democratica, secondo la Corte, il mantenimento della parola "prostituta" come professione della ricorrente non poteva considerarsi come corrispondente ad un "bisogno sociale imperativo"(ex art. 8 CEDU). Inoltre per le autorità l'eliminazione della qualificazione offensiva dal registro della polizia non costituiva affatto un problema tecnico. Per tali ragioni, la Corte anche nel caso in parola ha ravvisato una violazione dei principi convenzionali (art. 8).

3. c) Nella sentenza *M.K. v. France*[154], le impronte digitali del ricorrente, presunto autore di furti di libri, erano state inserite in uno schedario automatizzato. A seguito di un'assoluzione e di un'archiviazione, il ricorrente contestava la mancanza di proporzionalità dei mezzi utilizzati. In particolare, che le autorità disponessero di un margine discrezionale eccessivo, con un potere di conservazione dei dati personali generico e indifferenziato. Denunciava inoltre il rischio concreto

[154] *M.K. v. France*, no. 19522/09, 18 April 2013.

di abuso facendo riferimento al trattamento improprio che aveva interessato altri schedari. Infine che la durata di conservazione fosse stata fissata arbitrariamente e si fosse tradotta nell'assenza di limiti temporali.

Il procuratore della Repubblica francese aveva sostenuto che il rifiuto di cancellazione delle impronte prelevate in occasione del secondo procedimento era motivato dalla necessità di tutelare proprio gli interessi del ricorrente, permettendo di escludere il suo coinvolgimento in caso di fatti commessi da altri con usurpazione della sua identità.

Sotto quest'ultimo profilo, la Corte ha osservato che l'argomento basato su una presunta garanzia di tutela contro attività illegittime di terzi volte ad usurpare un'identità equivarrebbe, in sostanza, a giustificare la schedatura di tutta la popolazione presente sul territorio, il che risulterebbe eccessivo e non pertinente.

Secondo la Corte, le circostanze del caso di specie, relative a episodi di furti di libri, dimostrano che la misura contestata trova applicazione in caso di reati minori. La causa in parola si distingue tuttavia da quelle che riguardano reati di criminalità organizzata o aggressioni sessuali. Inoltre, la Corte osserva che la normativa nazionale impugnata non opera distinzioni basate sull'esistenza di una condanna giurisdizionale, se non addirittura di un'azione penale avviata dal pubblico ministero. La situazione nel caso di specie presenta analogie con la sentenza *S. and Marper*, in quanto il ricorrente aveva beneficiato di un'assoluzione nell'ambito di un primo procedimento, quando i fatti contestati successivamente non erano ancora archiviati. Nella sentenza *S. and Marper* la Corte aveva sottolineato il rischio di "stigmatizzazione", derivante dal fatto che le persone che avevano rispettivamente beneficiato di un'assoluzione e di una decisione di archiviazione, ed avevano dunque il diritto di beneficiare della presunzione di innocenza, venivano trattate allo stesso modo dei condannati.

Inoltre, la Corte constata che la conservazione delle informazioni inserite nello schedario è di venticinque anni. Visto che poi le possibilità di accoglimento delle domande di cancellazione sono poche, tale durata è assimilabile ad una conservazione indefinita.

In conclusione, la Corte ha ritenuto che lo Stato convenuto fosse andato oltre il suo margine di apprezzamento. Infatti, il regime di conservazione delle impronte digitali di persone sospettate di avere commesso dei reati, ma non condannate, non garantiva un giusto equilibrio tra gli interessi pubblici e privati concorrenti. La conservazione dei dati risultava pertanto sproporzionata rispetto al diritto del ricorrente al rispetto della vita privata.

3. d) Nella decisione *Dalea v. France*[155], la Corte ha ritenuto compatibile con i

[155] *Dalea v. France*, appl. no. 964/07, decision 2 February 2010.

principi del "processo equo"(art. 6) e della tutela della vita privata (art. 8) una disciplina nazionale che limita la possibilità degli individui di avere accesso diretto e di apportare modifiche ai dati personali contenuti nella banca dati del sistema informativo Schengen (SIS).

Nel caso di specie, ad un cittadino romeno, segnalato dalle autorità francesi nella banca dati del sistema informativo Schengen ai fini della non ammissione nel territorio dello Stato, era stato rifiutato un visto per recarsi in Germania e successivamente un visto per recarsi in Francia[156]. Il ricorrente lamentava di non aver ottenuto la comunicazione delle informazioni che lo riguardavano né la loro rettifica o cancellazione.

Per quanto riguarda la presunta violazione del diritto ad un processo equo (art. 6), contestato dal ricorrente il quale non aveva potuto ottenere le motivazioni della sua segnalazione nel SIS, la Corte ha dichiarato il ricorso inammissibile sul presupposto che la procedura di accesso, rettifica o cancellazione dei dati personali contenuti nella banca dati Schengen prevista dal diritto francese risulta collegata alla disciplina relativa al rilascio dei visti per i cittadini di Stati terzi. A tale riguardo, la Corte ha stabilito che le decisioni su ingresso, soggiorno ed espulsione degli stranieri non rientrano nel campo di applicazione della CEDU, visto che non danno luogo a controversie su diritti ed obblighi di natura civile, né riguardano la fondatezza di un'accusa in materia penale. In particolare, la CEDU non riconosce in quanto tale il diritto di entrare o soggiornare in uno Stato per chi non è cittadino; pertanto la decisione sulla non ammissione in territorio francese, di cui il ricorrente era stato oggetto, i suoi effetti e la sua durata non potevano rientrare nel campo di applicazione della Convenzione (art. 6, par. 1).

Per quanto riguarda i presunti danni alla vita privata (art. 8), il ricorrente, a seguito del divieto di viaggiare nello spazio Schengen, non era stato in grado di indicare alcun pregiudizio concreto. Egli infatti si era limitato a segnalare "notevoli danni" per i suoi affari senza ulteriori specificazioni e l'impossibilità di eseguire un intervento in Francia, senza che ciò avesse avuto alcuna conseguenza negativa sulla sua salute. Pertanto, la Corte ha ritenuto che l'ingerenza da parte delle autorità francesi nel diritto del ricorrente al rispetto della privacy risultava proporzionata allo

[156] La normativa francese in materia prevede che il diritto di accesso alle informazioni sensibili debba essere esercitato mediante la Commission Nationale Informatique et Libertés (CNIL). Nel caso di specie, la CNIL aveva rifiutato di rivelare al ricorrente i dati SIS che lo riguardavano, nonchè la loro rimozione o correzione. Pertanto, il ricorrente avanzava un ricorso per abuso di potere dinanzi al Conseil d'Etat. Quest'ultimo stabiliva che, sulla base delle indagini svolte, non era stato possibile conoscere le ragioni dell'inserimento del nominativo del ricorrente nella banca dati e che quindi non era possibile valutare se il rifiuto di rettifica o di eliminazione da parte del CNIL fosse legittimo. Infatti la CNIL affermava che il ricorrente era stato inserito nel SIS su richiesta dell'Agenzia francese Security Intelligence (DST). La giustificazione in parola, secondo il Consiglio di Stato, appariva valida, pertanto il ricorso del ricorrente per l'annullamento della decisione della CNIL veniva dichiarato infondato.

scopo perseguito e rispettava il requisito della "necessità" in una società democratica. In considerazione del fatto che l'interferenza nella vita privata del ricorrente derivava esclusivamente dall'inclusione nel sistema d'informazione Schengen per un lungo periodo, la Corte ha ribadito che a coloro che sono interessati da un provvedimento statale fondato su motivi di sicurezza nazionale può essere garantita protezione solo contro l'arbitrarietà.

3. e) Nella sentenza *E.B. and Others v. Austria*[157], in discussione era il rifiuto di modificare il casellario giudiziario a seguito della sopravvenuta dichiarazione di incostituzionalità della disposizione sulla base della quale i ricorrenti erano stati condannati[158].

A seguito dell'abrogazione del reato relativo a rapporti omosessuali fra adulti e minorenni, i ricorrenti chiesero che le loro condanne fossero eliminate dal casellario giudiziario. Tuttavia, il Ministero dell'Interno austriaco si rifiutava di adempiere alla richiesta, argomentando di non avere il potere di eliminare una condanna registrata legittimamente.

Vista la natura sensibile e l'impatto sulla vita privata delle persone interessate delle informazioni contenute nel casellario, la Corte ha ritenuto applicabile l'art. 14 in combinato disposto con l'art. 8. La circostanza che un reato sia stato dichiarato costituzionalmente illegittimo non avrebbe determinato automaticamente l'invalidità anche della *misura accessoria* della registrazione nel casellario giudiziale (contenuta in altra disposizione a carattere generale per tutti i reati). Tuttavia, considerato che la conservazione di una condanna sulla base di tali reati avrebbe potuto produrre conseguenze particolarmente gravi per le persone interessate, la nuova normativa in materia avrebbe dovuto prevedere una misura appropriata al riguardo.

In conclusione, la Corte ha riconosciuto la violazione dell'art. 8 nonché dell'art. 13 (diritto ad un ricorso effettivo).

3. f) Molto interessante è la sentenza *Bernh Larsen v. Norway*[159] che ha affermato la legittimità convenzionale della richiesta delle autorità fiscali rivolta ad una società di fornire copia dei dati di un server condiviso con altre società. La Corte ha accolto la tesi dei giudici nazionali che, per ragioni di efficienza fiscale, avevano ammesso la possibilità delle autorità di agire indipendentemente dal carattere misto della banca dati. In particolare, le autorità fiscali regionali norvegesi avevano chiesto che

[157] *E.B. and Others v. Austria*, nos. 31913/07, 38357/07, 48098/07, 48777/07 and 48779/07, 7 November 2013.

[158] I ricorrenti erano stati condannati per reati previsti dall'art. 209 del codice penale, che prevedeva l'illiceità dei rapporti omosessuali tra adulti e individui di sesso maschile consenzienti di età compresa tra i 14 e i 18 anni. La norma in parola era stata abrogata a seguito di una sentenza della Corte costituzionale. La Corte di Strasburgo aveva ritenuto la disposizione discriminatoria, vista la sua applicazione ai soli rapporti omosessuali tra individui di sesso maschile e non di sesso femminile.

[159] *Bernh Larsen Holding AS and Others v. Norway*, no. 24117/08, 14 March 2013.

ai revisori fiscali fosse consentito di effettuare copia di tutti i dati conservati nel server. La società ricorrente ne aveva consentito l'accesso, ma aveva rifiutato di fornire copia di tutta la documentazione del server, in quanto di proprietà di un'altra società e utilizzato in comune con altre aziende.

Tuttavia le autorità fiscali avevano esteso l'accertamento alle altre società. I ricorsi amministrativi e giurisdizionali delle varie società non avevano sortito alcun effetto favorevole in quanto le disposizioni in materia fiscale relative all'accesso alle banche dati e ai documenti contabili consentivano un ampio accesso senza necessità di una selezione preliminare dei dati rilevanti per l'indagine tributaria.

La Corte ha stabilito che, malgrado l'autorizzazione alla copia di tutti i dati sui server costituisse un'interferenza con il diritto alla vita privata (art. 8), l'interferenza in parola trovava fondamento giuridico in una legge dello Stato chiara, sufficientemente precisa e prevedibile. pertanto essa era stata adottata nell'interesse del benessere economico del Paese e perseguiva un obiettivo legittimo. La Corte ha condiviso le argomentazioni dei giudici nazionali secondo le quali, per ragioni di efficienza fiscale, i poteri di azione delle autorità sono relativamente ampi nella fase preparatoria e non possono essere vincolati dalle indicazioni del soggetto a cui i dati si riferiscono, malgrado l'archivio comprendesse documenti appartenenti ad altri soggetti fiscali. La Corte ha affermato peraltro che le disposizioni nazionali non conferivano alle autorità fiscali poteri illimitati, in quanto non consentono l'accesso ad archivi appartenenti interamente ad altri soggetti fiscali; tuttavia, nel caso di specie, in mancanza di una netta linea di demarcazione tra i vari archivi contenuti nel medesimo server, le autorità dovevano essere messe in grado di accedere a tutti i dati presenti sul server al fine di valutarne la rilevanza.

Per quanto riguarda la proporzionalità della misura, la Corte ha osservato che la procedura volta ad ottenere una copia dei dati contenuti nel server prevedeva una serie di garanzie contro eventuali abusi. Infatti l'intenzione delle autorità fiscali di effettuare la verifica era stata notificata alla società ricorrente con largo anticipo, pertanto i suoi rappresentanti avrebbero potuto esprimere osservazioni in occasione del sopralluogo; inoltre i dati erano stati acquisiti secondo una procedura di sicurezza (la copia dei dati era stata collocata in una busta sigillata e depositata presso l'ufficio delle imposte in attesa della decisione sul ricorso presentato dalle società interessate); il contribuente aveva visto riconosciuto il diritto ad essere presente in occasione della rottura del sigillo e a ricevere copia del rapporto di audit; il trattamento dei dati era lecito e proporzionato considerato anche che, completata la revisione, la copia del server sarebbe stata distrutta ed ogni traccia dei contenuti sarebbe stata cancellata dai computer delle autorità fiscali. Sulla base di tutte queste considerazioni, la Corte ha escluso la violazione del diritto al rispetto della vita privata.

4. a) La sentenza *Peck v. the United Kingdom*[160] riguardava immagini video acquisite mediante l'utilizzo di una telecamera a circuito chiuso installata da un Comune. Le immagini riguardavano un tentativo di suicidio. La Corte era stata chiamata ad esaminare la violazione del diritto al rispetto della vita privata, a seguito della divulgazione sui media dei filmati effettuati in strada. Le riprese video infatti mostravano i tagli sui polsi del ricorrente senza che la sua identità fosse risultata adeguatamente celata così da risultare irriconoscibile. In ogni caso, non si trattava di divulgazione di filmati sulla commissione di un reato per il quale il ricorrente fosse stato accusato o condannato.

In generale, secondo la Corte, registrazioni sistematiche, permanenti e di dominio pubblico pongono il problema della tutela della vita privata, ma il semplice monitoraggio delle azioni di un individuo in un luogo pubblico, che registra dati visibili, non causa in sé un'ingerenza nella vita privata. Se un individuo è visibile in una strada pubblica da qualsiasi altra persona presente, il monitoraggio con mezzi tecnologici della stessa scena pubblica non può alterare il "carattere pubblico" e l'accessibilità universale alle immagini. In materia di divulgazione di dati personali, la Corte ribadisce l'importanza della ponderazione tra i contrapposti interessi pubblici e privati in gioco ed il margine di apprezzamento lasciato allo Stato contraente. In ogni caso, il diritto interno deve predisporre idonee misure per vietare qualsiasi tipo di divulgazione contrastante con le garanzie previste dalla CEDU (art. 8).

Nel caso di specie, secondo la Corte, l'identificazione del ricorrente nelle indagini di polizia avrebbe potuto avvenire prima della diffusione dei filmati. In ogni caso, l'identità del ricorrente avrebbe potuto essere nascosta. Pertanto il mancato rispetto delle garanzie minime per la protezione della vita privata aveva determinato nella fattispecie in parola un'interferenza sproporzionata ed ingiustificata.

La Corte osserva che il concetto di "vita privata" è ampio e non suscettibile di definizione esaustiva. Il sesso, il nome, l'orientamento sessuale e la vita sessuale sono elementi importanti della sfera personale protetta dall'art. 8 CEDU. La norma in parola tutela altresì il diritto di identità e di sviluppo personale, nonchè di stabilimento e di sviluppo di relazioni con il mondo esterno (incluse attività di natura professionale o commerciale). Pertanto, nel concetto di "vita privata" può rientrare altresì l'interazione di una persona con gli altri in un contesto pubblico.

Il monitoraggio delle azioni di un individuo in un luogo pubblico con l'uso di apparecchiature fotografiche, che non registra dati visibili, non rappresenta in

[160] *Peck v. the United Kingdom*, no. 44647/98, ECHR 2003-I.

quanto tale un'ingerenza nella vita privata dell'individuo[161]. D'altra parte, la registrazione a carattere sistematico o permanente di dati può dar luogo a tale ingerenza. Pertanto, la raccolta di dati da parte dei servizi di sicurezza su singoli individui, anche senza l'uso di metodi di sorveglianza segreta, costituisce un'ingerenza nella vita privata dei ricorrenti.

Nel determinare se la divulgazione è stata "necessaria in una società democratica", la Corte ha valutato se, considerato il caso nel suo complesso, le ragioni addotte per giustificare la divulgazione fossero state "pertinenti e sufficienti" e se le misure adottate fossero state proporzionate rispetto ai legittimi obiettivi perseguiti.

Nei casi concernenti la divulgazione di dati personali, la Corte ha stabilito che alle autorità nazionali competenti deve essere lasciato un margine di apprezzamento al fine di trovare un giusto equilibrio tra i contrapposti interessi pubblici e privati. Tuttavia, la portata del margine in parola dipende da fattori quali la natura e la gravità degli interessi in gioco. Ha concluso pertanto che l'ingerenza contro il ricorrente non risultasse compatibile con la CEDU in mancanza di un motivo imperioso di interesse pubblico.

4. b) Nella sentenza *Vetter v. France*[162], alcuni testimoni anonimi avevano accusato il ricorrente di omicidio. Vista la sua assidua presenza presso l'abitazione di un amico, la polizia vi aveva installato alcuni dispositivi di ascolto, con l'autorizzazione del giudice per le indagini preliminari. Sulla base delle conversazioni registrate, il ricorrente era stato arrestato e processato per omicidio. Da sottolineare la mancanza nel diritto interno di specifiche disposizioni procedurali sull'installazione di dispositivi di ascolto in una proprietà privata.

Il punto giuridico centrale della sentenza in parola riguarda l'utilizzo dei dispositivi di ascolto "in conformità con la legge"(art. 8 CEDU). ll ricorrente contestava che, nell'ambito dell'indagine che aveva condotto alla sua incriminazione, gli investigatori avessero effettuato registrazioni nell'appartamento di un terzo. Denunciava pertanto l'illegalità di questa prassi, non prevista dal codice di procedura penale, per violazione del suo diritto al rispetto della vita privata.

La Corte ha riconosciuto come i fatti addotti dal ricorrente costituissero senza dubbio un'interferenza con i diritti convenzionali. Infatti l'intercettazione delle conversazioni telefoniche e l'ascolto delle conversazioni mediante l'installazione di microfoni possono arrecare un grave pregiudizio alla privacy. Le operazioni in parola devono pertanto basarsi su una normativa chiara e dettagliata. Ciò è essenziale, visto che l'uso di tecnologie sempre più sofisticate. La Corte ha ritenuto

[161] Si veda, ad esempio, *Herbecq and Another v. Belgium*, appl. nos. 32200/96 e 32201/96, Commission decision of 14 January 1998, DR 92-A, p. 92.
[162] *Vetter v. France*, no. 59842/00, 31 May 2005.

che la base giuridica debba fornire adeguate garanzie nei confronti di possibili abusi, così come in materia di intercettazioni telefoniche. In particolare, devono essere definite le categorie di persone alle quali possono essere applicate tali misure e il tipo di reati contestati. Al giudice dovrebbe essere richiesto di fissare un limite massimo di durata dell'esecuzione della misura; di specificare le condizioni per la predisposizione di verbali che sintetizzino le conversazioni registrate; di stabilire precauzioni per la conservazione delle registrazioni in caso di eventuale ispezione da parte del giudice e della difesa, nonchè le circostanze in base alle quali si possa procedere alla cancellazione ed alla distruzione, soprattutto a seguito del non luogo a procedere o del proscioglimento dell'imputato.

4. c) Nella decisione di irricevibilità nel caso *Kopke v. Germany*[163], la ricorrente, cassiera di un supermercato, era stata licenziata senza preavviso per furto, a seguito di una videosorveglianza effettuata a sua insaputa dal datore di lavoro con l'aiuto di un'agenzia investigativa privata[164]. Il ricorso interno dinanzi al giudice del lavoro era stato respinto, così come il ricorso costituzionale.

La "vita privata"della ricorrente (ex art. 8, par. 1) era stata pertanto interessata da tali misure di videosorveglianza. La Corte ha dovuto esaminare se lo Stato contraente, nell'ambito dei suoi obblighi positivi, avesse bilanciato da una parte il diritto della ricorrente al rispetto della sua vita privata e dall'altra l'interesse del datore di lavoro alla protezione del suo diritto di proprietà (art. 1 del Protocollo n. 1) nonchè l'interesse pubblico alla corretta amministrazione della giustizia.

Nel caso di specie, nessuna normativa nazionale stabiliva le condizioni in base alle quali un datore di lavoro poteva ricorrere alla videosorveglianza di un dipendente per indagare su un eventuale reato penale commesso durante l'attività lavorativa.

Tuttavia, secondo la Corte, la Corte nazionale federale del lavoro aveva elaborato importanti garanzie contro ingerenze arbitrarie nel diritto alla privacy dei lavoratori. Tale giurisprudenza era stata applicata dal giudice nazionale nel caso in parola. Inoltre, la videosorveglianza nascosta sul posto di lavoro a seguito di sospetti motivati, nel caso di specie di furto, non costituiva un'interferenza con la vita privata al punto tale da richiedere ad uno Stato un quadro legislativo per conformarsi agli obblighi positivi derivanti dall'art. 8 CEDU. Come rilevato dai giudici tedeschi, la videosorveglianza della ricorrente era stata eseguita a seguito di perdite ed irregolarità nei conti del dipartimento in cui era impiegata. Il sospetto di furto aveva riguardato la ricorrente e un altro dipendente, che erano stati gli unici

[163] *Kopke v. Germany*, appl. no. 420/07, Decision 5 October 2010.

[164] Dietro indicazione del datore di lavoro, la condotta della ricorrente sul luogo di lavoro era stata oggetto di videoregistrazione senza preavviso. Le immagini così ottenute erano state esaminate ed utilizzate nel pubblico procedimento dinanzi ai giudici del lavoro.

destinatari della misura di sorveglianza. La registrazione aveva avuto luogo per un tempo circoscritto (due settimane) ed aveva riguardato esclusivamente l'area della cassa accessibile al pubblico. Le immagini ottenute erano state visionate da un numero limitato di persone impiegate dall'agenzia investigativa e dai membri dello staff del datore di lavoro. Erano state utilizzate solo in occasione della cessazione del rapporto di lavoro e del procedimento dinanzi al giudice del lavoro. L'interferenza con la vita privata della ricorrente era stata pertanto limitata a quanto strettamente necessario per il conseguimento degli obiettivi perseguiti dalla videosorveglianza.

Inoltre i giudici nazionali avevano ritenuto che l'interesse del datore di lavoro alla protezione del suo diritto di proprietà poteva risultare salvaguardato soltanto mediante la raccolta di prove idonee a dimostrare la condotta criminale della ricorrente nel procedimento penale. Ciò risultava utile anche al fine del perseguimento dell'interesse pubblico alla buona amministrazione della giustizia. Inoltre, la videosorveglianza nascosta era servita per eliminare qualsiasi tipo di sospetto su altri dipendenti. In sostanza, non vi era una misura ugualmente efficace per proteggere i diritti di proprietà del datore di lavoro che avrebbe interferito in misura minore con il diritto della ricorrente al rispetto della sua vita privata. Un inventario non avrebbe potuto chiaramente collegare le perdite economiche ad un singolo lavoratore, così come la sorveglianza da parte dei superiori e dei colleghi (o una videosorveglianza aperta) non avrebbero condotto ad un risultato sicuro.

In conclusione, secondo la Corte, nulla indicava che le autorità nazionali non fossero riuscite a trovare un giusto equilibrio tra gli interessi rilevanti in gioco. Malgrado ciò, la Corte non ha mancato di rilevare che il bilanciamento operato dalle autorità nazionali tra gli interessi in gioco non sembrava l'unica via possibile per l'adempimento degli obblighi derivanti dalla Convenzione. Infatti, agli interessi contrastanti sarebbe stato possibile riconoscere, in futuro, un peso diverso, tenuto conto della portata delle ingerenze nella vita privata degli individui rese possibili dalle nuove tecnologie.

Sebbene lo scopo del principio convenzionale riguardi la protezione dell'individuo contro ingerenze arbitrarie da parte di pubbliche autorità, l'art. 8 non si limita ad imporre allo Stato di astenersi da tali ingerenze, bensì prevede obblighi positivi relativi all'effettivo rispetto della vita privata. A tale riguardo, il confine tra obblighi positivi e negativi dello Stato non si presta ad una definizione precisa. In ogni caso, si deve avere riguardo al giusto equilibrio tra gli interessi in gioco, che può includere interessi concorrenti privati e pubblici o diritti previsti dalla CEDU[165]. La Corte ribadisce, infine, che ci sono diversi modi di garantire il rispetto della vita

[165] *Evans v. the United Kingdom* [GC], no. 6339/05, §§ 75 and 77, ECHR 2007-I. V. altresì *Von Hannover v. Germany*, no. 59320/00, § 57, ECHR 2004-VI; *Reklos and Davourlis v. Greece*, no. 1234/05, § 36, 15 January 2009; *Benediktsdóttir v. Iceland*, appl. no. 38079/06, Decision, 16 June 2009.

privata e che la natura degli obblighi dello Stato dipende dal particolare aspetto della vita privata in discussione. La scelta dei mezzi per garantire la conformità convenzionale nel campo della protezione contro atti di individui si colloca, in linea di principio, all'interno del margine di apprezzamento dello Stato[166].

4. d) La sentenza *Van Vondel v. the Netherlands*[167] riguardava la fornitura da parte della polizia di assistenza tecnica ad un individuo per la registrazione delle sue conversazioni con il ricorrente in assenza di un quadro normativo[168].

Secondo la Corte, l'ottenimento da parte della polizia, ufficialmente ai fini di una un'indagine autorizzata, di registrazioni di conversazioni tra il ricorrente e il suo informatore costituiva un'ingerenza nella vita privata del ricorrente e nella corrispondenza, imputabile ad una pubblica autorità.

La Corte ricorda innanzitutto che il termine "vita privata" non deve essere interpretato in maniera restrittiva. In particolare, il rispetto della vita privata comprende il diritto di stabilire e sviluppare relazioni con altri esseri umani; inoltre, non vi è alcuna ragione di principio per escludere le attività di natura professionale dalla nozione di "vita privata". Pertanto riconosce una sfera di interazione di una persona con gli altri anche in un contesto pubblico, che può rientrare nell'ambito di applicazione della nozione di "vita privata".

La Corte ricorda altresì che la registrazione di conversazioni telefoniche private e l'uso privato di tali registrazioni non è di per sé contrastante con la CEDU, se ciò avviene attraverso l'uso di mezzi privati. Tuttavia, nel caso di specie, le registrazioni delle conversazioni del ricorrente erano state eseguite dall'informatore mediante le attrezzature fornite dalle autorità, che in almeno una occasione avevano dato altresì specifiche istruzioni circa le informazioni da ottenere. Pertanto, le autorità di polizia avevano fornito un contributo essenziale all'esecuzione della misura in discussione. La Corte ha ritenuto che non fosse stato l'informatore a controllare l'attività di registrazione. Sostenere il contrario avrebbe voluto dire consentire alle autorità inquirenti di eludere gli obblighi convenzionali mediante l'uso di privati cittadini.

Per quanto riguarda la questione se l'ingerenza avesse avuto luogo "in conformità con la legge"(ex art. 8, par. 2), la Corte ha ricordato che ciò comporta che la misura in questione debba avere una base nel diritto interno. Al contrario, il governo non

---

[166] V. *X and Y v. the Netherlands*, 26 March 1985, § 24, Series A no. 91; *M.C. v. Bulgaria*, no. 39272/98, § 150, ECHR 2003-XII; *K.U. v. Finland*, no. 2872/02, § 43, ECHR 2008.

[167] *Van Vondel v. the Netherlands*, no. 38258/03, 25 October 2007.

[168] Il ricorrente era stato un ufficiale di polizia, le cui conversazioni telefoniche con un informatore erano state registrate nel contesto di un'inchiesta parlamentare conseguente ad un'indagine penale. Egli stato condannato per aver giurato il falso nell'ambito dell'inchiesta parlamentare e per il tentativo di intimidazione di un potenziale testimone, suo ex informatore. I tribunali nazionali avevano basato la sentenza di condanna sulle registrazioni di conversazioni telefoniche che l'informatore aveva fatto di propria iniziativa con il ricorrente e con l'ausilio di dispositivi usati dalla polizia.

era riuscito a dimostrare che l'ingerenza in questione avesse un fondamento giuridico. Inoltre, poiché si trattava di una indagine conoscitiva, alla polizia non era stato consentito di avvalersi di poteri investigativi, come, per esempio, la registrazione segreta delle conversazioni. La Corte ha condannato pertanto lo Stato convenuto sul presupposto che, per ragioni pratiche, ad un testimone, la cui credibilità probabilmente era stata compromessa, fosse stata fornita assistenza tecnica al fine di provare la sua versione dei fatti. Riteneva inaccettabile la fornitura di tale assistenza da parte di pubbliche autorità in assenza di un quadro giuridico idoneo ad evitare abusi. Al ricorrente, infatti, era stata negata quella protezione minima, cui avrebbe avuto diritto in una società democratica.

Cap. II.
Il bilanciamento con la tutela della salute

1. *Armonienė v. Lithuania* – 2. *Gillberg v. Sweden* – 3. *Avilkina and Others v. Russia*

In numerose sentenze, la Corte ha affermato che "il rispetto della riservatezza dei dati sanitari è un principio vitale nei sistemi giuridici di tutte le Parti contraenti della Convenzione. E' fondamentale non solo per il rispetto della privacy di un paziente, ma anche per preservare la sua fiducia nella professione medica e nel servizio sanitario in generale"[169].

Tuttavia, la Corte ha ammesso che gli interessi di protezione della riservatezza dei dati medici di un paziente e di una comunità nel suo insieme possono essere superati dall'interesse di indagine e di perseguimento dei reati e della trasparenza dei procedimenti giudiziari, dove tali interessi assumano un'importanza preminente.

1. Nel caso *Armonienė v. Lithuania*[170], malgrado i tribunali interni avessero dichiarato che il loro diritto alla privacy fosse stato gravemente violato, i ricorrenti avevano ricevuto un risarcimento irrisorio. In particolare, lamentavano un basso risarcimento del danno non patrimoniale ottenuto sulla base del diritto interno dell'epoca. In entrambi i casi, la Corte non si è discostata dalle conclusioni cui erano giunti i giudici nazionali circa la violazione della privacy dei ricorrenti. In particolare, la circostanza che essi vivessero in un piccolo villaggio aveva aumentato il loro disagio ed esclusione dalla vita sociale, vista la possibilità che tutti venissero a conoscenza della loro malattia. La Corte ha espresso perplessità sulla circostanza che le informazioni circa la salute del ricorrente diffuse dal giornale fossero state confermate dal personale medico. In ogni caso, ha stabilito che la pubblicazione dell'articolo contestato non trovava giustificazione in un legittimo interesse pubblico.

Sulla base delle diverse prassi esistenti negli Stati contraenti, il concetto di "vita privata" varia notevolmente da caso a caso. Pertanto, secondo la Corte, quello in parola è un settore nel quale gli Stati godono di un ampio margine di discrezionalità nel definire le misure da adottare per garantire il rispetto della CEDU, tenuto conto delle esigenze e delle risorse della comunità e dei singoli. La Corte ricorda tuttavia che il diritto al rispetto della vita privata, così come ogni altra disposizione convenzionale, deve essere interpretato in modo tale da garantire che i diritti siano concreti ed efficaci.

---

[169] A tal proposito *Z. v. Finland*, 25 February 1997, §§ 95-99, *Reports of Judgments and Decisions* 1997-I; *M.S. v. Sweden*, 27 August 1997, § 41, *Reports of Judgments and Decisions* 1997-IV.

[170] V. *Armonienė v. Lithuania*, no. 36919/02, 25 November 2008. Il caso riguardava la pubblicazione in prima pagina da parte del più importante quotidiano della Lituania di un articolo circa la diffusione del virus dell'AIDS in una parte remota del Paese, con l'indicazione dei nomi di alcune persone che erano risultate positive al test dell'HIV. Come fonte della notizia l'articolo citava il personale medico dell'ospedale locale. Le persone interessate citavano in giudizio il giornale (separatamente) per violazione del loro diritto alla privacy. Il tribunale aveva riconosciuto in loro favore la pubblicazione di informazioni personali senza consenso e in mancanza di un legittimo interesse pubblico. In entrambi i casi, tuttavia, il tribunale rilevava che non era stato dimostrato che le informazioni lesive del diritto alla privacy fossero state pubblicate intenzionalmente.

Secondo la Corte, in generale, il rispetto della riservatezza dei dati sanitari è un principio fondamentale nei sistemi giuridici di tutti gli Stati contraenti, specie in caso di una persona affetta da HIV. In tale contesto, infatti, la divulgazione dei dati personali può danneggiare notevolmente la vita privata e familiare, così come quella sociale e lavorativa della persona, esponendola a giudizi negativi e al rischio di esclusione sociale.

Nel caso di specie, la Corte ha valutato la possibile esistenza di un interesse pubblico che giustificasse la pubblicazione di informazioni sulla salute dei ricorrenti e i loro dati anagrafici. A tale riguardo, è giunta alla conclusione che ciò non corrispondeva ad alcun interesse pubblico preminente. Infatti, l'unico scopo apparente era quello di soddisfare la curiosità del pubblico e non di dare un contributo ad un dibattito di interesse generale per la società.

La Corte, pur riconoscendo la discrezionalità degli Stati contraenti in materia di risarcimento per danno morale e malgrado la compatibilità di limiti a tale risarcimento con l'obbligo positivo ex art. 8 CEDU, ha tuttavia stabilito che i limiti in parola non devono svuotare di significato il diritto alla protezione della privacy. L'imposizione di pesanti sanzioni alla stampa avrebbe potuto avere un effetto negativo sull'esercizio della libertà di stampa. Tuttavia, in caso di gravissimo abuso, deve ritenersi prevalente l'interesse della vittima ad ottenere un giusto risarcimento dei danni subiti, anche per scoraggiare la reiterazione di condotte lesive. Pertanto, la Corte ha rigettato l'eccezione preliminare del Governo relativa alla qualificazione del ricorrente come vittima e ha riconosciuto che lo Stato convenuto non aveva garantito il diritto del ricorrente al rispetto della sua vita privata e familiare.

Anche nella sentenza collegata *Biriuk v. Lithuania*[171], la ricorrente aveva chiesto il risarcimento del danno nei confronti del medesimo quotidiano a causa della pubblicazione del suo nome in relazione alla sieropositività. Anche in questo caso la Corte ha ritenuto che l'articolo di stampa non contribuisse ad alcun dibattito d'interesse generale e ha ribadito che la protezione dei dati personali, e non ultimo dei dati sanitari, è fondamentale affinché una persona possa godere del proprio diritto al rispetto della vita privata e familiare. La Corte ha qui sottolineato la gravità del fatto che, secondo l'articolo di giornale, il personale medico di un ospedale avesse fornito informazioni sull'infezione da HIV in manifesta violazione dell'obbligo al segreto medico. Di conseguenza, lo Stato convenuto era stato condannato.

2. Nella sentenza *Gillberg v. Sweden*[172], il ricorrente era stato il responsabile di una ricerca scientifica eseguita su numerosi bambini ai cui genitori aveva garantito la massima riservatezza circa il trattamento dei dati raccolti. Successivamente, altri due ricercatori chiedevano di avere accesso ai dati e, di fronte al diniego da parte

[171] *Biriuk v. Lithuania*, no. 23373/03, 25 November 2008.
[172] *Gillberg v. Sweden*, no. 41723/06, 2 November 2010.

dell'Università, presentavano ricorso ad un tribunale, che si esprimeva in senso favorevole all'utilizzo dei dati sensibili, seppur a determinate condizioni. Quando l'autore della ricerca rifiutava di rendere disponibili i dati, sulla base della garanzia di riservatezza fatta ai partecipanti, veniva condannato per abuso d'ufficio.

Il ricorso dell'autore della ricerca per violazione del diritto alla riservatezza (art. 8) e della libertà di espressione (art. 10) veniva deciso in senso negativo dalla terza sezione della Corte e poi devoluta alla Grande Camera.

Per quanto riguarda la violazione del diritto al rispetto della "vita privata", secondo il ricorrente la condanna penale aveva pregiudicato il suo onore e la sua reputazione. A tale riguardo, la Corte ha affermato che l'art. 8 non potesse essere invocato per la perdita di reputazione che derivi da azioni proprie, quali ad esempio la commissione di un reato.

Quanto alle conseguenze negative a livello sociale, psicologico ed economico, la Corte ha osservato l'assenza di qualsiasi giurisprudenza che riconosca che una condanna penale di per sé costituisca un'ingerenza nel diritto del condannato al rispetto della vita privata. Pertanto ha ritenuto che, sotto il profilo in parola, i diritti del ricorrente non risultassero violati.

La Grande Camera ha osservato che la condanna era fondata sul mancato rispetto dei doveri di pubblico ufficiale da parte del ricorrente, che non aveva dato esecuzione alla sentenza del giudice svedese. A parere della Corte, la condanna del ricorrente era conforme alla legge e perseguiva obiettivi legittimi, vale a dire la prevenzione dei disordini e della criminalità e la tutela dei diritti e delle libertà altrui. Il fatto che la Corte d'appello non avesse considerato come circostanza attenuante il tentativo del ricorrente di protezione dell'identità dei partecipanti alla ricerca non costituiva, a parere della Corte, un superamento del margine di apprezzamento da parte dello Stato. Inoltre, la condanna inflitta al ricorrente non poteva considerarsi sproporzionata o arbitraria rispetto agli scopi legittimi perseguiti. Infine, esclude altresì la violazione dell'art. 10 CEDU (libertà di espressione) declinato dal ricorrente come diritto a non diffondere documenti riservati.

Nella loro opinione dissenziente, i giudici Gyulumyan e Ziemele hanno sottolineato che la distruzione dei dati raccolti da parte del team di ricerca del ricorrente risultava motivato dall'interesse di proteggere le famiglie coinvolte nella ricerca universitaria. I ricercatori avevano assicurato la riservatezza delle informazioni raccolte. Secondo i giudici, la garanzia di riservatezza risulta essenziale nel settore delle ricerche mediche e sociali. E' solo la garanzia del rispetto della riservatezza che consente l'ottenimento di dati più accurati negli studi. In altre parole, se l'obiettivo della scienza è quello di progredire in ambiti importanti, la riservatezza e la protezione dei dati trattati risulta di fondamentale importanza.

Tuttavia, osservano i due giudici, nel campo della ricerca medica la riservatezza non costituisce un obiettivo primario. Al contrario, è il dibattito pubblico sui risultati delle ricerche a costituire un aspetto fondamentale sia sotto il profilo della qualità che della trasparenza dei progressi scientifici. Inoltre il dovere di rendere pubblici i risultati di una ricerca prescinde dalla loro positività o negatività.

In ogni caso, l'interesse pubblico alla diffusione delle scoperte scientifiche deve trovare un giusto bilanciamento con il principio di riservatezza dei singoli. I giudici si sono interrogati se il diritto di accesso ai documenti, così come previsto dalla normativa dello Stato convenuto, risultasse adeguato rispetto alle moderne esigenze della ricerca medica e al diritto alla privacy. Essi sono giunti alla conclusione che, nel caso di specie, la sentenza penale avesse avuto conseguenze eccessive sulla vita del ricorrente. Infatti, se è vero che uno Stato deve promuovere la scienza medica sia nell'interesse della società che per ragioni di concorrenza e di sviluppo economico, ciò deve avvenire nel rispetto dei diritti umani di coloro che accettano di partecipare alle ricerche e nel rispetto di coloro che le eseguono. Pertanto i giudici dissenzienti hanno auspicato un'applicazione meno rigida del principio che disciplina l'accesso alle informazioni. La tutela del diritto alla vita privata nel contesto della ricerca scientifica risulta infatti una questione complessa che i giudici nazionali non avrebbero dovuto ignorare.

3. La sentenza *Avilkina and Others v. Russia*[173] riguarda il diritto al rispetto della vita privata e familiare in relazione alla diffusione di informazioni mediche confidenziali.

Il ricorso dinanzi alla Corte veniva presentato da un'organizzazione religiosa e da alcuni testimoni di Geova di cittadinanza russa[174]. A seguito del rifiuto di ricevere una trasfusione di sangue, essi denunciavano la divulgazione delle loro cartelle cliniche a favore delle autorità inquirenti russe, per violazione degli artt. 8 e 14 CEDU (divieto di discriminazione). Infatti, in occasione di un'inchiesta sulla legalità delle attività dell'organizzazione religiosa ricorrente, gli ospedali avevano ricevuto l'ordine di segnalare i casi di rifiuto di trasfusioni di sangue da parte di testimoni di Geova. La Corte ha stabilito che non sussisteva alcuna necessità sociale urgente che giustificasse la divulgazione di informazioni mediche confidenziali alle autorità inquirenti. Rivelando informazioni confidenziali senza che i ricorrenti ne fossero preventivamente informati e senza dar loro la possibilità di opposizione, l'autorità inquirente aveva impiegato mezzi coercitivi sproporzionati.

[173] *Avilkina and Others v. Russia*, no. 1585/09, 6 June 2013.

[174] Le autorità russe, nel reprimere il culto dei testimoni di Geova, avevano violato libertà fondamentali garantite dalla Costituzione della Federazione Russa e dalla Convenzione europea. In argomento, v. *Krupko and Others v. Russia*, no. 26587/07, 26 June 2014.

CAP. III

Il bilanciamento con la libertà di espressione e il diritto alla reputazione

1. *Von Hannover v. Germany*. – 2. *Axel Springer AG v. Germany*. – 3. *Mosley v. United Kingdom*. – *4. Nagla v. Latvia*.

1. Per quanto riguarda la tutela dell'immagine (come espressione dell'identità personale), com'è noto, l'art. 10 CEDU consente alla stampa di pubblicare fotografie di un personaggio pubblico pur in assenza del suo consenso. Nella sentenza *Von Hannover v. Germany*[175], concernente la pubblicazione su vari tabloid tedeschi di alcune fotografie della principessa Carolina di Monaco scattate abusivamente all'interno della sua residenza privata, la Corte ha avuto occasione di affrontare la questione del rapporto tra gli articoli 8 e 10 CEDU, assumendo una posizione assai critica nei confronti dell'informazione scandalistica e del fenomeno dei paparazzi. Secondo la Corte, i fattori di cui si discorre sono essenzialmente tre. In primo luogo, il grado di esposizione pubblica e mediatica dell'uomo politico o di governo (che dipende, a seconda dei casi, dalla natura delle funzioni pubbliche esercitate, dall'ampiezza del consenso elettorale, dalla posizione assunta nell'ambito di governo, nonché dalle stesse scelte mediatiche operate dall'interessato). In secondo luogo, lo specifico aspetto della nozione di "vita privata" che viene interessato dall'attività intrusiva dei mezzi di informazione (immagine, riservatezza, reputazione). In terzo luogo, l'effettiva presenza di un interesse generale alla conoscenza di aspetti relativi alla vita privata di un personaggio pubblico.

Dopo aver ribadito la necessità di contemperare la libertà di espressione (nella quale rientra la pubblicazione di fotografie) con il diritto al rispetto della vita privata, specie se l'acquisizione delle immagini abbia luogo "in un clima di continua molestia che induce nella persona interessata un sentimento molto forte di intrusione nella propria vita privata e persino di persecuzione", la Corte ha ritenuto necessario tracciare una distinzione fondamentale tra il diritto di cronaca su questioni di interesse generale che contribuisce al dibattito in una società democratica (ad esempio, l'operato degli uomini politici nell'esercizio delle loro funzioni) e la cronaca che riguarda dettagli della vita privata di un individuo che, per di più, non esercita funzioni ufficiali.

Malgrado i personaggi pubblici siano inevitabilmente esposti ad una maggiore attenzione da parte dei media, essi devono poter avere una "legittima aspettativa alla protezione ed al rispetto della loro vita privata", specie quando la pubblicazione delle loro fotografie e relativi commenti sia del tutto svincolata dall'esigenza di contribuire alla discussione su questioni di interesse generale, bensì soltanto rivolta a soddisfare la curiosità di una particolare categoria di lettori.

La Corte ha affermato il principio secondo cui nei confronti di un personaggio noto il pubblico non può vantare un interesse legittimo a conoscere i dettagli della sfera intima. In ogni caso, anche se tale interesse sussiste insieme a quello commerciale della stampa, la libertà di espressione deve cedere di fronte all'esigenza di protezione

[175] V. *Von Hannover v. Germany*, no. 59320/00, §§ 56-81, ECHR 2004-VI, su cui v. 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*, n. 4/2010, pp. 105-124.

della vita privata. Nella sentenza in parola, pertanto, l'operazione di bilanciamento fra il diritto della stampa alla pubblicazione delle immagini (che le giurisdizioni interne avevano ritenuto prevalente) e il diritto al rispetto della privacy, si è conclusa a favore di quest'ultimo.

Nella seconda sentenza *Von Hannover v. Germany*[176], la Corte invece non ha riscontrato violazione del diritto al rispetto della vita privata della ricorrente, alla quale era stato negato un provvedimento inibitorio contro la pubblicazione di una fotografia che la ritraeva in vacanza e di un articolo che riportava la malattia del Principe Ranieri. La Corte, in questo caso, ha ritenuto che i giudici nazionali avessero correttamente conciliato il diritto alla libertà di espressione con quello di privacy. Essi infatti avevano qualificato l'articolo sulla malattia come notizia circa un evento della società moderna e la relativa fotografia, considerata in quel contesto, aveva contribuito in qualche misura ad un dibattito d'interesse generale.

Nella giurisprudenza della Corte pertanto il criterio fondamentale per il bilanciamento degli interessi in gioco in questo settore è la presenza di un interesse pubblico generale preminente.

2. Nella sentenza *Axel Springer AG v. Germany*[177], la Corte ha considerato che il divieto imposto da un tribunale nazionale al responsabile di un giornale, che intendeva pubblicare un articolo sull'arresto e sulla condanna di un noto attore, costituisse una violazione dell'art. 10 CEDU.

Visto che i giudici nazionali avevano compresso il diritto alla libertà di espressione della società ricorrente, anche in questo caso la Corte è stata chiamata a determinare se tale ingerenza risultasse necessaria in una società democratica.

In base ai criteri per il bilanciamento del diritto alla libertà di espressione con quello al rispetto della vita privata fissati nella sua giurisprudenza precedente, la Corte ha osservato innanzitutto che gli articoli pubblicati riguardavano l'arresto e la condanna di un personaggio noto. I fatti giudiziari di norma sono considerati di interesse generale[178]. Poi, vista la sua notorietà, la persona interessata poteva essere

[176] *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, § 118 and § 124, ECHR 2012, su cui A. SACCUCCI, cit.

[177] *Axel Springer AG v. Germany* [GC], no. 39954/08, §§ 90 and 91, 7 February 2012.

[178] La società ricorrente era editrice di un giornale quotidiano nazionale a larga diffusione che aveva pubblicato un articolo in prima pagina sulla star di una popolare serie televisiva che era stato arrestato a Monaco, al Festival della birra, per possesso di cocaina. Il pezzo era accompagnato da un dettagliato articolo in un'altra pagina con tre fotografie dell'attore. Subito dopo la pubblicazione, l'attore aveva ottenuto un'ingiunzione per impedire ulteriori pubblicazioni dell'articolo o delle fotografie. Il divieto di pubblicazione dell'articolo fu confermato in appello (la società ricorrente non impugnò il divieto concernente la pubblicazione delle fotografie). Nel novembre 2005 l'ingiunzione continuò con riferimento a quasi tutto l'articolo e la società ricorrente fu condannata a pagare una sanzione minima. Nel frattempo, il giornale aveva pubblicato un secondo articolo, che riportava la condanna dell'attore per possesso illegale di droga in seguito alla confessione dello stesso. L'attore ricorse ed ottenne un'ingiunzione che limitava la pubblicazione del secondo articolo sostanzialmente

qualificata come figura pubblica. Inoltre, la circostanza che fosse stato arrestato in pubblico e che avesse confessato rilasciando numerose interviste implicava che la sua legittima aspettativa di protezione della privacy risultasse ridotta.

Per quanto riguarda le modalità di ottenimento dell'informazione e la sua affidabilità, il primo articolo sull'arresto dell'attore si basava su informazioni fornite dall'ufficio del procuratore. Secondo la Corte, il giornale ricorrente non aveva agito in mala fede. Infatti aveva ricevuto conferma dell'informazione dalle autorità procedenti e non c'era nulla che suggeriva che non avesse ricercato un bilanciamento tra l'interesse alla pubblicazione e il diritto al rispetto della sua vita privata. Tuttavia, alla luce di tutte le circostanze, i giornalisti avevano ritenuto che non vi fossero motivi per preservare l'anonimato dell'attore.

Inoltre gli articoli pubblicati non avevano rivelato dettagli circa la vita privata dell'attore, ma avevano riguardato soprattutto le circostanze del suo arresto e l'esito del processo penale. Negli articoli erano assenti commenti lesivi privi di fondamento. Il giornale ricorrente non aveva impugnato l'ingiunzione che vietava la pubblicazione delle foto e non era stato dimostrato che la pubblicazione degli articoli aveva determinato serie conseguenze per l'attore. Pertanto, sulla base di tutte queste osservazioni, la Corte ha ritenuto che le restrizioni imposte al giornale ricorrente non risultassero proporzionate rispetto allo scopo legittimo di protezione della vita privata dell'attore.

3. Nella sentenza *Mosley v. United Kingdom*[179], il caso riguardava la pubblicazione su un giornale di fotografie private del ricorrente. Vista l'impossibilità di richiedere un provvedimento inibitorio preventivo, a causa della mancanza di un obbligo di notifica preliminare, egli lamentava la violazione del diritto al rispetto della vita privata (art. 8 CEDU).

Secondo la Corte, sebbene la divulgazione di fotografie avesse generalmente finalità d'intrattenimento e non d'informazione, il caso rientrava indubbiamente nell'ambito di applicazione dell'art. 10 CEDU ("Libertà di espressione"), sul quale possono prevalere gli interessi giuridici tutelati dall'art. 8 CEDU nel caso in cui l'informazione sia di natura intima e privata e la divulgazione sia priva di un pubblico interesse. Tuttavia, particolare attenzione deve essere rivolta ai limiti alla pubblicazione che possono costituire una forma di censura. Alla luce dell'eventuale effetto dissuasivo che sorgerebbe in caso di obbligo di notifica preliminare, dei dubbi sulla sua efficacia e dell'ampio margine di apprezzamento in questo settore, la Corte ha escluso la presenza di un obbligo di notifica preliminare vincolante sulla base dell'art. 8.

---

sulla stessa base dei motivi della prima ingiunzione. La decisione fu confermata in appello. La società ricorrente fu alla fine condannata a pagare per le successive violazioni dell'ingiunzione.

[179] *Mosley v. the United Kingdom*, no. 48009/08, § §129 and 130, 10 May 2011.

4. La sentenza *Nagla v. Latvia*[180] riguardava una perquisizione, effettuata d'iniziativa dalla polizia e convalidata *ex post* da un giudice, sul *pc* (e relativi accessori) di una giornalista televisiva, allo scopo di sequestrare materiale digitale riconducibile ad un suo informatore, all'epoca dei fatti sottoposto a procedimento penale per l'accesso abusivo a sistemi informatici e per la diffusione illecita di dati elettronici. Vista l'interferenza con la libertà di ricevere e diffondere informazioni (art. 10 CEDU), la Corte ha ritenuto che, da una parte, la perquisizione fosse prescritta dalla legge e perseguisse uno scopo legittimo; ma che, dall'altra, non rispettasse il requisito della "necessità" in uno Stato democratico. Infatti, l'attività di ricerca della prova era stata attivata d'urgenza per pericolo che il materiale da sequestrare potesse venire distrutto, cancellato o danneggiato, malgrado fossero trascorsi mesi dall'ultimo contatto fra le due persone.

La Corte ha ribadito che il diritto di un giornalista a non svelare la fonte non è un privilegio da concedere o ritirare a seconda della liceità o meno della fonte medesima, bensì è un elemento essenziale della libertà di espressione che non deve essere compresso per non incorrere in violazione della CEDU (art. 10).

Secondo la Corte, i giudici nazionali avrebbero dovuto tener conto del fatto che la tutela delle fonti è un elemento essenziale della professione giornalistica e della libertà di espressione. Quest'ultimo infatti è un diritto doppio perché include il diritto della collettività a ricevere informazioni su questioni scottanti di interesse pubblico. Pertanto le perquisizioni della casa e della redazione della giornalista avevano rappresentato una grave compromissione del suo diritto alla libertà di espressione, ma anche quello di ogni individuo a ricevere informazioni. Infatti, sottolinea la Corte, la conoscenza degli stipendi dei dipendenti pubblici risulta un interesse pubblico della collettività, specie in tempo di crisi.

[180] *Nagla v. Latvia*, no. 73469/10, 16 July 2013. Una giornalista televisiva aveva trasmesso un servizio, basato su notizie acquisite da una fonte anonima, riguardo "falle" esistenti nel database dei salari e delle dichiarazioni dei redditi di funzionari e dipendenti pubblici. A seguito dell'apertura di un'inchiesta, la donna si era rifiutata di svelare la propria fonte. Di qui le perquisizioni nella sua abitazione, il sequestro di un laptop, di alcuni hard disk esterni, chiavette usb e altro. Le autorità inquirenti avevano infine raggiunto lo scopo, vale a dire l'individuazione della fonte giornalistica. Tuttavia, visto che i giudici nazionali avevano confermato l'obbligo di rivelare l'identità di colui che aveva svelato dati riservati e che pertanto aveva commesso un illecito, la giornalista si rivolgeva alla Corte per violazione dell'art. 10 CEDU.

Parte III
La giurisprudenza della Corte di giustizia

Cap. I
L'esercizio di poteri pubblici

1. – *Österreichischer Rundfunk*. – 2. *Huber*. – 3. *YS*.

1. La tutela della vita privata è stata posta dalla Corte di giustizia in relazione con altri interessi perseguiti dallo Stato. Una delle prime occasioni è costituita dalla sentenza *Österreichischer Rundfunk e al.*[181], in cui la tutela della vita privata è stata contrapposta all'esigenza dello Stato di verificare l'adeguatezza degli stipendi dei dipendenti di enti pubblici.

La pronuncia traeva origine dal rinvio pregiudiziale in merito all'obbligo gravante sugli enti pubblici di comunicare gli stipendi e le pensioni oltre un determinato livello dei loro dipendenti e pensionati, nonché il nome dei beneficiari.

Le questioni pregiudiziali poste alla Corte di giustizia riguardavano innanzitutto se una normativa che prevede l'obbligo di un ente pubblico di raccolta e trasmissione dei dati sui redditi dei propri dipendenti al fine della loro pubblicazione fosse compatibile con le norme di diritto dell'UE in materia di protezione dei dati personali. In caso di risposta positiva al quesito in parola, se le disposizioni dell'UE che si oppongono a tale normativa nazionale siano direttamente applicabili, nel senso che l'ente obbligato alla comunicazione può farle valere per impedire l'applicazione di norme nazionali con esse incompatibili e può pertanto non opporre ai dipendenti un obbligo imposto dalla legge nazionale.

Secondo l'avvocato generale Tizzano, l'attività di controllo finalizzata a garantire un'ampia informazione dei cittadini sugli stipendi percepiti nell'ambito degli enti pubblici austriaci era prevista e disciplinata con legge costituzionale, in base ad un'autonoma scelta politico–istituzionale e non sulla base di un obbligo dell'UE. Pertanto, ad avviso dell'avvocato generale, non formando oggetto di alcuna specifica disciplina dell'UE, tale attività non rientrava nella competenza dell'Unione.

Per quanto riguarda la prima questione pregiudiziale, i dati trattati costituivano dati personali ex art. 2, lett. a) della direttiva 95/46/CE, in quanto si trattava di informazioni concernenti persone fisiche identificate o identificabili. Secondo la direttiva, i dati devono essere rilevati per finalità determinate, esplicite e legittime. Il trattamento dei dati personali è lecito ove esso sia necessario per adempiere un obbligo legale al quale è soggetto il responsabile del trattamento, oppure ove sia necessario per l'esecuzione di un compito di interesse pubblico[182]. Gli Stati possono derogare alla normativa dell'UE ove sia necessario per la salvaguardia di un rilevante interesse economico o finanziario dello Stato o di un compito di controllo, ispezione, disciplina connesso all'esercizio di pubblici poteri di cui è investito il responsabile del trattamento cui vengono comunicati i dati. Le disposizioni della direttiva, inoltre, devono essere interpretate alla luce dei diritti fondamentali.

La Corte di giustizia ha richiamato l'art. 8 CEDU, che, pur enunciando un

[181] Sentenza della Corte di giustizia del 20 maggio 2003, *Österreichischer Rundfunk e al.*, cause riunite C-465/00, C-138/01 e C-139/01, in *Racc.*, p. I-4989.
[182] V. artt. 6, par. 1, lett. b), lett. c), art. 7 lett. c) e lett. e) della direttiva 95/46/CE.

principio di non ingerenza delle autorità pubbliche nell'esercizio del diritto alla vita privata, ammette tale ingerenza nei casi in cui sia prevista dalla legge e costituisca un provvedimento che, in una società democratica, è necessario alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione delle infrazioni penali, alla tutela della salute e della morale, alla tutela dei diritti e delle libertà altrui. La Corte ha pertanto esaminato se la normativa nazionale in discussione prevedesse un'ingerenza nella vita privata e se tale ingerenza risultasse giustificata alla luce dell'art. 8 CEDU per valutare l'applicazione della direttiva, in particolare degli articoli 6, 7, 13. Proprio come avrebbe fatto la Corte di Strasburgo, la Corte di giustizia ha proceduto a valutare la sussistenza di un'ingerenza nella vita privata.

Secondo la Corte, la semplice registrazione dei dati non può costituire un'ingerenza nella vita privata; la comunicazione ad un terzo è suscettibile, invece, di arrecare un vero e proprio pregiudizio (ex art. 8 CEDU), a prescindere dall'ulteriore utilizzo.

Come avrebbe fatto la Corte di Strasburgo, la Corte di giustizia ha esaminato se tale ingerenza potesse ritenersi giustificata. Secondo la Corte tale ingerenza era specificamente prevista dal "BezBegrBVG" (vale a dire dalla legge costituzionale federale relativa alla limitazione degli stipendi dei funzionari pubblici). Tuttavia, occorreva verificare se tale norma fosse stata redatta in modo sufficientemente preciso per consentire ai destinatari della legge di regolare la loro condotta, in conformità con il requisito di prevedibilità sancito dalla giurisprudenza della CEDU. La Corte ha inteso dunque utilizzare il medesimo standard di Strasburgo e ha citato, infatti, la giurisprudenza in parola[183]. La Corte, tuttavia, ha lasciato l'ultima parola al giudice nazionale (par. 79), dichiarando che spettava ai giudici del rinvio verificare se la normativa nazionale sulla divulgazione del nome delle persone interessate in relazione ai redditi percepiti soddisfacesse il requisito di prevedibilità.

La Corte tuttavia ha ritenuto che tale valutazione dovesse essere fatta solo dopo aver verificato il rispetto del principio di proporzionalità in relazione agli obiettivi perseguiti. Tale esame è stato, pertanto, condotto direttamente dalla Corte di giustizia. Inoltre quest'ultima ha dovuto verificare se l'ingerenza rispettasse il requisito della "necessità" in una società democratica. Anche in questo caso la Corte di giustizia ha adottato lo standard di Strasburgo e ha ricordato che cosa si intende per "necessario" ai sensi della giurisprudenza della CEDU, vale a dire un bisogno sociale imperioso e che la misura adottata sia proporzionata alla finalità legittima perseguita. La Corte ha ricordato, infine, che le autorità nazionali dispongono in proposito di un margine discrezionale la cui portata dipende non solo dalla finalità, ma altresì dal carattere proprio dell'ingerenza.

Secondo la Corte, occorre bilanciare l'interesse dello Stato a garantire un

[183] *Rekvényi v. Hungary* [GC], no. 25390/94, ECHR 1999-III.

impiego ottimale delle finanze pubbliche ed in particolare il mantenimento degli stipendi entro limiti ragionevoli con la gravità del pregiudizio arrecato al diritto delle persone interessate al rispetto della loro vita privata. A ciò si aggiunge anche il diritto del contribuente di essere informato sull'impiego delle finanze pubbliche, specie in materia di spese per il personale. La Corte ha concluso, pertanto, che l'ingerenza derivante dall'applicazione di una normativa nazionale come quella in oggetto potesse essere giustificata (ex art. 8, par. 2 CEDU) solo nei limiti in cui la divulgazione dei redditi annui e dei beneficiari risultasse necessaria e proporzionata rispetto all'obiettivo di mantenere gli stipendi entro limiti ragionevoli. La verifica di ciò spettava al giudice nazionale. La Corte ha, dunque, lasciato la verifica finale al giudice nazionale, secondo lo spirito di collaborazione proprio del rinvio pregiudiziale.

Per quanto riguarda la seconda questione pregiudiziale, la Corte di giustizia ha ritenuto che le disposizioni della direttiva, ostative alla normativa nazionale ritenuta ingiustificata, sono direttamente applicabili, in quanto sufficientemente chiare e precise per poter essere fatte valere da un singolo ed applicate dai giudici nazionali.

In definitiva, nel bilanciare l'esigenza di pubblico controllo degli stipendi e la tutela dei dati personali, la Corte non ha esplicitamente conferito una prevalenza all'uno o all'altro e costruito una gerarchia, ma ha ricercato un giusto equilibrio sulla base del principio di proporzionalità. Degno di nota è che la Corte ha tenuto come costante parametro di riferimento il sistema della CEDU e la giurisprudenza di Strasburgo, dettando dei criteri di giudizio per il giudice nazionale, ma lasciando a quest'ultimo la decisione nel caso concreto. Mediante quest'opera di bilanciamento si rende, dunque, manifesto il dialogo tra giudici nell'ordinamento dell'Unione europea, nonché il coordinamento dei diversi livelli di tutela dei diritti fondamentali.

2. Com'è noto, i dati personali possono essere trattati lecitamente se "è necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito" il titolare del trattamento "o il terzo a cui vengono comunicati i dati […]"[184].

Nella causa *Huber c. Bundesrepublik Deutschland*[185], il sig. Huber, cittadino austriaco residente in Germania, chiedeva all'Ufficio federale per l'immigrazione e i rifugiati di cancellare i dati che lo riguardavano dal registro centrale degli stranieri (denominato "AZR"). Tale registro, contenente i dati personali relativi ai cittadini dell'UE che non hanno la cittadinanza tedesca e che risiedono in Germania da oltre tre mesi, è utilizzato per finalità statistiche nonché dalle forze dell'ordine e dalle autorità giudiziarie nell'ambito d'indagini e operazioni relative ad attività criminali

[184] V. art. 7, lett. e) della direttiva 95/46/CE sulla protezione dei dati personali, cit.

[185] Sentenza della Corte di giustizia del 16 dicembre 2008, *Huber c. Bundesrepublik Deutschland*, causa C-524/06, in *Racc*., p. I-09705.

o pregiudizievoli per la pubblica sicurezza. Il giudice del rinvio chiedeva alla Corte se il trattamento dei dati personali nell'ambito del registro centrale degli stranieri, a cui anche altre autorità pubbliche avevano accesso, risultasse compatibile con il diritto dell'UE (principio di non discriminazione, art. 18 TFUE), vista l'assenza di un registro simile per i cittadini tedeschi.

A tale riguardo, l'avvocato generale Poiares Maduro individuava tre aspetti di disparità di trattamento. In primo luogo, i dati personali dei cittadini stranieri erano conservati non solo nei registri comunali (come quelli dei cittadini nazionali), ma anche nel registro centrale degli stranieri; in secondo luogo, il registro centrale conteneva un maggior numero di informazioni rispetto ai registri comunali; in terzo luogo la possibilità di rapida consultazione dei dati relativi agli stranieri, mentre ciò risultava impossibile per quelli relativi ai cittadini. Secondo il giudice, gli aspetti in parola andavano esaminati alla luce del divieto di discriminazione e in base alla direttiva 2004/387CE[186] in tema di diritto di soggiorno. Egli ha ritenuto che l'ufficio dell'immigrazione tedesco trattasse dati ulteriori rispetto a quanto richiesto da quest'ultima direttiva e che pertanto non potesse trovarvi giustificazione. Allo stesso modo, il trattamento centralizzato dei dati relativi agli stranieri non sarebbe risultato giustificato, a meno di dimostrare l'assenza di altre e più efficienti modalità di attuazione delle norme in materia di immigrazione e soggiorno. Secondo l'avvocato generale era compito del giudice nazionale valutare tali circostanze.

Per quanto riguarda l'applicazione della direttiva 95/46/CE, l'avvocato generale ha verificato se il trattamento centralizzato dei dati degli stranieri potesse essere considerato come "necessario" alla luce dell'art. 7 della direttiva in parola. Egli ha ricostruito il concetto di "necessità" che "ha una lunga storia nel diritto comunitario e costituisce un elemento consolidato del criterio di proporzionalità. Esso comporta che l'autorità che adotta una misura interferente con un diritto tutelato dall'ordinamento dell'Unione europea per conseguire uno scopo legittimo deve dimostrare che essa rappresenta la misura meno restrittiva per raggiungere tale scopo. Inoltre, se il trattamento dei dati personali può ledere il diritto fondamentale alla vita privata e familiare assume rilevanza anche l'art. 8 CEDU […]". L'avvocato generale ha sottolineato il parallelismo tra il livello di tutela della CEDU e quello della direttiva comunitaria, ricordando che la Corte, nella precedente sentenza *Österreichischer Rundfunk* ha statuito che "se una misura nazionale è incompatibile con l'art. 8 CEDU, non può essere compatibile neppure con l'art. 7, lett. e), della direttiva 95/46/CE . [...] La Corte europea dei diritti dell'uomo ha dichiarato che l'aggettivo "necessaria" implica che esista per lo Stato "una pressante esigenza sociale" di agire in un determinato modo e che la misura adottata sia proporzionata

[186] 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.

al legittimo scopo perseguito".

La Corte di giustizia ha ritenuto in primo luogo che, ai sensi della direttiva, i dati personali possano essere trattati lecitamente solo se è necessario per l'esecuzione di un compito d'interesse pubblico o connesso all'esercizio di pubblici poteri. Pertanto "considerato l'obiettivo di garantire un livello di tutela equivalente in tutti gli Stati membri, la nozione di necessità come risultante dall'art. 7, lett. e), della direttiva 95/46/CE […] non può avere un contenuto variabile in funzione degli Stati membri. Si tratta quindi di una nozione autonoma del diritto comunitario che deve essere interpretata in maniera tale da rispondere pienamente alla finalità di tale direttiva come definita dal suo art. 1, n. 1"[187].

La Corte ha sottolineato che il diritto alla libera circolazione di un cittadino dell'Unione nel territorio di uno Stato membro di cui questi non ha la nazionalità non è incondizionato, ma può essere subordinato alle limitazioni e alle condizioni previste dal trattato nonché dalle relative disposizioni di attuazione. Pertanto se, in linea di principio, risultava legittimo che uno Stato membro disponesse di un registro centralizzato quale ausilio per l'applicazione della normativa in materia di soggiorno, il registro in parola non poteva contenere informazioni diverse da quelle a tal fine necessarie. La Corte ha concluso che il sistema in parola sarebbe risultato conforme al diritto dell'Unione se avesse contenuto unicamente i dati necessari per l'applicazione di detta normativa e se il carattere centralizzato avesse consentito un'applicazione più efficiente della normativa medesima. Il giudice nazionale avrebbe dovuto accertare se dette condizioni risultassero soddisfatte nel caso di specie. Diversamente, la conservazione e il trattamento dei dati personali in un registro come l'AZR per finalità statistiche non avrebbero potuto essere considerati come necessari ai sensi dell'art. 7, lett. e), della direttiva 95/46/CE[188].

Infine, per quanto riguarda la questione dell'utilizzo dei dati contenuti nel registro per finalità di lotta alla criminalità, la Corte ha ritenuto che l'obiettivo in parola riguardasse "necessariamente la repressione dei reati commessi, a prescindere dalla cittadinanza dei loro autori". Visto che tale registro non conteneva dati personali relativi ai cittadini dello Stato membro interessato, questa differenza di trattamento costituiva una discriminazione vietata dall'art. 18 del TFUE. Pertanto, tale disposizione, come interpretata dalla Corte, "osta all'istituzione da parte di uno Stato membro, per finalità di lotta alla criminalità, di un sistema di trattamento di dati personali riguardante specificamente i cittadini dell'Unione non aventi la nazionalità di tale Stato membro"[189].

La Corte di giustizia ha condiviso le conclusioni dell'avvocato generale, anche se ha sviluppato il suo ragionamento in maniera diversa. L'analisi è partita innanzitutto

[187] V. sentenza *Huber c. Bundesrepublik Deutschland*, cit., par. 52.
[188] *Ivi*, paragrafi 54, 58, 59 e 66-68.
[189] *Ivi*, paragrafi 78 e 81.

dalla delimitazione dell'ambito di applicazione della direttiva 95/46/CE. Infatti, visto che l'art. 3, par. 2 ne esclude l'applicabilità in caso di trattamento dei dati connesso alla lotta alla criminalità, essa può essere utilizzata come parametro di legittimità soltanto in relazione ad attività relative all'applicazione della normativa di soggiorno e con finalità statistiche. La Corte ha esaminato la necessità di un tale trattamento dei dati in relazione alla finalità di applicazione della normativa in materia di soggiorno. Essa, anche alla luce della direttiva 2004/38 , ha ritenuto che in linea di principio si può considerare necessario che uno Stato membro disponga delle informazioni e dei documenti pertinenti per verificare l'esistenza di un diritto di soggiorno di un cittadino di un altro Stato membro nel suo territorio e dunque la tenuta di un registro centrale risulta compatibile con il divieto di discriminazione fondato sulla nazionalità contenuto nell'art. 18 TFUE.

La Corte ha rilevato, tuttavia, che il registro in parola non potesse contenere informazioni diverse da quelle richieste dalla direttiva e che dovesse essere utilizzato solo dalle autorità incaricate di applicare la normativa sul diritto di soggiorno. Infine, il trattamento centralizzato e non solo locale poteva essere ritenuto necessario soltanto se utile ad un'applicazione più efficace della normativa relativa al diritto di soggiorno. Pertanto la Corte ha ritenuto che l'esigenza di applicare efficacemente tale normativa potesse costituire una giustificazione del trattamento dei dati, con prevalenza di tale interesse dello Stato rispetto alla tutela della riservatezza dei soggetti coinvolti. Essa ha rinviato al giudice nazionale per l'accertamento di una tale circostanza.

Per quanto riguarda invece il trattamento dei dati per fini statistici, la conclusione della Corte è stata diversa. Infatti, ha ritenuto che non si potesse considerare necessario un registro come quello del caso di specie, in quanto sarebbe stato sufficiente un trattamento di informazioni anonime. In questo caso, dunque, la Corte ha riconosciuto un'ingerenza eccessiva da parte dello Stato nella vita personale dei cittadini di altri Stati membri.

La Corte ha proceduto, infine, alla verifica della legittimità del trattamento dei dati personali relativi ai cittadini di altri Stati dell'Unione per fini di lotta alla criminalità. Visto che tale ambito esulava dall'applicazione della direttiva 95/46/CE, il parametro di riferimento era costituito dall'art. 18 TFUE. Sebbene la finalità perseguita risultasse legittima, la Corte ha ritenuto che non fosse sufficiente a giustificare un trattamento sistematico dei dati degli stranieri e risultasse discriminatoria.

Nel caso in parola è importante sottolineare che la Corte ha scelto di condividere il medesimo livello di tutela del Consiglio d'Europa per la tutela della vita privata in relazione al trattamento dei dati personali. Il bilanciamento con le altre esigenze statali (vale a dire l'efficace applicazione della normativa in materia di soggiorno e immigrazione; l'elaborazione di dati statistici; la lotta alla criminalità) è stato

condotto in relazione alle norme dell'UE di volta in volta rilevanti. Anche in questo caso la Corte ha mostrato grande cooperazione con il giudice nazionale, cui ha rinviato l'accertamento in concreto della necessità di una tale normativa. Infatti la Corte ha ritenuto che egli disponesse di maggiori elementi per valutare l'assenza di strumenti meno invasivi per assicurare le finalità legittime perseguite dallo Stato.

3. Nella sentenza *YS*[190], la questione sottoposta alla Corte prendeva le mosse dal rifiuto del Ministero dell'immigrazione olandese di trasmettere al ricorrente un documento amministrativo che costituiva un mero atto preventivo all'adozione della decisione finale sul permesso di soggiorno. Tale documento era definito quale semplice minuta contenente un'analisi giuridica solo eventualmente ripresa nella motivazione del provvedimento finale[191].

Il giudice del rinvio chiedeva, in particolare, se l'analisi giuridica della minuta, oltre ai dati personali in essa contenuti, si potesse qualificare come "dato personale" ex direttiva 95/46/CE e se il rispetto dei legittimi interessi della riservatezza del processo decisionale consentisse alle autorità competenti un diniego del diritto di accesso al documento in parola.

Secondo la Corte, non vi erano dubbi in merito al fatto che i dati relativi al richiedente che costituivano informazioni concernenti la persona fisica dovessero qualificarsi come dati personali e quindi essere comunicati a richiesta e trattati come previsto dalla direttiva 95/46/CE. Tuttavia, l'analisi giuridica contenuta nella minuta, pur potendo comprenderne alcuni, non costituiva di per sé un "dato personale"; infatti tale analisi "costituisce non già un'informazione riguardante il richiedente (…), ma tutt'al più (...) un'informazione riguardante la valutazione e l'applicazione, da parte dell'autorità competente di tale diritto"[192] alla situazione del richiedente, con la conseguente impossibilità, della persona interessata, di assicurarsi circa la sua esattezza.

---

[190] V. sentenza del 17 luglio 2014, *Y.S. c. Minister voor Immigratie, Integratie en Asiel*, cause riunite C 141/12 e C 372/12, non ancora pubblicata in *Racc*. Le domande erano state presentate nell'ambito di due controversie che contrapponevano, da un lato, un cittadino di un Paese terzo (che aveva presentato domanda di permesso di soggiorno temporaneo nei Paesi Bassi) e il Ministero dell'Immigrazione; dall'altro, altri cittadini di Paesi terzi che avevano presentato un'identica domanda, in merito al rifiuto da parte del medesimo Ministero di trasmettere loro la copia di un documento amministrativo redatto preventivamente all'adozione delle decisioni riguardanti le loro domande di permesso di soggiorno.

[191] Di norma, la minuta contiene, tra l'altro, le seguenti informazioni: dati relativi al richiedente quali nome, data di nascita, cittadinanza, sesso, etnia, religione e lingua; dati relativi all'iter del procedimento; elementi relativi alle dichiarazioni rese e ai documenti prodotti dal richiedente; disposizioni giuridiche applicabili e, infine, una valutazione dei summenzionati elementi alla luce delle disposizioni giuridiche applicabili. La minuta fa parte del processo preparatorio interno, ma non della decisione finale, sebbene determinate considerazioni che vi figurano possano essere riprese nella motivazione di tale decisione.

[192] *Ivi*, par. 40.

Cap. II
Le autorità indipendenti di controllo sui dati

1. *Commissione c. Germania*. – 2. *Commissione c. Austria*. – 3. *Commissione c. Ungheria*

1. La sentenza *Commissione c. Germania*[193] è la prima delle due pronunce della Corte di giustizia che riguardano l'indipendenza delle autorità nazionali di controllo della protezione dei dati personali. Infatti, l'art. 8 della Carta dei diritti fondamentali dell'Unione europea prevede che il rispetto delle regole in materia sia "soggetto al controllo di un'autorità indipendente".

Secondo la Corte, nel caso di specie, lo Stato membro ha violato gli obblighi dell'UE[194], in quanto ha sottoposto le autorità di controllo per il trattamento dei dati personali ad una vigilanza da parte dello Stato (in particolare dai Länder), venendo meno così al principio secondo cui le autorità di controllo della protezione dei dati devono essere "pienamente indipendenti". La direttiva infatti ha previsto che le autorità di controllo non debbano essere influenzate da altre autorità statali o da altri enti esterni all'apparato statale, garantendo così l'assenza di qualsiasi influenza esterna sulle decisioni. Il termine "pienamente" indipendente implica che l'indipendenza deve sussistere rispetto a qualsiasi soggetto e sotto qualsiasi profilo. Pertanto, sarebbe incompatibile con la misura dell'UE assoggettare le autorità competenti per il controllo sul trattamento dei dati in settori diversi da quello pubblico ad un controllo di fatto, di diritto o di servizio da parte dello Stato. Poiché la normativa di ciascuno dei Länder assoggetta invece le autorità di controllo a diverse combinazioni di questi tre tipi di controllo, ciò determina una violazione dell'obbligo di garantire che le autorità di controllo siano "pienamente indipendenti".

Sotto il profilo teleologico, il legislatore dell'UE ha considerato essenziale la piena indipendenza, grazie alla quale la funzione delle autorità di controllo di cui all'art. 28 della direttiva può essere efficacemente espletata. La nozione di "pienamente indipendente" è ulteriormente chiarita dal contesto in cui la norma è stata adottata. Anche sotto il profilo sistematico, il requisito secondo cui le autorità di controllo degli Stati membri devono essere "pienamente indipendenti" è coerente con la normativa esistente nell'UE nel settore della tutela dei dati.

La tesi sostenuta dalla Germania di un'indipendenza relativa, cioè di un'indipendenza delle autorità di controllo solo dagli stessi controllati, secondo la Corte non si concilia con la formulazione chiara ed esaustiva della direttiva, che esige al contrario un'indipendenza assoluta. Inoltre, la previsione del secondo comma dell'art. 28, n. 1, sarebbe svuotata di qualsiasi contenuto. La Corte respinge altresì l'argomentazione secondo cui l'art. 95 CE, in quanto fondamento normativo della direttiva ed i principi di sussidiarietà e di proporzionalità suggeriscano un'interpretazione restrittiva del requisito della piena indipendenza.

Secondo la Corte, è vietata un'interpretazione restrittiva delle disposizioni della

[193] Sentenza del 9 marzo 2010, *Commissione europea c. Repubblica federale di Germania*, causa C-518/07, in *Racc.*, p. I-01885.
[194] V. art. 28, n. 1, secondo comma, della direttiva 95/46/CE.

direttiva 95/46/CE in fattispecie a carattere non economico. La garanzia dell'indipendenza delle autorità nazionali di vigilanza richiesta dalla direttiva in parola, volta a garantire l'efficacia del rispetto delle disposizioni relative alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, deve essere interpretata al fine del conseguimento di tale obbiettivo. Non è possibile alla luce di quanto previsto dalla direttiva attribuire uno status particolare alle autorità di controllo ed ai loro agenti. Pertanto le autorità in parola devono agire nel massimo rispetto del requisito dell'imparzialità.

La Corte ha affermato che l'indipendenza prevista dalla disposizione della direttiva esclude non solo qualsiasi influenza esercitata dagli organismi controllati, ma anche qualsiasi imposizione e ogni altra influenza esterna, diretta o indiretta, che possa rimettere in discussione lo svolgimento, da parte delle suddette autorità, del loro compito, consistente nello stabilire un giusto equilibrio fra la protezione del diritto alla vita privata e la libera circolazione dei dati personali. Pertanto, il concetto di indipendenza, in base a quanto affermato dal giudice dell'Unione, risulterebbe minato se le autorità di vigilanza influenzassero politicamente le decisioni delle autorità di controllo. Le autorità di controllo sono custodi del diritto al rispetto della vita privata e le loro decisioni non possono essere sospettate di parzialità. In conclusione, la vigilanza esercita dai Länder non risultava compatibile con le disposizioni della direttiva e con l'interpretazione della stessa fornita dalla Corte di giustizia.

2. Anche nella sentenza *Commissione c. Austria*[195], la Corte di giustizia ha riconosciuto l'inadempienza dello Stato membro relativamente all'istituzione di un'autorità di controllo indipendente per la tutela dei dati personali (ex art. 28, par. 1, della direttiva 95/46/CE).

La Commissione europea e il Garante europeo per la protezione dei dati si esprimevano in modo negativo sulla piena indipendenza nell'esercizio delle sue funzioni della *Commissione per la protezione dei dati austriaca.* In particolare, la Commissione sottolineava il collegamento in termini organizzativi con la Cancelleria federale che esercita una supervisione di servizio su tutti i collaboratori. Inoltre la direzione della Commissione spettava ad un funzionario amministrativo della cancelleria federale ed anche gli atti di ordinaria amministrazione erano gestiti da un funzionario federale. Il collegamento funzionale tra la Commissione per la tutela dei dati e la Cancelleria federale pertanto era fonte di manifesti conflitti di interesse e di dovere di lealtà. La Commissione sottolineava che il cancelliere federale vantava in definitiva un diritto di supervisione e di impartire istruzioni. Pertanto sussisteva un alto rischio di abuso finalizzato all'esercizio di un influenza

[195] Sentenza del 16 ottobre 2012, *Commissione europea c. Repubblica d'Austria*, causa C-614/10, non ancora in *Racc*.

politica.

Al contrario, l'Austria sosteneva che la *Commissione per la protezione dei dati* fosse "un'autorità collegiale con funzioni giurisdizionali" in base alla legge costituzionale federale e che costituisse pertanto un giudice indipendente (ex art. 267 TFUE e art. 6 CEDU).

La Corte di giustizia ha ribadito che l'istituzione di un'autorità di controllo indipendente negli Stati membri costituisce un elemento essenziale del rispetto della tutela delle persone con riguardo al trattamento dei dati personali. In base all'art. 28 e alle finalità generali della direttiva 95/46/CE, la Corte ha fornito un'interpretazione autonoma ed estensiva dell'espressione "in piena indipendenza". Le autorità di controllo infatti 2devono godere di un'indipendenza che consenta loro di svolgere le proprie funzioni senza influenze esterne. Tale indipendenza esclude non solo qualsiasi influenza esercitata dagli organismi controllati, ma anche qualsivoglia imposizione e ogni altra influenza esterna, diretta o indiretta, che possa rimettere in discussione lo svolgimento, da parte delle menzionate autorità, del loro compito, consistente nello stabilire un giusto equilibrio fra la protezione del diritto alla vita privata e la libera circolazione dei dati personali"[196]. La Corte distingue l'indipendenza delle autorità di controllo rispetto a quella degli organi giurisdizionali (ai sensi dell'art. 267 TFUE). Dal concetto di indipendenza deve essere esclusa anche ogni forma di influenza indiretta che possa orientare le decisioni dell'autorità di controllo.

In conclusione, ai sensi dell'interpretazione fornita dalla Corte, la Commissione austriaca così come strutturata non è stata ritenuta soddisfare i requisiti di indipendenza derivanti dalla normativa dell'Unione.

3. La sentenza *Commissione c. Ungheria*[197] ha riconosciuto la violazione del diritto dell'Unione da parte dello Stato membro convenuto che ha posto fine al mandato del commissario incaricato della protezione dei dati personali anticipatamente. Infatti, l'indipendenza delle autorità responsabili della protezione dei dati personali obbliga gli Stati membri a rispettare la durata del mandato ad esse conferito[198].

Ritenendo che la cessazione anticipata del mandato del commissario costituisse una violazione della direttiva (la quale impone il rispetto dell'indipendenza delle

[196] *Ivi*, par. 41.

[197] V. sentenza del 6 novembre 2012, *Commissione c. Ungheria*, causa C-286/12, non ancora in *Racc*.

[198] Fino al 2012, in Ungheria le funzioni di controllo sul trattamento dei dati personali erano esercitate da un commissario *ad hoc*. Nel 2008, era avvenuta la nomina di un nuovo commissario per la protezione dei dati per una durata di sei anni. Tuttavia, con effetto dal 1° gennaio 2012, il Parlamento aveva deciso di riformare il sistema di protezione dei dati e di istituire un'autorità nazionale incaricata della protezione dei dati e della libertà di informazione in sostituzione della funzione di commissario. Il commissario in carica aveva dovuto lasciare prima della scadenza e cedere il posto ad un altro, nominato presidente della nuova autorità per nove anni.

autorità incaricate del controllo), la Commissione proponeva un ricorso per inadempimento nei confronti dell'Ungheria dinanzi alla Corte di giustizia. Il Garante europeo della protezione dei dati interveniva nel procedimento a sostegno della Commissione.

Nella sentenza in parola, la Corte ha ricordato che le autorità di controllo istituite conformemente alla direttiva devono poter svolgere le proprie funzioni senza subire influenze esterne. Tale requisito implica, da un lato, che esse non siano vincolate da alcuna istruzione nell'esercizio delle loro funzioni e, dall'altro, che le loro decisioni siano adottate senza alcuna influenza politica, dovendo evitarsi anche solo il rischio di una tale influenza. Nel caso di specie, consentire a uno Stato membro di porre fine al mandato di un'autorità di controllo prima della sua scadenza, senza rispettare le norme e le garanzie prestabilite a tal fine dalla legislazione applicabile, avrebbe potuto indurre tale autorità a subire una forma di obbedienza al potere politico. Pertanto, l'indipendenza dell'autorità di controllo comprende necessariamente l'obbligo di rispettare la durata del mandato.

L'interpretazione della Corte risultava peraltro avvalorata dalle norme sulla cessazione del mandato del Garante europeo della protezione dei dati. Il mandato del Garante può, infatti, cessare anticipatamente solo per motivi gravi e oggettivamente verificabili. A tale proposito, la Corte osserva che la normativa ungherese in precedenza prevedeva anch'essa motivi di tale tenore per giustificare una cessazione anticipata del mandato del commissario per la protezione dei dati.

In tali condizioni, la Corte ha dichiarato che, ponendo anticipatamente fine al mandato dell'autorità di controllo della protezione dei dati personali, l'Ungheria era venuta meno agli obblighi cui era tenuta in forza della direttiva.

Cap. III
Accesso agli atti

– 1. *Volker und Markus Schecke*. – 2. *Commissione c. Bavarian Lager*.

1. La sentenza *Volker und Markus Schecke*[199] riguardava l'accesso agli atti relativi ai fondi strutturali. Gli Stati membri, in base al diritto dell'UE relativo al finanziamento delle spese della PAC (politica agricola comune), sono tenuti alla pubblicazione annuale a posteriori dei nominativi dei beneficiari del FEAGA (fondo europeo agricolo di garanzia) e del FEASR (fondo europeo agricolo per lo sviluppo rurale) nonché degli importi ricevuti da ciascun beneficiario per ciascuno di tali fondi. L'agenzia federale tedesca per l'agricoltura e l'alimentazione disponeva di un sito internet dotato di motore di ricerca attraverso il quale era possibile estrarre l'elenco dei beneficiari dei fondi. Successivamente alcuni dei beneficiari in parola ricorrevano al tribunale amministrativo per inibire la pubblicazione dei loro dati personali la quale, secondo i ricorrenti, violava la normativa dell'UE in materia di protezione dei dati. Il Tribunale amministrativo rinviava la questione alla Corte di giustizia.

La richiesta in esame poneva il problema della ponderazione fra l'interesse pubblico alla gestione trasparente dei fondi strutturali e l'interesse alla protezione dei dati personali e della vita privata. Secondo la Corte, l'obiettivo della trasparenza va bilanciato con la tutela dei diritti fondamentali derivante dagli artt. 7 e 8 della Carta dei diritti fondamentali dell'UE e le deroghe alla protezione della vita privata e dei dati personali devono essere assolutamente necessarie in una società democratica e rispettare il principio di proporzionalità.

Secondo la Corte, il contemperamento equilibrato dei diversi interessi in gioco presuppone, prima dell'adozione di determinate misure, la verifica della "necessità" per la realizzazione dell'interesse legittimo perseguito dalle stesse. Nella sentenza in esame, la Corte ha affermato riguardo alle persone fisiche beneficiarie dei fondi, che non vi fosse stato un adeguato bilanciamento fra l'interesse generale dell'Unione di garanzia della trasparenza e corretta gestione delle finanze pubbliche con l'interesse privato alla protezione dei dati personali. L'assenza di criteri precisi riguardanti la frequenza, il tipo, l'entità e i periodi di percezione degli aiuti da parte delle persone fisiche beneficiarie oltrepassava i limiti imposti dal principio di proporzionalità. La Corte in questo caso ha stabilito che l'obiettivo della trasparenza non potesse prevalere sul diritto fondamentale alla tutela dei dati personali e della vita privata.

Al contrario, per le persone giuridiche beneficiarie degli aiuti del FEAGA e del FEASR, l'obbligo di pubblicazione risultava conforme al principio di proporzionalità. A tal proposito, la Corte ha stabilito che il grado di gravità della violazione del diritto alla protezione dei dati personali varia a seconda che si tratti di persone fisiche o di persone giuridiche. Infatti le persone giuridiche sono già soggette ad un obbligo più gravoso di pubblicazione dei dati che le riguardano. Le autorità nazionali competenti non possono verificare prima della pubblicazione se la

[199] V. sentenza del 9 novembre 2010, *Volker und Markus Schecke GbR e Hartmut Eifert c. Land Hessen*, cause riunite C-92/09 e C-93/09, in *Racc.*, p. I-11063.

denominazione di ogni persona giuridica beneficiaria di stanziamenti del FEAGA e del FEASR riguardi persone fisiche. Tale tipo di verifica costituirebbe un onere amministrativo eccessivo. Pertanto la Corte ha riconosciuto che normativa dell'Unione in riferimento alle persone giuridiche bilancia opportunamente i diversi interessi coinvolti.

2. Nella sentenza *Commissione c. Bavarian Lager*[200], la Corte ha esaminato il rapporto tra i regolamenti 1049/2001/CE[201] e 45/2001/CE[202].

Com'è noto, il regolamento 1049/2011/CE sancisce come regola generale l'accesso del pubblico ai documenti delle istituzioni, ma sono ammesse delle limitazioni, in conformità con il diritto dell'UE relativo alla protezione dei dati personali, qualora la tutela della vita privata e l'integrità dell'individuo venissero compromesse. Un possibile pregiudizio alla vita privata e all'integrità dell'individuo deve essere sempre analizzato e valutato conformemente con la legislazione comunitaria, specificamente con il regolamento 45/2001/CE.

L'art. 1, n. 1, del regolamento in parola assicura infatti la tutela dei diritti e delle libertà fondamentali delle persone fisiche, in particolare il diritto alla vita privata in riferimento al trattamento di dati personali, ma non permette di distinguere i casi di trattamento di dati in due categorie: una categoria nella quale il trattamento sia analizzato esclusivamente in base all'art. 8 della CEDU e un'altra categoria in cui tale trattamento risulti soggetto alle disposizioni del regolamento 45/2001/CE.

La Corte afferma che con il regolamento in parola è stato istituito da parte del legislatore dell'Unione un sistema di protezione completo il quale assicura all'interno degli Stati membri un'applicazione coerente ed omogenea della disciplina riguardante la protezione delle libertà e dei diritti fondamentali delle persone fisiche in riferimento al trattamento dei dati personali.

I diritti attribuiti alle persone, i cui dati sono oggetto di trattamento, costituiscono regole di tutela delle libertà e dei diritti fondamentali. Infatti il diritto dell'Unione relativo alla protezione dei dati personali è finalizzato alla tutela delle libertà e dei diritti fondamentali. Le disposizioni del regolamento in esame sono vincolanti e si applicano "ad ogni trattamento di dati personali effettuato da tutte le istituzioni e gli organismi comunitari" e "in qualsiasi circostanza".

In tale contesto qualora una domanda fondata sul regolamento 1049/2001/CE sia diretta a ottenere l'accesso a documenti che contengono dati personali, sono

[200] Sentenza del 29 giugno 2010, *Commissione europea c. Bavarian Lager Co. Ltd*, causa C-28/08 P, in *Racc.*, p. I-06055.

[201] Regolamento (CE) n. 1049/2001 del Parlamento europeo e del Consiglio, del 30 maggio 2001, relativo all'accesso del pubblico ai documenti del Parlamento europeo, del Consiglio e della Commissione, in *GUCE* L 145 del 31 maggio 2001, p. 43.

[202] Regolamento (CE) n. 45/2001 del Parlamento europeo e del Consiglio del 18 dicembre 2000 concernente la tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni e degli organismi comunitari, nonché la libera circolazione di tali dati, cit.

integralmente applicabili le disposizioni del regolamento 45/2001/CE. Nel caso di specie, il mancato rinvio, da parte del Tribunale in prima battuta, alla normativa dell'Unione con l'applicazione esclusivamente delle deroghe previste dal'art. 8 CEDU, è causa di un'interpretazione restrittiva del regolamento 1049/2001/CE, che mina l'equilibrio che il legislatore dell'Unione europea ha cercato di raggiungere tra i due regolamenti in questione.

Nel merito, la Corte ha dichiarato che la Commissione ha legittimamente deciso che l'elenco dei partecipanti ad una riunione tenutasi nell'ambito di un procedimento per inadempimento contiene dati personali che permette l'identificazione delle persone che vi hanno partecipato alla luce delle disposizione del regolamento 45/2001/CE.

In tal contesto, la Commissione ha preteso da parte della ricorrente, per le persone che non avessero prestato il consenso espresso, la dimostrazione della necessità del trasferimento di tali dati personali in conformità delle disposizioni dell'art. 8, lett. b), del regolamento 45/2001/CE.

CAP. IV

Altre questioni interpretative della direttiva 95/46/CE

1. *Asociación Nacional de Establecimientos Financieros de Crédito*. – 2. *Deutsche Telekom AG*. – 3. *Institut professionnel des agents immobiliers*. – 4. *Ryneš*.

1. Nella sentenza *Asociación Nacional de Establecimientos Financieros de Crédito*[203], la Corte di giustizia è stata chiamata a pronunciarsi in via pregiudiziale sull'interpretazione dell'art. 7, lett. f), della direttiva 95/46/CE, relativa al trattamento dei dati personali, nonché alla libera circolazione di tali dati. In primo luogo, la Corte specifica che l'obiettivo della direttiva in questione è quello di realizzare una completa armonizzazione delle legislazioni nazionali volta a garantire la libera circolazione dei dati personali nel rispetto dei diritti e degli interessi dei titolari dei dati. È la stessa direttiva che all'art. 7 fornisce un elenco esaustivo e tassativo dei casi in cui il trattamento dei dati può considerarsi lecito. Pertanto a questa fattispecie non si applica il margine di discrezionalità ai sensi dell'art. 5 della direttiva. Gli Stati membri possono avvalersi del margine di discrezionalità di cui godono per il raggiungimento dell'equilibrio fra libera circolazione dei dati e protezione della vita privata soltanto attraverso provvedimenti nazionali che precisino i principi della direttiva.

Ai sensi dell'art 7, lett. f), il trattamento dei dati personali è lecito se necessario alla realizzazione del legittimo interesse perseguito dal responsabile del trattamento e dai terzi ai quali tali dati vengono comunicati. Va comunque ricercata una ponderazione dei diversi diritti in gioco che va adattata alle circostanze del caso concreto in considerazione della tutela del diritto fondamentale della vita privata e dei dati personali sancita dagli artt.7 e 8 della Carta. Il rispetto dei citati diritti fondamentali riferiti ad ogni persona fisica identificata ed identificabile può subire delle limitazioni al verificarsi di determinate circostanze valutabili in forza del margine di apprezzamento concesso agli Stati membri.

La Corte afferma che non possono essere ammesse mediante norme nazionali condizioni per il trattamento dei dati personali diverse da quelle contemplate all'art. 7 lett. f). Pertanto tale disposizione osta a che uno Stato membro escluda in modo categorico e generalizzato la possibilità che talune categorie di dati personali siano oggetto di trattamento, senza consentire la ponderazione dei diritti e degli interessi contrapposti in gioco.

Inoltre nel caso di specie il giudice del rinvio chiede anche se la disposizione esaminata abbia un effetto diretto in quanto si tratta di una direttiva incondizionata, sufficientemente precisa ed invocabile dai singoli davanti ai giudici nazionali in caso recepimento scorretto o tardivo da parte dello Stato membro. La Corte di giustizia a tal proposito stabilisce che l'art. 7 lett. f) prescrive un obbligo incondizionato con efficacia diretta.

[203] Sentenza del 24 novembre 2011, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) e Federación de Comercio Electrónico y Marketing Directo (FECEMD) c. Administración del Estado*, cause riunite C-468/10 e C-469/10, non ancora pubblicata in *Racc*.

2. Nella sentenza *Deutsche Telekom AG c. Germania*[204], la Corte di giustizia esamina su rinvio pregiudiziale la problematica della gestione dei dati presenti sugli elenchi abbonati e trattati, ai sensi della direttiva sul servizio universale, dalle compagnie telefoniche che operano in regime di concorrenza. Infatti la domanda di pronuncia pregiudiziale ha per oggetto l'interpretazione dell'art. 25, n. 2, della direttiva 2002/22 , relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, nonché dell'art. 12 della direttiva 2002/58 , relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche.

In primo luogo, la Corte di giustizia sottolinea come la disposizione comunitaria della direttiva sul servizio universale prescriva un obbligo di comunicazione di dati solamente in capo alle imprese che forniscono numeri telefonici agli abbonati. Tale interpretazione è conforme alla finalità di garantire il rispetto dell'obbligo di servizio universale sancito all'art. 5, n. 1, della direttiva stessa. Infatti almeno un elenco completo o un servizio completo di consultazione degli elenchi deve essere garantito ai fruitori finali da parte degli Stati membri. Il raggiungimento dell'obiettivo di fornitura del servizio universale presuppone da parte dell'impresa, operante nel settore, la costituzione di una banca dati alla luce di quanto previsto dall' art. 5, n. 1.

La Corte analizza se l'art. 25, n. 2 sia rivolto ad un'armonizzazione completa, oppure permetta agli Stati membri di imporre alle imprese che attribuiscono numeri di telefono l'obbligo di comunicare alle imprese che vogliono fornire elenchi e servizi di consultazione accessibili al pubblico, oltre alle "informazioni necessarie" anche i c.d. "dati esterni".

Secondo la Corte, in considerazione delle finalità della disposizione, gli Stati possono predisporre regolamentazioni diverse per consentire l'entrata di nuovi operatori nel mercato della fornitura di elenchi e servizi di consultazione. Quindi il diritto dell'UE non osta ad una normativa nazionale, la quale, rivolta ad un'impresa che attribuisce numeri di telefono a utenti finali, incida sulle imprese di comunicazioni elettroniche in modo generale e non discriminatorio, a condizione che non pregiudichi le competenze spettanti alle autorità nazionali di regolamentazione.

Nel caso di specie, la normativa tedesca non pregiudica affatto le competenze attribuite dal diritto comunitario del settore alle suddette autorità. L'art. 25, n. 2, della direttiva sul servizio universale non predispone alcuna competenza specifica e non prescrive obblighi particolari. La disposizione in parola impone obblighi soltanto agli Stati membri.

La Corte di giustizia, richiamando una propria consolidata giurisprudenza,

[204] Sentenza del 5 maggio 2011, *Deutsche Telekom AG c. Bundesrepublik Deutschland*, causa C-543/09, in *Racc.* p. 03441.

ricorda, in termini generali, come: "Il diritto alla protezione dei dati personali non appare come una prerogativa assoluta, ma va considerato alla luce della sua funzione sociale"[205]. In base a tale principio e alla luce delle disposizioni della direttiva, gli abbonati devono ricevere un'informativa completa riguardante le finalità della compilazione degli elenchi e la possibilità di ulteriori utilizzazioni prima dell'inserimento negli stessi. In tal modo l'abbonato può acconsentire (ai sensi degli artt. 2, lett. h) e 7, lett. a), della direttiva 95/46/CE) alla pubblicazione, in elenchi pubblici, di dati personali che lo riguardano.

Pertanto nel caso di trasmissione dei dati ad un'impresa terza, non è necessario acquisire un ulteriore consenso dall'abbonato che abbia autorizzato esplicitamente la cessione dei propri dati ad altre imprese attive nel mercato. La Corte rileva che il consenso fornito dall'abbonato preventivamente informato è finalizzato alla pubblicazione dei dati che lo riguardano e si estende al trattamento di tali dati da parte di imprese terze operanti nel settore della fornitura di elenchi e di servizi di consultazione accessibili al pubblico, a condizione che i dati raccolti siano trattati per lo stesso scopo della pubblicazione. Sul punto i giudici europei affermano, in conclusione, che: "Quando l'abbonato ha acconsentito alla trasmissione dei dati personali che lo riguardano ad un'impresa determinata affinché siano inseriti in un elenco pubblico di tale impresa, la trasmissione degli stessi dati ad un'altra impresa che intende pubblicare un elenco pubblico, senza che detto abbonato abbia nuovamente prestato il proprio consenso, non può ledere la sostanza stessa del diritto alla tutela dei dati personali, riconosciuto dall'art. 8 della Carta"[206].

3. La Corte di giustizia nella sentenza *Institut professionnel des agents immobiliers*[207], facendo riferimento ad una consolidata giurisprudenza[208], ha affermato che eventuali deroghe e limitazioni riguardanti la protezione dei dati personali devono applicarsi solo nella misura in cui ciò sia strettamente necessario. Secondo costante giurisprudenza, la tutela del diritto fondamentale alla vita privata richiede che le deroghe e le restrizioni alla tutela dei dati personali debbano operare entro i limiti dello stretto necessario[209].

La questione pregiudiziale attiene all'interpretazione della direttiva 95/46/CE. Il giudice di rinvio si interroga sul valore da attribuire alle prove fornite dagli investigatori privati, che potrebbero essere ottenute senza rispettare gli obblighi relativi al trattamento dei dati personali. La legge nazionale impone l'obbligo di

[205] *Ivi*, par. 51.
[206] *Ivi*, par. 66.
[207] Sentenza del 7 novembre 2013, causa C-473/12, *Commissione europea c. Italia*, non ancora pubblicata in *Racc.*
[208] *Ivi*, punto 39 e giurisprudenza ivi citata.
[209] V. sentenze del 16 dicembre 2008, *Satakunnan Markkinapörssi e Satamedia*, causa C-73/07, in *Racc.* p. I-9831, par. 56, nonché del 9 novembre 2010, *Volker und Markus Schecke e Eifert*, causa C-92/09 e C-93/09, in *Racc.*, p. I-11063, paragrafi 77 e 86.

informare previamente la persona interessata dell'indagine condotta dagli investigatori oppure di informarla al momento della registrazione dei dati in questione. Tali circostanze tuttavia rendono impossibile l'attività stessa d'investigazione. La legge prevede esenzioni qualora le attività svolte riguardino l'informazione del pubblico o la vita culturale, il mantenimento della sicurezza e dell'ordine pubblico e la difesa dei diritti fondamentali dei soggetti più vulnerabili.

Il giudice del rinvio osserva che gli investigatori privati si troverebbero in una circostanza diversa poiché pur essendo la loro professione regolamentata da una legge nazionale che ne definisce i contorni e subordina l'esercizio della professione all'autorizzazione del Ministro dell'Interno, tuttavia tale attività è estranea alla tutela di tali diritti fondamentali e interessi generali e riguarda di solito la tutela di interessi privati.

La Corte di giustizia dell'Unione chiarisce che la direttiva 46/95 consente agli Stati membri, al momento della trasposizione nel diritto interno, la facoltà di trasporre una o più deroghe previste all'obbligo di informare le persone interessate del trattamento dei loro dati personali. Pertanto, l'attività di investigatore privato che agisce per conto di un organismo professionale rientra nell'ambito della deroga prevista dalla direttiva.

4. Con la sentenza *Ryneš*[210], la Corte di giustizia fissa i principi dell'uso di strumenti di controllo puntati sulla pubblica via limitandoli alla necessità funzionale di difesa dei beni, della salute e della vita di chi li ha installati. Le telecamere di sorveglianza private all'ingresso degli edifici e a protezione delle finestre sono ammesse soltanto se servono a proteggere un "interesse legittimo" di chi le installa.

La direttiva sulla tutela dei dati personali si applica alla videoregistrazione realizzata mediante una videocamera di sorveglianza installata da una persona sulla

[210] V. sentenza dell'11 dicembre 2014, *František Ryneš contro Úřad pro ochranu osobních údajů*, causa C-212/13, non ancora in *Racc*. Il sig. Ryneš e la sua famiglia erano stati oggetto diverse volte di attacchi da parte di uno sconosciuto e, inoltre, le finestre della loro abitazione erano state infrante in diverse occasioni. In risposta a queste aggressioni, il sig. Ryneš aveva installato sulla casa della sua famiglia una videocamera di sorveglianza la quale filmava l'ingresso di quest'ultima, la pubblica via nonché l'ingresso della casa situata di fronte. Quando una finestra della casa veniva nuovamente infranta, le registrazioni della videocamera di sorveglianza consegnate alla polizia avevano consentito di identificare due sospetti a carico dei quali erano stati attivati procedimenti penali. Tuttavia, uno dei sospetti contestava la legalità del trattamento dei dati registrati dalla videocamera di sorveglianza. In effetti il sig. Ryneš aveva violato le norme in materia di tutela dei dati personali e gli veniva inflitta un'ammenda. Infatti i dati del sospetto erano stati registrati senza il suo consenso mentre egli si trovava sulla pubblica via, ossia nella parte della strada situata dinanzi la casa. Investito di un ricorso in cassazione, la Corte suprema amministrativa della Repubblica ceca chiedeva alla Corte di giustizia se la registrazione allo scopo di tutelare la vita, la salute e beni di Ryneš (ossia, la registrazione di dati personali di individui che avevano attaccato la sua abitazione dalla pubblica strada) costituisse un trattamento di dati non disciplinato dalla direttiva, essendo tale registrazione effettuata da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

sua abitazione familiare e diretta verso la pubblica via e consente nondimeno di valutare l'interesse legittimo di detta persona a proteggere i beni, la salute e la vita propri nonché della sua famiglia.

La direttiva sulla tutela dei dati personali consente, in linea di principio, di trattare dati di tal genere solo in presenza del consenso dell'interessato. Nondimeno, essa non si applica al trattamento di dati effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico.

Nella sua sentenza, la Corte ricorda, in primo luogo, che la nozione di "dati personali" ai sensi della direttiva comprende qualsiasi informazione riguardante una persona fisica identificata o identificabile. È considerata identificabile la persona che può essere identificata, direttamente o indirettamente, mediante riferimento ad uno o più elementi specifici, caratteristici della sua identità fisica. Pertanto, l'immagine di una persona registrata da una telecamera costituisce un dato personale, poiché consente di identificare la persona interessata. Parimenti, la videosorveglianza che comprenda la registrazione e l'immagazzinamento di dati personali rientra nella sfera d'applicazione della direttiva, poiché costituisce un trattamento automatizzato di tali dati.

In secondo luogo, la Corte dichiara che l'esenzione prevista dalla direttiva relativamente al trattamento di dati effettuato da una persona fisica per l'esercizio di attività a carattere esclusivamente personale o domestico deve essere interpretata in modo restrittivo. Pertanto, una videosorveglianza che si estende allo spazio pubblico e che, di conseguenza, è diretta al di fuori della sfera privata della persona che tratta i dati non può essere considerata "un'attività esclusivamente personale o domestica". Applicando la direttiva, il giudice nazionale deve tenere in considerazione, nel contempo, il fatto che le sue disposizioni consentono di valutare l'interesse legittimo del responsabile del trattamento alla protezione dei beni, della salute e della vita.

In particolare, in primo luogo, il trattamento di dati personali può essere effettuato senza il consenso dell'interessato, quando è necessario alla realizzazione dell'interesse legittimo del responsabile del trattamento. In secondo luogo, una persona non deve essere informata del trattamento dei suoi dati, se l'informazione di quest'ultima si rivela impossibile o implica sforzi sproporzionati. In terzo luogo, gli Stati membri possono limitare la portata degli obblighi e dei diritti previsti dalla direttiva, quando tale limitazione è necessaria per salvaguardare la prevenzione, la ricerca, l'accertamento e il perseguimento di infrazioni penali o la tutela dei diritti e delle libertà altrui.

Nel contempo, l'applicazione delle disposizioni della direttiva consente eventualmente di tener conto degli interessi legittimi del responsabile del trattamento, consistenti, come nel procedimento principale, nella tutela dei beni,

della salute e della sua vita nonché della sua famiglia[211].

[211] V. art. 7, lett. f), art. 11, par. 2 nonché art. 13, par. 1, lettere d) e g) della direttiva 46/95/CE.

PARTE IV
Profili specifici di Internet

Cap. I
Giurisprudenza della Corte di Strasburgo

1. Introduzione. – 1.a) *KU v. Finland*. – 1.b) *Editorial Board di Pravoye Delo e Shtekel v. Ukraina*. – 1.c) *Ahmet Yildirim v. Turkey* – 1.d) *Animal Defenders International v. United Kingdom* 1.e) *Delfi AS v. Estonia* – 1.f) *Times Newspapers Limited v. United Kingdom* (n. 1 e 2). – 1.g) *Ashby Donald e Neij e Sunde Kolmisoppi*.

1. La prima novità tecnica affrontata dalla Corte di Strasburgo è stata quella dell'inclusione della tutela delle conversazioni telefoniche nell'ambito di applicazione dell'art. 8 CEDU[212].

La Corte di giustizia si riferisce per la prima volta ad Internet nella sentenza *Zenatti*[213] a proposito delle conseguenze dell'utilizzo del web rispetto all'esercizio delle libertà fondamentali del mercato. In questo contesto, Internet viene considerato come uno strumento per il superamento o l'elusione delle "barriere" normative fra gli Stati membri; in particolare, la questione riguarda il possibile contrasto fra la normativa italiana sul monopolio per la gestione e l'organizzazione di scommesse con la libera prestazione di servizi[214]. Per quanto riguarda la Corte di Strasburgo, la prima volta in cui Internet ha assunto autonoma rilevanza è stata nella sentenza *Éditions Plons c. France*[215] per la diffusione delle informazioni di un libro sul presidente Mitterrand avvenuta, tra l'altro, via internet e pertanto con un danno non più contenibile mediante provvedimenti cautelari[216].

Nel 2007, la Corte ha esteso l'ambito di applicazione dell'art. 8 CEDU al web e al controllo delle e–mail: "According to the Court's case–law, telephone calls from business premises are prima facie covered by the notions of 'private life' and 'correspondence' for the purposes of Article 8 § 1 […]. It follows logically that e–mails sent from work should be similarly protected under Article 8, as should information derived from the monitoring of personal Internet usage"[217].

1.a) Tuttavia è soltanto nella sentenza *K.U. v. Finland*[218] con il concetto di obblighi positivi che la Corte di Strasburgo riesce a coinvolgere la responsabilità dei soggetti privati, vale a dire gli operatori della rete (Internet Service Providers – ISO).

Il caso era originato dalla pubblicazione, ad opera di uno sconosciuto, di un annuncio su Internet nel quale veniva indicato come autore il ricorrente (all'epoca dodicenne) e in cui, oltre a fare menzione della sua età, era fornita una serie di dettagli: le sue caratteristiche fisiche, una sua immagine ricavata da un sito Internet

---

[212] *Klass and Others v. Germany*, 6 September 1978, § 41, Series A no. 28: "Although telephone conversations are not expressly mentioned in paragraph 1 of Article 8 (art. 8-1), the Court considers, as did the Commission, that such conversations are covered by the notions of "private life" and "correspondence" referred to by this provision".

[213] Sentenza della Corte di giustizia del 21 ottobre 1999, *Questore di Verona c. Diego Zenatti*, causa C-67/98, in *Racc.*, p. I-07289.

[214] La Corte di giustizia era alle prese con il caso di un operatore italiano che agiva, mediante il web, come intermediario di un bookmaker britannico, non abilitato a offrire i propri servizi nel territorio italiano.

[215] *Editions Plon v. France*, no. 58148/00, ECHR 2004-IV.

[216] 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*, 4/2010, pp. 105-124.

[217] *Copland v. the United Kingdom*, no. 62617/00, § 41, ECHR 2007-I.

[218] *K.U. v. Finland*, no. 2872/02, ECHR 2008.

da lui gestito all'epoca, i suoi contatti. L'annuncio era finalizzato a ricercare una persona con cui intrattenere "una relazione intima".

I familiari del minore chiedevano all'autorità giudiziaria di ordinare all'Internet service provider di fornire le generalità della persona fisica cui risultava attribuito l'indirizzo IP utilizzato per la connessione e la pubblicazione dell'annuncio. Tuttavia, né il giudice di primo grado né quello d'appello accoglievano la richiesta, fondando il rigetto sull'assenza di una previsione che, in relazione alla fattispecie di reato ipotizzata nel caso specifico, autorizzasse la rivelazione di dati personali da parte del provider. Un obbligo in tal senso, infatti, secondo la legislazione finlandese, sussisteva solo in presenza di determinati illeciti.

La Corte di Strasburgo ha considerato che il diniego costituisse una violazione del diritto al rispetto della vita privata tutelato dall'art. 8 CEDU[219].

Secondo la Corte, una protezione pratica ed effettiva del ricorrente, a nome del quale e a sua insaputa era stato pubblicato illegalmente un annuncio su Internet, implicava l'adozione di misure efficaci tendenti ad identificare e perseguire l'autore dell'annuncio. In quest'ultimo caso, infatti, il comportamento assumeva natura penale.

1.b) La sentenza della Corte di Strasburgo *Editorial Board*[220] riguardava la mancanza di adeguate garanzie legislative nello Stato contraente per l'utilizzo da parte dei giornalisti di informazioni tratte da internet. Il caso riguardava un procedimento di diffamazione contro un giornale locale e il suo capo–redattore a seguito della pubblicazione di una lettera scaricata da Internet in cui si sosteneva che alcuni alti funzionari locali fossero corrotti e coinvolti nel crimine organizzato[221]. La Corte ha dovuto stabilire se la condanna rivolta al capo–redattore risultasse conforme all'art. 10 CEDU (libertà di espressione). A tale riguardo, ha riconosciuto la violazione del principio in parola, a causa della mancanza nella legislazione nazionale di adeguate garanzie per i giornalisti che utilizzano le informazioni ottenute da Internet. In particolare, "having regard to the role the Internet plays in the context of professional media activities … and its importance for the exercise of

[219] *Ivi*, par. 49: "Although freedom of expression and confidentiality of communications are primary considerations and users of telecommunications and Internet services must have a guarantee that their own privacy and freedom of expression will be respected, such guarantee cannot be absolute and must yield on occasion to other legitimate imperatives, such as the prevention of disorder or crime or the protection of the rights and freedoms of others. Without prejudice to the question whether the conduct of the person who placed the offending advertisement on the Internet can attract the protection of Articles 8 and 10, having regard to its reprehensible nature, it is nonetheless the task of the legislator to provide the framework for reconciling the various claims which compete for protection in this context. Such framework was not, however, in place at the material time, with the result that Finland's positive obligation with respect to the applicant could not be discharged".

[220] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, no. 33014/05, ECHR 2011.

[221] I tribunali nazionali avevano condannato i ricorrenti e ordinato di pubblicare delle scuse e pagare una multa.

the right to freedom of expression generally (…), the Court consider[ed] that the absence of a sufficient legal framework at the domestic level allowing journalists to use information obtained from the Internet without fear of incurring sanctions seriously hinders the exercise of the vital function of the press as a 'public watchdog' (…)"[222].

Nonostante tale estensione nei confronti dei più vari strumenti comunicativi, la Corte ha colto l'occasione per sottolineare la diversità tra la stampa e la pubblicazione su internet, ribadendo come, per la particolare diffusione che la pubblicazione elettronica realizza, si possa prevedere una diversa disciplina tra i due media. Così la Corte non ha interpretato estensivamente le norme che in base al Press Act in vigore in Ucraina disciplinavano l'esonero dei giornalisti dalla responsabilità. Nulla, infatti, prevedeva la normativa nazionale in merito alla responsabilità dei giornalisti che riproducono notizie pubblicate su internet, neanche quando, come nel caso concreto, l'editore indichi la fonte e prenda la distanza dal contenuto riprodotto.

1.c) Nella sentenza *Ahmet Yıldırım v. Turkey*[223], la Corte di Strasburgo ha sottolineato come Internet oggi sia diventato uno dei principali mezzi di esercizio, da parte degli individui, del loro diritto alla libertà di espressione e d'informazione e come vi si trovino degli strumenti essenziali di partecipazione alle attività e ai dibattiti relativi a questioni politiche e di interesse pubblico. Il caso riguardava una decisione del tribunale di bloccare l'accesso a Google Sites, che ospitava un sito internet il cui proprietario stava affrontando un procedimento penale per aver insultato la memoria di Atatürk, un eroe nazionale turco. Come risultato della decisione, l'accesso a tutti gli altri siti ospitati dal servizio era stato bloccato. Il ricorrente lamentava di non essere in grado di accedere al suo sito internet a causa di questo provvedimento disposto nell'ambito di un procedimento penale, con il quale egli non aveva alcun collegamento personale o con il suo sito. Egli sosteneva che la misura avesse violato il suo diritto alla libertà di ricevere o di comunicare informazioni o idee. La Corte ha riconosciuto violazione dell'art. 10 CEDU (libertà di espressione). Infatti gli effetti della misura in questione risultavano arbitrari e il blocco di accesso a tutti gli altri siti risultava una misura insufficiente per prevenire eventuali abusi.

1.d) Più recentemente, nella sentenza della Grande Camera *Animal Defenders International v. the United Kingdom*, la Corte ha definito questi "nuovi mezzi" come dei potenti strumenti di comunicazione[224] .

[222] *Ivi*, par. 64.
[223] *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 54, ECHR 2012.
[224] *Animal Defenders International v. the United Kingdom* [GC], no. 48876/08, § 124, ECHR 2013.

Nel caso di specie, la Corte ha respinto il ricorso dell'Animal Defenders International contro il Regno Unito, con il quale lamentava la violazione del diritto di libertà di espressione (art. 10 CEDU), in quanto era stato negato il permesso di trasmettere in televisione uno spot di sensibilizzazione contro lo sfruttamento dei primati negli zoo, nei circhi e nella pubblicità[225]. L'Autorità di controllo inglese (BACC) aveva negato il permesso di trasmettere lo spot, affermando che si trattava di un messaggio pubblicitario di carattere "politico" e, come tale, proibito dalla legge inglese sulle trasmissioni radiotelevisive[226].

La House of Lords affermò, in particolare, che il divieto di pubblicità politica nella legge britannica è giustificato dallo scopo di impedire che il dibattito pubblico sia alterato in ragione di investimenti economici e che, pertanto, la scelta normativa non fosse incompatibile con l'art. 10 CEDU.

L'Animal Defenders International presentò ricorso alla Corte di Strasburgo, rilevando come il divieto fosse sproporzionato in quanto colpiva anche gruppi di sensibilizzazione sociale ed anche in periodi al di fuori delle campagne elettorali.

La Grande Camera ha invece affermato che non vi fosse stata alcuna violazione dei principi della CEDU, ritenendo che i giudici nazionali avessero adeguatamente motivato la decisione, condividendo il principio che la libertà di espressione può essere limitata in ragione del mantenimento di garanzie di non influenza politica e, comunque, potendo la ONG ricorrente utilizzare altri mezzi di informazione, quali giornali e internet. Si sottolinea che la decisione della Grande Camera è stata adottata a stretta maggioranza, con una vistosa spaccatura tra i giudici (8 favorevoli e 7 contrari). Inoltre, con questa sentenza, la Corte ha operato un clamoroso *revirement* della propria precedente giurisprudenza in tema di libertà di espressione: infatti, come rilevato dai giudici dissenzienti, il caso in parola risultava identico ad alcuni precedenti in cui si era pervenuti invece ad accertamento di infrazione[227].

La sentenza sottolinea il rilievo dell'assenza di un "consenso europeo" in materia di pubblicità politica ai fini dell'estensione del margine di apprezzamento nazionale. Si è visto che la Corte attribuisce un notevole rilievo alla assenza di un atteggiamento condiviso nei confronti del problema della pubblicità politica nel contesto dei paesi europei aderenti alla CEDU. Infatti, anche sulla base dei risultati

[225] Nel 2005 l'Animal Defenders International, nell'ambito della campagna "My Mate's a primate", aveva realizzato uno spot, nel quale si vedeva una ragazzina dentro una gabbia, poi scorrevano in successione tre messaggi: "A chimp has the mental age of a four year old"; "Although we share 98% of our genetic make-up they are still caged and abused to entertain us"; e "To find out more, and how you can help us to stop it, please order your £10 educational information pack". Nella parte finale, appariva uno scimpanzè nella stessa posizione della ragazzina.

[226] V. Communications Act 2003. La decisione venne confermata dall'High Court nel dicembre 2006 e dalla House of Lords nel marzo 2008.

[227] V. sentenze *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland (no. 2)*, no. 32772/02, 4 October 2007; *Verein gegen Tierfabriken Schweiz (VgT) v. Switzerland (no. 2)* [GC], no. 32772/02, ECHR 2009.

di uno studio condotto al riguardo, la Corte ha concluso che alle autorità nazionali andrebbe riconosciuto un più ampio margine di apprezzamento, anche con riferimento alle restrizioni in materia di libertà di espressione, almeno a partire dalla sentenza *Handyside*[228]. Tuttavia, la semplice constatazione della disomogeneità delle legislazioni nazionali non dovrebbe essere sufficiente, dovendosi pur sempre verificare se ci si trovi di fronte a situazioni che ammettono una pluralità di soluzioni, tutte astrattamente legittime. L'assenza di un "consenso europeo" viene ritenuta rilevante laddove ci si trovi sin dall'inizio in presenza di situazioni che non consentono una soluzione obbligata, perché coinvolgono scelte di ordine etico (ad es. il concetto di osceno), o perché richiedono delicate e complesse operazioni di "bilanciamento" tra diritti confliggenti (come nel caso della sentenza *Evans*[229]). Ma nel caso deciso dalla sentenza in commento, non pare si possa affermare che ci si trovasse in una simile situazione. Infatti, l'esigenza di porre dei limiti alla comunicazione pubblicitaria per salvaguardare l'equilibrio e la correttezza della competizione politica è un'esigenza che appare oggi riconosciuta dalla stragrande maggioranza dei paesi aderenti alla CEDU, e che non presenta implicazioni di ordine "etico", o più latamente "culturale", tali da rendere ammissibili soluzioni differenti da Stato a Stato e l'unica valutazione che la Corte era chiamata a svolgere era quella relativa alla "necessità" e "proporzionalità" della restrizione concretamente adottata.

In questa diversa prospettiva, l'assenza di un consenso europeo in materia, a ben vedere, lungi dal legittimare le scelte del legislatore nazionale, ben potrebbe essere invocata, all'opposto, per mettere in discussione la tesi del governo britannico, ripresa e fatta propria prima dai giudici nazionali e poi dalla Corte, sull'impraticabilità di soluzioni meno restrittive.

In effetti, come si è visto, l'esame delle soluzioni adottate nei diversi paesi evidenzia come siano possibili soluzioni più duttili ed articolate; anzi come sia sempre più esiguo il numero dei paesi che mantengono in vita un divieto assoluto e generalizzato come quello del Regno Unito. In molti Stati contraenti un divieto analogo non esiste del tutto, o, se esiste, è modulato in modo da renderne più duttile e selettiva l'applicazione.

1.e) La sentenza della Grande Camera *Delfi AS v. Estonia*[230] soppesa due esigenze che

[228] *Handyside v. the United Kingdom*, 7 December 1976, Series A no. 24.
[229] *Evans v. the United Kingdom* [GC], no. 6339/05, ECHR 2007-I.
[230] *Delfi AS v. Estonia*, no. 64569/09, 10 October 2013. La ricorrente, la Delfi AS, era una società anonima registrata in Estonia. Possedeva uno dei più importanti siti internet di informazioni del Paese. Il sito in questione pubblicò un articolo su una società di traghetti, riguardo la decisione di modifica del percorso seguito per raggiungere alcune isole. Tale modifica del percorso aveva provocato una serie di ritardi nell'apertura di strade, che avrebbero rappresentato un collegamento più economico e più rapido per le isole rispetto al servizio dei traghetti. Pertanto molti lettori del sito

sorgono oggi in materia di libertà di espressione, vale a dire la protezione da una parte della libertà di Internet e quindi, dei diritti e libertà dei suoi utenti (art. 10 CEDU); dall'altra, dell'onore e della reputazione delle persone (art. 8 CEDU). Tutti interessi che devono essere giustamente bilanciati in una società democratica e che, nella sentenza in parola, vengono ponderati con riferimento ai commenti postati dai lettori su un portale web di notizie. A tale riguardo, la Corte cita la sua precedente giurisprudenza[231].

Il proprietario di una società di traghetti citava in giudizio il gestore di uno dei più importanti siti internet di informazioni dello Stato contraente, ottenendo una sentenza di condanna per commenti diffamatori di cui il gestore veniva dichiarato responsabile. L'appello fu rigettato dalla Corte Suprema. In particolare, i tribunali nazionali rigettarono l'argomentazione della società ricorrente secondo la quale, ai sensi della direttiva UE 2000/31 sul commercio elettronico, il suo ruolo di società fornitrice di servizi internet o di immagazzinamento dati era meramente tecnico, passivo e neutrale, ritenendo, al contrario, che il portale esercitasse un controllo sulla pubblicazione dei commenti. Invocando l'art. 10 (libertà di espressione), la società Delfi lamentava che i tribunali nazionali l'avessero ritenuta responsabile dei commenti scritti dai suoi lettori.

Nella sentenza in parola, la Corte interpreta la CEDU alla luce delle attuali caratteristiche di internet. Da una parte, considera sproporzionato porre sulla vittima di diffamazione via Internet l'onere dell'identificazione degli autori e allo stesso tempo accoglie i desideri degli utenti di non svelare la loro identità nell'esercizio della loro libertà di espressione; dall'altra, ritiene che sia un compito più oneroso per la persona potenzialmente danneggiata che per l'operatore di un portale Internet, quello di individuare dichiarazioni diffamatorie su Internet, e quindi pone sulla società proprietaria del sito Internet l'onere della tutela della reputazione delle persone.

La Corte ha citato al riguardo la sua precedente giurisprudenza, in particolare la sentenza *Krone Verlag GmbH & Co. KG v. Austria (n. 4)*[232], nella quale ha stabilito che lo spostamento del rischio del risarcimento del danno della persona diffamata alla società di gestione (di norma in una migliore posizione finanziaria rispetto a quella del diffamatore) non risultava un'ingerenza sproporzionata nel diritto alla libertà di espressione della medesima società.

In primo luogo, la Corte ha esaminato l'argomentazione della società ricorrente secondo cui la trasposizione della direttiva 2000/31 sul commercio elettronico nella legislazione estone limitava la sua responsabilità per i commenti diffamatori dei suoi lettori. Secondo la

---

avevano scritto messaggi offensivi o minacciosi nei riguardi della società di traghetti e del suo proprietario.

[231] *Von Hannover v. Germany (no. 2)* [GC], nos. 40660/08 and 60641/08, ECHR 2012.

[232] *Krone Verlag GmbH & Co. KG v. Austria* (no. 4), no. 72331/01, 9 November 2006.

Corte, spettava ai tribunali nazionali risolvere le questioni relative all'interpretazione del diritto interno. I tribunali nazionali si erano basati sulle disposizioni del codice civile per dichiarare la società ricorrente responsabile e condannarla; l'ingerenza nel suo diritto alla libertà di espressione era pertanto legittima e conforme alla CEDU.

La Corte ha inoltre osservato che l'art. 10 CEDU autorizza l'ingerenza degli Stati membri nella libertà di espressione per la protezione della reputazione di altri, purché l'ingerenza sia proporzionata alle circostanze. La questione essenziale era pertanto se tale ingerenza risultasse proporzionata, dati i fatti della causa.

Per pronunciarsi su tale questione, la Corte ha valutato quattro questioni chiave. In primo luogo, il contesto dei messaggi[233]. I commenti erano offensivi, minacciosi e diffamatori. Data la natura dell'articolo, la società avrebbe dovuto aspettarsi dei messaggi offensivi e avrebbe dovuto prestare maggiore attenzione al fine di evitare di essere ritenuta responsabile di danno alla reputazione altrui.

In secondo luogo[234], le misure adottate dalla società ricorrente per impedire la pubblicazione di commenti diffamatori. La pagina web in cui era pubblicato l'articolo dichiarava che gli autori dei commenti sarebbero stati responsabili del loro contenuto e che non erano consentiti commenti minacciosi od offensivi. Essa eliminava automaticamente i messaggi contenenti una serie di parole volgari e gli utenti potevano segnalare i commenti offensivi cliccando su un'icona, per consentirne l'eliminazione. Tuttavia, gli avvisi in parola non erano stati sufficienti ad impedire che un gran numero di commenti offensivi fosse inserito nel sito. Inoltre tali messaggi offensivi non erano stati eliminati in tempo utile dal dispositivo di filtraggio automatico delle parole chiave, né dal sistema di notifica e rimozione.

In terzo luogo[235], per quanto riguarda la responsabilità dei reali autori dei commenti, la Corte rileva che il proprietario della compagnia di traghetti avrebbe potuto in linea di massima tentare di citare in giudizio gli autori specifici dei messaggi offensivi invece della società di gestione del sito. Tuttavia sarebbe stato estremamente difficile accertare l'identità degli autori dato che i lettori potevano fare commenti senza registrarsi. Pertanto molti messaggi risultavano anonimi. Attribuire alla società ricorrente la responsabilità dei commenti risultava pertanto più pratico, ma anche ragionevole, dato che il portale di informazioni traeva un profitto commerciale dai messaggi che venivano pubblicati. A tale riguardo, la Corte compie un ragionamento molto interessante circa gli obblighi positivi degli Stati scaturiti dall'art. 8 CEDU, i quali possono comportare l'adozione di misure tendenti ad assicurare il rispetto della vita privata nella sfera delle relazioni degli individui tra loro; essa perciò "non è convinta" che le misure che permettono alla parte danneggiata di far ricorso soltanto contro gli autori dei commenti diffamatori,

[233] *Ivi*, par. 86.
[234] *Ivi*, paragrafi 87-90.
[235] *Ivi*, paragrafi 91-92.

avrebbero garantito nel caso di specie l'effettiva protezione del diritto alla vita privata della persona danneggiata. La Corte nota inoltre che è stata la scelta della società ricorrente di ammettere commenti scritti da utenti non registrati, assumendo così una certa responsabilità per quei commenti. Per fare il bilancio dei diritti e interessi in gioco, la Corte ritiene importante la facilità con cui si rende pubblica l'informazione su internet e la quantità sostanziale di informazione che lì si trova, ciò che significa che individuare dichiarazioni diffamatorie e rimuoverle è un compito difficile. Secondo la Corte, è difficile per l'operatore di un portale di notizie, ma è un compito ancora più oneroso per le persone potenzialmente danneggiate, le quali meno probabilmente avrebbero risorse per monitorare in continuazione la situazione.

In quarto luogo[236], la Corte ha considerato lievi le conseguenze dei procedimenti interni per la società ricorrente, vista l'irrisoria entità della multa inflitta e alla luce del fatto che i giudici non le avessero nemmeno ingiunto l'adozione in futuro di misure di protezione dei diritti di terzi con modalità che avrebbero potuto limitare la sua libertà di espressione.

Tenuto conto di tutte queste considerazioni, la Corte ha riconosciuto l'assenza di un'ingerenza ingiustificata e sproporzionata nel diritto alla libertà di espressione della società ricorrente da parte dello Stato contraente.

1.f) Nel caso *Times Newspapers Ltd v. the United Kingdom (n. 1 e 2)*[237], la società ricorrente, proprietaria ed editrice del quotidiano The Times, sosteneva che la norma di diritto interno, in base al quale ogni ogni pubblicazione diffamatoria dà luogo ad un autonomo motivo di azione costituiva una restrizione ingiustificata e sproporzionata del suo diritto alla libertà di espressione. Infatti la società in parola era stata citata in giudizio per diffamazione, in una prima causa, per la pubblicazione su stampa di due articoli diffamatori e, in una seconda, per non averli rimossi dal proprio sito internet. In particolare, la società ricorrente sosteneva che si dovesse distinguere tra la prima pubblicazione di una notizia su internet e le possibili consultazioni successive.

Secondo la Corte, i siti internet contribuiscono grandemente a migliorare l'accesso del pubblico all'attualità e, in generale, a facilitare la comunicazione dell'informazione. A tale riguardo, la Corte ha ritenuto applicabile l'art. 10 CEDU anche in caso di costituzione di archivi *on line*.

Infatti, il quotidiano in parola aveva pubblicato due articoli presumibilmente diffamatori di un individuo. Entrambi gli articoli erano stati caricati sul sito web, nello stesso giorno in cui erano stati pubblicati nella versione cartacea del giornale.

[236] *Ivi*, par. 93.
[237] *Times Newspapers Ltd v. the United Kingdom (nos. 1 and 2)*, nos. 3002/03 and 23676/03, ECHR 2009.

Nel corso dei due procedimenti diffamatori contro il giornale ricorrente, i giudici nazionali avevano imposto non la cancellazione dei contenuti diffamotori bensì l'aggiunta di una nota in calce che informasse dell'avvenuta sentenza che aveva riconosciuto il carattere diffamatorio dell'articolo in parola.

Secondo la Corte, nel caso di specie non vi era stata alcuna violazione dell'art. 10 CEDU. Infatti, gli archivi *on line* erano gestiti dal medesimo giornale e i giudici nazionali non avevano imposto alcun obbligo di rimozione. La richiesta di aggiunta di una nota adeguata alla versione web non poteva pertanto considerarsi come sproporzionata.

La Corte, con la sentenza in parola, coglie l'occasione per sottolineare l'importanza dell'archivio su internet riguardante eventi passati, da un lato per la sua facilità di accesso e gratuità; dall'altro, per l'utilità per motivi di studio e ricerca. In tale ambito, gli Stati godono di un margine di discrezionalità nel bilanciamento degli interessi coinvolti; soprattutto, in caso di creazione di nuovi archivi, risulta fondamentale la garanzia della veridicità delle informazioni. Pertanto l'accuratezza dell'archivio *on line* prevale sulla libertà di espressione, vista la mancanza di urgenza nella pubblicazione dell'articolo.

1.g) Come abbiamo visto, la Corte ha riconosciuto come la comunicazione via internet possa essere considerata un mezzo tutelato dalla CEDU[238]. Nelle sentenze *Ashby Donald*[239] e *Neij e Sunde Kolmisoppi*, la Corte afferma come le attività dei ricorrenti siano a tutti gli effetti protette dal diritto alla libertà di espressione (art. 10 CEDU), estendendo l'ambito di tutela ad attività potenzialmente lesive di diritti dei privati, quale il diritto d'autore, che si svolgono *on line*[240]. Grazie all'estensione dell'ambito di applicazione dell'art. 10, si rafforza così la tutela della libertà d'espressione su internet. Il bilanciamento dei diritti fra libertà di espressione su internet e diritto d'autore viene effettuato caso per caso senza prevalenza *a priori* di

[238] V. altresì Decision *Perrin v. United Kingdom*, application n. 5446/03, 8 October 2005. V. anche il Commento generale n. 34 del Comitato dei diritti umani, secondo il quale: "[I]nternet and mobile based electronic information dissemination systems, have substantially changed communication practices around the world. There is now a global network for exchanging ideas and opinions that does not necessarily rely on the traditional mass media intermediaries". Si veda *General Comment 34: Freedoms of opinion and expression*, CCPR/ C/GC/34 (GC 34), del 12 settembre 2011, par. 15. Sull'interpretazione dell'art. 19 del Patto sui diritti civili e politici si veda M. O'FLAHERTY, *Freedom of Expression: Article 19 of the ICCPR and the Human Rights Committee's General Comment No 34*, in *Human Rights Law Review*, 2012, p. 627.

[239] *Ashby Donald and Others v. France*, no. 36769/08, 10 January 2013.

[240] V. sentenza *Ashby Donald v. France*, cit., par. 34: "[…] la publication des photographies litigieuses sur un site Internet dédié à la mode et proposant au public des images de défilés à la consultation libre ou payante et à la vente relève de l‟exercice du droit à la liberté d‟expression, et que la condamnation des requérants pour ces faits s‟analyse en une ingérence dans celui-ci". V. altresì par. 27: "Ils en déduisent que le public a le droit d'être informé sur l‟actualité de la mode et qu‟interdire à des médias sous prétexte de contrefaçon de diffuser des photographies de défilés porte une atteinte disproportionnée à ce droit".

quest'ultimo.

La Corte conferma nel caso *Ashby Donald* che l'art. 10 trova applicazione alla comunicazione via Internet, qualsiasi sia il tipo di messaggio che si tratti di veicolare. Il caso riguardava la condanna di alcuni fotografi di moda per violazione del copyright in seguito alla pubblicazione di foto su un sito internet senza l'autorizzazione delle case di moda interessate.

La Corte ha escluso la violazione della CEDU. Nelle circostanze del caso e tenendo conto dell'ampio margine di apprezzamento riconosciuto alle autorità nazionali, la natura e la gravità delle sanzioni inflitte dai giudici nazionali ai ricorrenti non erano tali da ritenere che l'ingerenza in questione fosse sproporzionata rispetto all'obiettivo perseguito.

La decisione sulla ricevibilità *Neij e Sunde Kolmisoppi v. Sweden*[241] riguardava il ricorso da parte dei co–fondatori di "The Pirate Bay", uno dei più grandi siti web del mondo per la condivisione di file *torrent*, contro la loro condanna per violazione del Copyright Act. La Corte ha dichiarato il ricorso irricevibile, sul presupposto che la condivisione di file su Internet, anche di materiale protetto da copyright e per fini di lucro, non risulta coperto dal diritto di "ricevere e diffondere informazioni" ai sensi dell'art. 10 CEDU. Tuttavia, i giudici nazionali avevano giustamente equilibrato gli interessi in gioco, vale a dire il diritto dei ricorrenti di ricevere e diffondere informazioni e la necessità di proteggere i diritti d'autore.

In questo contesto è facile comprendere la portata innovativa delle sentenze della Corte di Strasburgo che ampliano l'ambito d'applicazione dell'art. 10 al fine di porre la libertà d'espressione come limite alla tutela del diritto d'autore. Resta tuttavia da chiedersi su quali basi la Corte si spinga fino a questa soluzione. In questo, la prassi recente della Corte mostra alcune difformità.

Nella sentenza *Ashby Donald*, i giudici di Strasburgo affermano che la pubblicazione delle fotografie costituisse un esercizio della libertà d'espressione dei ricorrenti, richiamando la giurisprudenza precedente in materia di pubblicazioni fotografiche. La giurisprudenza richiamata offre spunti per ricostruire l'*iter* argomentativo della Corte. Nel caso *Von Hannover*, ad esempio, la prospettiva della Grande Camera era quella di un bilanciamento tra il diritto alla vita privata del ricorrente e il diritto alla pubblicazione, che rientra nel classico bilanciamento tra diritti.

Nella decisione *Neji e Sunde Kolmisoppi* la Corte precisa meglio in che termini una condanna per violazione delle norme sul diritto d'autore possa costituire un'interferenza nell'esercizio della libertà d'espressione dei ricorrenti. I giudici di Strasburgo, infatti, menzionano espressamente "the right to impart information and the right of the public to receive it", considerando non solo il diritto individuale a

[241] Decision *Neij e Sunde Kolmisoppi v. Sweden*, application no. 40397/12, 19 February 2013.

fornire informazioni, ma anche il diritto a riceverle. In particolare, la Corte si sofferma sul ruolo fondamentale di internet e afferma che: "Article 10 applies not only to the content of the information but also to the means of transmission or reception since any restriction imposed on the means necessarily interferes with the right to receive and impart information". Il fondamento giuridico è pertanto da ricercarsi nel diritto a impartire e a ricevere informazioni. Deriva da ciò l'esistenza di un obbligo negativo a carico delle autorità nazionali, le quali devono astenersi da attività che ostacolino una normale circolazione delle informazioni.

Questa impostazione è applicata dalla Corte anche ai casi di bilanciamento tra libertà d'espressione e tutela del diritto d'autore. Nel caso *Ashby Donald*, i giudici di Strasburgo affermano che, vista la necessità di tutela del diritto d'autore, e la protezione riconosciuta dalla CEDU: "les autorités internes disposaient en l'espèce d'une marge d'appréciation particulièrement importante".

In *Neji and Sunde Kolmisoppi*, la Corte si spinge oltre, affermando come, nel bilanciamento tra libertà d'espressione e tutela del diritto d'autore, quest'ultima richieda la necessaria adozione, da parte dello Stato, di azioni positive volte ad un'efficace protezione.

In conclusione, la Corte, pur ammettendo la possibilità che una sanzione comminata per la tutela del diritto d'autore possa costituire un'interferenza, seppur illegittima, nel godimento della libertà d'espressione, riconosce agli Stati un notevole e ampio margine di discrezionalità. Ciò è senz'altro dovuto al fatto che, nei casi di specie, la Corte si sia dovuta pronunciare in un ambito prettamente commerciale, in cui erano assenti motivi "d'interesse pubblico".

1.h) La Corte di Strasburgo è tornata nella sentenza *Węgrzynowski and Smolczewski v. Poland* a pronunciarsi sull'equilibrio tra libertà di stampa e diritto alla reputazione nei casi di diffusione di articoli attraverso internet[242]. La Corte ha considerato la rimozione di un articolo dal sito internet di un giornale *on line* una misura sproporzionata, malgrado i giudici nazionali avessero giudicato diffamatorio il testo pubblicato nella versione cartacea del giornale, riconducendo nell'alveo della tutela della libertà di espressione gli archivi web dei giornali.

Il caso riguardava la vicenda di due giornalisti che lavoravano per un quotidiano polacco e che erano stati condannati per diffamazione a mezzo stampa per la pubblicazione di alcuni articoli in cui si era affermato come i ricorrenti, entrambi avvocati, avessero conseguito dei vantaggi a seguito della loro partecipazione in alcuni affari che coinvolgevano dei politici. Un anno dopo la sentenza della Corte di appello, che aveva confermato quella di primo grado, i ricorrenti avevano denunciato che nel sito internet del giornale era rimasto pubblicato l'articolo

[242] *Węgrzynowski and Smolczewski v. Poland*, no. 33846/07, 16 July 2013.

diffamatorio. I ricorrenti sottolineavano, peraltro, come fosse estremamente agevole, tramite il motore di ricerca di Google, avere accesso a queste informazioni. Gli avvocati, pertanto, si erano rivolti nuovamente ai giudici, chiedendo la rimozione degli articoli dal sito internet del giornale, ma le istanze erano state rigettate. Il giudice nazionale, tra l'altro, stabiliva che la rimozione dell'articolo dal sito internet sarebbe equivalso ad una censura e avrebbe determinato una riscrittura della storia, in contrasto con i principi dell'archivio.

In appello, i ricorrenti sostenevano come ogni nuova lettura dell'articolo sul sito internet del giornale equivaleva ad una nuova pubblicazione e come i principi tradizionali che governano l'archivio di documenti su stampa non potessero trovare applicazione riguardo agli archivi su internet. Il termine "archivio", infatti, si sarebbe dovuto intendere come un insieme di documenti che hanno perso di attualità. Internet, invece, non sarebbe uno strumento per archiviare materiale, bensì per comunicare e informare su argomenti correnti. Il fatto, quindi, che una parte di un sito internet fosse definito come "archivio" non avrebbe avuto l'effetto di rendere applicabile il relativo regime giuridico. La Corte tuttavia rigettava l'appello evidenziando che la circostanza che i ricorrenti, nel corso del primo giudizio, non avessero fatto una specifica richiesta in ordine alla pubblicazione *on line* rendeva impossibile l'esame di fatti preesistenti al giudizio di primo grado.

La Corte di Strasburgo, adita in ordine alla violazione dell'art. 8 CEDU, non ha riconosciuto fondata la violazione del diritto al rispetto alla vita privata, bilanciando la tutela di questo diritto con la libertà di espressione (ex art. 10 CEDU). Dopo avere ricordato come sia un principio ormai consolidato nella propria giurisprudenza che la libertà di espressione costituisca un elemento fondamentale per una società democratica, la Corte ha osservato il particolare riguardo che deve essere prestato nei confronti delle sanzioni e delle misure imposte alla stampa[243].

La Corte ha sottolineato che internet è uno strumento di informazione e di comunicazione che va distinto dai media su stampa, specialmente con riguardo alla capacità di immagazzinare e trasmettere informazioni. Per tale motivo il network elettronico non può essere sottoposto alle medesime regole vigenti per la stampa. Il rischio infatti di nuocere il diritto al rispetto della vita privata è molto più elevato mediante lo strumento elettronico. Pertente la politica inerente alla riproduzione di materiale su stampa e su internet può differire.

La Corte ha ribadito anche che, in conformità con i propri precedenti giudiziari, gli archivi su internet ricadono all'interno dell'ambito di protezione dell'art. 10 della CEDU ed ha evidenziato il contributo sostanziale di tali archivi nel rendere facilmente e gratuitamente accessibili le notizie, costituendo in tal modo un importante strumento per l'istruzione e per la ricerca. La Corte ha reputato che,

[243] *Ivi*, par. 57.

piuttosto che la rimozione dagli archivi internet della notizia diffamatoria, si debba aggiungere una nota nell'articolo sul sito che informi il pubblico sulla pronuncia del tribunale con cui si è accertato il carattere diffamatorio dell'informazione archiviata.

CAP. II
La giurisprudenza della Corte di giustizia

1. *SABAM*. – 2. *Promusicae*. – 3. *UPC Telekabel Wien*. – 4. *Digital Rights*. – 5. *Google Spain.*

1. Con le sentenze *SABAM*[244], la Corte di giustizia affronta il problema della pirateria informatica che consiste nella violazione del diritto d'autore e dei diritti connessi su internet e nello scaricamento illecito di file di opere protette. La Corte di giustizia deve stabilire se l'interpretazione di alcune direttive comunitarie alla luce dei diritti fondamentali applicabili osti alla predisposizione di un sistema di filtraggio idoneo a bloccare il trasferimento e lo scambio di file che possa pregiudicare il diritto d'autore.

Secondo la giurisprudenza della Corte di Strasburgo in materia, il filtraggio delle comunicazioni costituisce un'ingerenza nel rispetto al diritto della vita privata, familiare e della corrispondenza. Infatti Internet facilita la divulgazione delle informazioni; pertanto il diritto di trasmettere e di ricevere informazioni deve essere applicato anche alle comunicazioni in rete.

Nei casi in parola, la Corte di giustizia ha riconosciuto come la tutela del diritto d'autore debba essere bilanciata con la tutela dei diritti fondamentali così come sanciti dalla Carta dei diritti fondamentali dell'UE ed elaborati nella giurisprudenza della Corte di Strasburgo. Sulla compatibilità di alcune misure richieste dalla SABAM (società belga per la tutela dei diritti d'autore) volte a istituire un sistema di filtraggio del traffico su internet a totale carico di un internet service provider e di un gestore di social network, la Corte riteneva di dover bilanciare il rispetto del diritto d'autore, potenzialmente leso dai contenuti immessi in rete, con altri diritti fondamentali[245], asserendo come le autorità nazionali, nell'adottare misure sanzionatorie per violazione delle norme sul diritto d'autore, debbano tener conto del rispetto dei diritti fondamentali[246].

L'iter argomentativo della Corte di giustizia nei casi appena citati apre senz'altro la strada ad una più efficiente applicazione dei diritti umani nel caso in cui le autorità nazionali sanzionino, o adottino misure per prevenire eventuali violazioni delle norme sul diritto d'autore. Ciò che, tuttavia, manca nelle sentenze sui "casi SABAM" è una presa di posizione sul rapporto tra diritto d'autore e libertà

---

[244] V. sentenza della Corte di giustizia del 24 novembre 2011, causa C-70/10, *Scarlet Extended SA c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, in *Racc.*, p. I-11959; v. altresì sentenza del 16 febbraio 2012, causa C-360/10, *Netlog NV c. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*. Per un commento, A. MONTANARI, *Prime impressioni sul caso SABAM c. Netlog NV: gli Internet Service Provider e la tutela del diritto d'autore on line (Corte di Giustizia CE, 16 febbraio 2012, causa C-360/10)*, in *Il diritto del commercio internazionale*, 2012, p. 1075 ss.; M. BELLIA, G. A. M. BELLOMO, M. MAZZONCINI, in *Il diritto industriale*, 2012, p. 346; A. SPAGNOLO, *Bilanciamento tra diritto d'autore, libertà d'impresa e libertà fondamentali nella giurisprudenza recente della Corte di giustizia*, in *Giurisprudenza di merito*, 2013, p. 125 ss.

[245] A tale riguardo, v. sentenza della Corte di giustizia, causa C-360/10, cit., par. 42: "the protection of the fundamental right to property, which includes the rights linked to intellectual property, must be balanced against the protection of other fundamental rights".

[246] *Ivi*, par. 43: "in the context of measures adopted to protect copyright holders, national authorities and courts must strike a fair balance between the protection of copyright and the protection of the fundamental rights of individuals who are affected by such measures".

d'espressione[247]. In tali pronunce, infatti, la Corte di giustizia affronta il tema dal punto di vista della libertà d'impresa, diritto sancito nella Carta dei diritti fondamentali dell'Unione europea (art. 16), ritenendo che le misure richieste dalla SABAM fossero eccessive rispetto a tale diritto, facendolo quindi prevalere nell'ambito della consueta opera di bilanciamento.

Sul punto relativo alla libertà d'espressione, la Corte si limita semplicemente ad affermare come le misure richieste dalla SABAM "could potentially undermine freedom of information"[248], senza entrare di più nel dettaglio.

Il diritto alla protezione della proprietà è sancito dall'art. 1 del primo Protocollo alla CEDU nonché dall'art. 17, par. 1, della Carta, mentre il par. 2 dello stesso articolo menziona esplicitamente un aspetto importante del diritto alla proprietà, vale a dire la protezione della proprietà intellettuale. L'ordinamento giuridico dell'UE prevede diverse direttive volte all'effettiva tutela della proprietà intellettuale, in particolare i diritti d'autore. La proprietà intellettuale abbraccia non solo quella letteraria e artistica, ma anche brevetti, marchi e diritti connessi.

Come chiarito dalla giurisprudenza della Corte, la protezione del diritto fondamentale alla proprietà dev'essere conciliata con la protezione di altri diritti fondamentali, in particolare con il diritto alla protezione dei dati[249]. Com'è noto, spesso si verificano casi in cui gli enti preposti alla protezione del diritto d'autore chiedano ai fornitori di servizi Internet di rivelare l'identità degli utenti di piattaforme di condivisione di file *on line*. Tali piattaforme spesso consentono agli utenti di internet di scaricare brani musicali gratuitamente, anche se questi sono protetti dal diritto d'autore.

A tale riguardo, la Corte di giustizia afferma che le direttive in questione sono rivolte agli Stati membri per l'effettiva protezione della proprietà intellettuale e del diritto d'autore, ma tali normative non possono contravvenire agli obblighi derivanti dalla tutela dei dati personali. A tal proposito va sottolineato che il diritto fondamentale di proprietà, la proprietà intellettuale, il diritto d'autore e il diritto ad un ricorso effettivo rientrano nei principi generali del diritto comunitario. Tuttavia anche il rispetto della vita privata e la protezione dei dati personali costituiscono diritti fondamentali alla luce della Carta. Pertanto il caso sottoposto all'analisi dei giudici europei pone la problematica della conciliazione dei diversi interessi fondamentali coinvolti.

Il delicato compito di bilanciare i diritti fondamentali in questione spetta inizialmente al legislatore e in fase interpretativa alla Corte di giustizia. Pertanto gli

---

[247] In questo senso v. 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; E. PSYCHOGIOPOULOU, *Copyright Enforcement, Human Rights Protection and the Responsibilities of Internet Service Providers after Scarlet*, in *European Intellectual Property Review*, 2012, p. 554.
[248] Sentenza della Corte di giustizia, causa C-360/10, cit., par. 52.
[249] *Ashby Donald and Others v. France*, no. 36769/08, 10 January 2013, cit.

Stati membri sono tenuti al rispetto dell'equilibrio scaturito dall'operato del legislatore e della Corte malgrado il margine normativo loro concesso per il recepimento delle direttive. All'interno degli Stati membri i giudici e le autorità nazionali devono interpretare il diritto interno in conformità delle direttive europee e alla luce dei principi generali e dei diritti fondamentali dell'Unione europea.

All'interno dell'UE il diritto autore, anche quando l'interesse dei titolari è soprattutto di natura privata, rappresenta ugualmente un interesse della collettività. Pertanto l'accesso ad archivi di dati di imprese private può costituire una minaccia alla protezione del diritto fondamentale in parola.

La Corte, in conclusione, afferma che le direttive in materia, lette in modo sistematico e interpretate secondo la tutela dei diritti fondamentali applicabili, devono essere interpretate nel senso che ostano all'ingiunzione ad un fornitore di accesso ad Internet (service provider) di predisporre un sistema di filtraggio di tutte le comunicazioni elettroniche che transitano per i suoi servizi, in particolare mediante programmi "peer–to–peer". Tale sistema di filtraggio infatti andrebbe applicato indistintamente a tutta la clientela del fornitore, a titolo preventivo, a sue spese esclusive e senza limiti nel tempo.

2. Nella sentenza *Promusicae*[250], la Corte afferma che la direttiva 2002/58/CE (in materia di tutela dei dati nel settore delle comunicazioni elettroniche) unitamente alle direttive richiamate dal giudice del rinvio, è espressione della conciliazione tra i diversi interessi pubblici e privati in gioco. Infatti le disposizioni di quest'ultime disciplinano le condizioni di liceità del trattamento dei dati personali. Il recepimento e l'applicazione delle stesse da parte degli Stati membri non deve essere fonte di situazioni di conflitto fra i diversi diritti fondamentali dell'ordinamento giuridico dell'UE. La Corte ribadisce l'importanza del rispetto del principio di proporzionalità in sede di trasposizione degli atti comunitari, quale fattore di primaria importanza per il giusto contemperamento degli interessi in parola.

Inoltre, la Corte di giustizia afferma, relativamente all'interpretazione del diritto dell'UE in esame, che gli Stati membri non sono tenuti ad istituire un obbligo di comunicazione dei dati personali per garantire l'effettiva tutela del diritto d'autore nell'ambito di un procedimento civile. Tuttavia gli Stati membri sono tenuti in sede di trasposizione ad assicurare il giusto equilibrio tra i diversi diritti fondamentali protetti. Il ruolo fondamentale nell'operare una corretta conciliazione spetta in un'ultima istanza alle autorità nazionali mediante l'interpretazione conforme al principio di proporzionalità delle direttive trasposte.

[250] Sentenza del 29 gennaio 2008, *Productores de Música de España (Promusicae) c. Telefónica de España SAU*, causa C-275/06, in *Racc.*, p. I-00271.

3. Nella sentenza *UPC Telekabel Wien*[251], la Corte di giustizia è tornata ad occuparsi dei profili di responsabilità degli internet service providers in relazione all'accesso, da parte di abbonati, a materiali protetti messi a disposizione del pubblico su internet da un terzo.

La decisione in parola è stata originata dall'iniziativa giudiziaria intrapresa da due società di produzione cinematografica nei confronti di un fornitore di accesso ad internet, stabilito in Austria. Le due società, per porre fine alla violazione dei propri diritti commessa dai gestori di un sito internet che trasmetteva in streaming alcuni film da esse prodotti senza i necessari consensi, avevano chiesto ed ottenuto, in via di urgenza, che fosse ingiunto al provider di bloccare l'accesso dei suoi abbonati a tale sito internet. Il fornitore di accesso ad internet riteneva che una tale ingiunzione non potesse essere emessa nei suoi confronti, in quanto non poteva essere considerato un intermediario che consentiva la violazione dei diritti delle società di produzione, non avendo alcun rapporto commerciale con i gestori del sito in questione. Inoltre sosteneva che non era dimostrabile che gli abbonati al servizio di UPC Telekabel avessero agito in modo illecito; infine che le misure di blocco ordinate risultavano facilmente aggirabili da parte degli utenti e che alcune di esse sarebbero state eccessivamente onerose.

Nell'ambito di tale giudizio, la Corte suprema austriaca aveva rivolto alla Corte di giustizia alcune questioni pregiudiziali relative all'interpretazione della disciplina comunitaria in materia (di cui alla direttiva 2001/29), volte, in particolare, a chiarire se, e a quali condizioni, le autorità giurisdizionali degli Stati membri dell'Unione potessero ingiungere ad un fornitore di servizi di accesso ad internet di adottare misure di blocco di siti che mettevano a disposizione del pubblico materiali protetti dal diritto d'autore senza la preventiva autorizzazione dei titolari dei diritti.

Con la sentenza in esame, la Corte di giustizia ha chiarito che un fornitore di accesso ad Internet che, come nel caso di specie, consenta ai suoi abbonati l'accesso a materiali protetti messi a disposizione del pubblico su internet da un terzo, è un intermediario i cui servizi sono utilizzati per violare un diritto d'autore sulla base della direttiva 2001/29 (art. 8, par. 3), che prevede la facoltà per i titolari dei diritti di chiedere un provvedimento inibitorio nei confronti di tali intermediari.

Per quanto riguarda i caratteri dell'ingiunzione emessa a carico del fornitore di accesso ad internet, la Corte di giustizia, dopo aver richiamato la necessità di garantire un giusto equilibrio tra i vari diritti coinvolti, ha chiarito che: "I diritti fondamentali riconosciuti dal diritto dell'Unione devono essere interpretati nel senso che non ostano a che sia vietato, con un'ingiunzione pronunciata da un giudice, a un fornitore di accesso ad Internet di concedere ai suoi abbonati l'accesso ad un sito Internet che metta in rete materiali protetti senza il consenso dei titolari dei diritti,

[251] Sentenza del 27 marzo 2014, causa C-314/12, *UPC Telekabel Wien GmbH c. Constantin Film Verleih GmbH e Wega Filmsproduktionsgesellschaft mbH*, non ancora in *Racc*.

qualora tale ingiunzione non specifichi quali misure tale fornitore d'accesso deve adottare e quest'ultimo possa evitare sanzioni per la violazione di tale ingiunzione dimostrando di avere adottato tutte le misure ragionevoli, a condizione tuttavia che, da un lato, le misure adottate non privino inutilmente gli utenti di Internet della possibilità di accedere in modo lecito alle informazioni disponibili e, dall'altro, che tali misure abbiano l'effetto di impedire o, almeno, di rendere difficilmente realizzabili le consultazioni non autorizzate dei materiali protetti e di scoraggiare seriamente gli utenti di Internet che ricorrono ai servizi del destinatario di questa stessa ingiunzione dal consultare tali materiali messi a loro disposizione in violazione del diritto di proprietà intellettuale, circostanza che spetta alle autorità e ai giudici nazionali verificare"[252].

4. La sentenza *Digital Rights*[253] inaugura una nuova fase del controllo giurisdizionale a carattere para–costituzionale della Corte sul diritto secondario in forza dell'applicazione dei diritti fondamentali. La Corte non si limita a controllare le disposizioni della direttiva 2006/24 tramite il ricorso ai principi di stretta necessità e proporzionalità, indicando gli elementi correttivi che consentirebbero di superare gli ostacoli di legittimità riscontrati. In questo modo, svolge il ruolo tipico di una corte costituzionale fornendo indicazioni *de iure condendo* per il legislatore dell'Unione: la necessità di differenziazione delle fattispecie a seconda della gravità dei reati ed in funzione delle persone interessate; l'utilizzazione di criteri oggettivi per l'accesso ai dati da parte delle autorità nazionali competenti; le garanzie contro i rischi di abusi o accesso illecito; l'obbligo di conservazione dei dati all'interno del territorio dell'UE.

Secondo la Corte di giustizia, l'estensione della direttiva 2006/24 a tutti i mezzi di comunicazione elettronica ha carattere generalizzato e massivo, rappresentando un'ingerenza nei diritti fondamentali, dal momento che non prevede: differenziazioni ai fini del perseguimento dell'obiettivo della lotta contro crimini gravi; deroghe per persone nei confronti dei quali non vi sia alcuna prova circa il loro coinvolgimento con un crimine grave; eccezioni, quando ad esempio le comunicazioni siano soggette all'obbligo del segreto professionale o collegamenti diretti e specifici con la minaccia alla sicurezza pubblica.

Proprio la mancanza nella direttiva contestata di indicazioni precise volte a restringere l'ambito di operatività delle interferenze nel godimento dei diritti protetti dagli articoli 7 e 8 della Carta (a quanto strettamente necessario in ordine alla realizzazione dell'obiettivo di interesse generale perseguito, ossia la prevenzione, l'investigazione ed il perseguimento della criminalità) ne rende l'intero contenuto

[252] *Ivi*, par. 64.

[253] Sentenza dell'8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Rights Ireland Ltd c. Minister for Communications*, *Marine and Natural Resources e altri c. Kärntner Landesregierung e altri*, non ancora in *Racc*.

contrastante con il principio di proporzionalità, come previsto dalle c.d. "clausole orizzontali" della Carta ed in particolare dall'art. 52, par. 1[254].

In relazione al *contenuto essenziale* dei diritti della Carta, la Corte sviluppa alcune considerazioni sull'art. 7 della direttiva 2006/24 . La conservazione dei dati ivi prevista, che pure rappresenta un'ingerenza particolarmente grave, non è tale da violare il contenuto essenziale dei diritti fondamentali coinvolti, in quanto esclude il contenuto delle comunicazioni o delle informazioni consultate[255]. Pertanto la conservazione dei dati prevista dalla direttiva *non è idonea ad arrecare pregiudizio al contenuto essenziale dei diritti fondamentali* al rispetto della vita privata e alla protezione dei dati di carattere personale. Infatti, la direttiva oltre ad escludere il contenuto delle comunicazioni elettroniche in quanto tale, prevede che i fornitori di servizi o di reti debbano rispettare determinati principi di protezione e di sicurezza dei dati. Neanche in relazione all'art. 8, poiché la direttiva prevede espressamente il rispetto di alcuni principi riguardanti la protezione e la sicurezza dei dati conservati[256].

Invece, sul rispetto del *criterio di proporzionalità*, la Corte rileva come la direttiva non prevede sufficienti garanzie per la sicurezza e la protezione, nonostante la massività della raccolta, la sensibilità di taluni dati e il forte rischio derivante da accessi illegali. Non è inoltre garantita la distruzione dei dati alla fine del periodo né l'obbligo di custodia all'interno dell'Unione europea, escludendo così il controllo di un'autorità indipendente.

In linea di principio, qualora l'oggetto di un ricorso riguardi la valutazione di un'ingerenza nei diritti fondamentali, la discrezionalità del legislatore viene fortemente limitata, così come il controllo esercitato dalla Corte di giustizia.

Non si può neanche escludere l'impatto sull'esercizio della libertà di espressione garantita dall'art. 11 della Carta dal momento che i dati possono riguardare le abitudini, i trasferimenti, le attività, le relazioni sociali e gli ambienti sociali frequentati dai soggetti coinvolti[257].

La Corte di giustizia ha dichiarato invalida la direttiva sulla conservazione dei dati[258], in quanto ha considerato alcune disposizioni come determinanti un'ingerenza di vasta portata e di particolare gravità rispetto ai diritti fondamentali del rispetto

[254] *Ivi*, par. 38: "Eventuali limitazioni all'esercizio dei diritti e delle libertà riconosciuti dalla presente Carta devono essere previste dalla legge e rispettare *il contenuto essenziale* di detti diritti e libertà. Nel rispetto del principio di proporzionalità, possono essere apportate limitazioni solo laddove siano necessarie e rispondano effettivamente a finalità di interesse generale riconosciute dall'Unione o all'esigenza di proteggere i diritti e le libertà altrui".
[255] *Ivi*, par. 39.
[256] *Ivi*, par. 40.
[257] *Ivi*, par. 28.
[258] Direttiva 2006/24/CE del Parlamento europeo e del Consiglio, del 15 marzo 2006, riguardante la conservazione di dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione e che modifica la direttiva 2002/58/CE.

della vita privata e alla protezione dei dati di carattere personale, non limitata allo stretto necessario.

La Corte ha affermato che la conservazione dei dati, oggetto della direttiva 2006/24 , costituisce *prima face* un'ingerenza nei diritti fondamentali dei soggetti coinvolti perchè i dati da conservare consentono di: 1) sapere con chi e con quale mezzo un utente ha comunicato; 2) determinare il momento nonché il luogo di origine; 3) conoscere la frequenza delle comunicazioni dell'abbonato o dell'utente registrato con determinate persone in uno specifico periodo. Tali dati, considerati congiuntamente, possono fornire indicazioni assai precise sulla vita privata dei soggetti in questione, quali le abitudini quotidiane, i luoghi di soggiorno e gli spostamenti, le attività svolte, le relazioni sociali e gli ambienti sociali[259]. Inoltre, da un lato, la conservazione ed il successivo utilizzo dei dati avvengono senza informazione dell'utente; dall'altro, incidono direttamente e specificamente sulla vita privata dei soggetti coinvolti ai sensi degli articoli 7 e 8 della Carta[260].

La Corte di giustizia affronta la valutazione dell'ingerenza in relazione al soddisfacimento di un obiettivo o finalità di interesse generale. La conservazione e la trasmissione alle autorità nazionali competenti risponde effettivamente all'*obiettivo di interesse generale* della lotta alla criminalità grave ed alla difesa della pubblica sicurezza. A tal fine, la Corte ha affermato che, sebbene l'obiettivo primario della direttiva 2006/24 fosse l'armonizzazione delle disposizioni nazionali nel mercato dei dati personali, lo "scopo materiale" della direttiva era quello di garantire la disponibilità dei dati in questione a fini di indagine, accertamento e perseguimento di reati gravi, contribuendo così alla lotta contro il crimine e quindi al mantenimento della sicurezza pubblica. Tale scopo materiale della direttiva sembrava così soddisfare il requisito del perseguimento di una finalità di interesse generale.

Accertato che l'atto normativo aveva come obiettivo materiale o secondario quello della lotta contro i crimini gravi e della salvaguardia della sicurezza dei cittadini europei, la Corte di giustizia verifica l'inesistenza di una relazione tra i dati per i quali sussiste l'obbligo di conservazione e l'esistenza di una minaccia alla sicurezza pubblica. Nella direttiva non erano previste puntuali limitazioni di tale obbligo ad un periodo di tempo circoscritto o ad una delimitata zona geografica o ancora ad una ristretta cerchia di soggetti, in qualche modo probabilmente coinvolti in attività criminose di una certa gravità, ovvero con riguardo a specifici soggetti che potrebbero per altre ragioni contribuire alla prevenzione, all'investigazione o al perseguimento di gravi crimini.

Pertanto, la Corte ritiene che il legislatore dell'Unione abbia ecceduto i limiti imposti dal rispetto del principio di proporzionalità. A tale riguardo, la Corte osserva

[259] V. sentenza *Digital Rights*, cit., par. 27.
[260] *Ivi*, par. 29.

che considerato il ruolo dalla protezione dei dati personali e la portata e la gravità dell'ingerenza in questione, il potere discrezionale del legislatore dell'Unione risulta ridotto e che occorre quindi procedere a un controllo rigoroso. Anche se la conservazione dei dati imposta dalla direttiva può essere considerata idonea a raggiungere l'obiettivo perseguito dalla medesima, l'ingerenza vasta e particolarmente grave di tale direttiva nei diritti fondamentali in parola *non è sufficientemente regolamentata in modo da essere effettivamente limitata allo stretto necessario*.

In primo luogo, infatti, la direttiva trova *applicazione generalizzata* all'insieme degli individui, dei mezzi di comunicazione elettronica e dei dati relativi al traffico, senza che venga operata alcuna differenziazione, limitazione o eccezione in ragione dell'obiettivo della lotta contro i reati gravi.

In secondo luogo, la direttiva non prevede alcun criterio oggettivo che consenta di *garantire che le autorità nazionali* competenti abbiano accesso ai dati e possano utilizzarli *solamente per prevenire, accertare e perseguire penalmente reati* che possano essere considerati, tenuto conto della portata e della gravità dell'ingerenza nei diritti fondamentali summenzionati, sufficientemente gravi da giustificare una simile ingerenza. Al contrario, la direttiva si limita a fare generico rinvio ai "reati gravi" definiti da ciascuno Stato membro nella propria legislazione nazionale. Inoltre, la direttiva non stabilisce *i presupposti materiali e procedurali* che consentono alle autorità nazionali competenti di avere accesso ai dati e di farne successivo uso. L'accesso ai dati, in particolare, non è subordinato al *previo controllo di un giudice o di un ente amministrativo indipendente*.

In terzo luogo, quanto alla *durata della conservazione dei dati*, la direttiva impone che essa non sia inferiore a sei mesi, senza operare distinzioni tra le categorie di dati a seconda delle persone interessate o dell'eventuale utilità dei dati rispetto all'obiettivo perseguito. Inoltre, tale durata è compresa tra un minimo di sei ed un massimo di ventiquattro mesi, senza che la direttiva precisi i criteri oggettivi in base ai quali la durata della conservazione deve essere determinata, in modo da garantire la sua limitazione allo stretto necessario.

La Corte constata peraltro che la direttiva non prevede garanzie sufficienti ad assicurare una protezione efficace dei dati contro i rischi di abusi e contro qualsiasi accesso e utilizzo illeciti dei dati. Essa rileva, tra l'altro, che la direttiva autorizza i fornitori di servizi a tenere conto di *considerazioni economiche* in sede di determinazione del livello di sicurezza da applicare (in particolare per quanto riguarda i costi di attuazione delle misure di sicurezza) e non garantisce la *distruzione irreversibile* dei dati al termine della loro durata di conservazione.

La Corte censura, infine, il fatto che la direttiva *non impone che i dati siano conservati sul territorio dell'Unione*. La direttiva non garantisce, quindi, il pieno controllo da parte di un'autorità indipendente del rispetto delle esigenze di

protezione e di sicurezza, come è invece espressamente richiesto dalla Carta. Orbene, un controllo siffatto, compiuto sulla base del diritto dell'Unione, costituisce un elemento essenziale del rispetto della protezione delle persone con riferimento al trattamento dei dati personali. Nel quadro dell'art. 51, par. 1, della Carta, tale questione richieda chiaramente una risposta positiva[261].

Sulla base delle osservazioni in parola, la Corte di giustizia ha affermato che gli obblighi imposti dalla direttiva 2006/24 sui fornitori di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione di conservare, per un certo periodo di tempo, i dati relativi alla vita privata di una persona e le sue comunicazioni costituisca un'ingerenza in sé nei diritti garantiti dall'art. 7 della Carta dei diritti fondamentali dell'UE. Allo stesso modo, la possibilità per le autorità nazionali competenti di accedere a tali dati, precedentemente conservati, costituisce un'ingerenza non solo nei diritti garantiti dall'art. 7 della Carta, ma anche nel diritto fondamentale alla protezione dei dati personali, ai sensi dell'art. 8 della Carta stessa, in quanto l'accesso a tali dati comporta il loro trattamento da parte delle autorità nazionali competenti. Secondo la Corte di giustizia, quindi, l'ingerenza delle misure della direttiva 2006/24 nei confronti dei diritti fondamentali di cui agli articoli 7 e 8 della Carta sarebbe particolarmente grave.

Infatti, come opportunamente sottolineato dall'avvocato generale Cruz Villalón, il fatto che i dati siano conservati e successivamente utilizzati senza che l'abbonato o l'utente registrato sia informato al riguardo è molto probabile che generino nella persona in questione la percezione che la propria vita privata sia costantemente sorvegliata[262].

La legislazione UE deve stabilire delle norme chiare e precise concernenti lo scopo e l'applicazione delle misure della direttiva in questione imponendo delle garanzie minime affinché le persone coinvolte, i cui dati sono stati trattenuti, siano sufficientemente tutelate contro il rischio di abuso e contro ogni accesso o uso illegittimo di quei dati.

La direttiva 2006/24/CE, inoltre, non prevede alcun criterio oggettivo per la determinazione dei limiti all'accesso ai dati ed al loro utilizzo successivo da parte delle competenti autorità nazionali, al fine di prevenire o perseguire penalmente reati che possano essere considerati sufficientemente gravi da giustificare un'ingerenza nella tutela dei diritti di cui agli articoli 7 e 8 della Carta dei diritti fondamentali dell'UE. Al contrario, la direttiva, fa riferimento ai crimini gravi, ma solo in via generale e comunque rimandando alle definizioni previste dagli

[261] V. in particolare sentenze del 23 novembre 2010, *Tsakouridis*, causa C-145/09, in *Racc.*, p. I-11979, paragrafi da 50 a 52; del 21 febbraio 2013, *Banif Plus Bank*, causa C-472/11, non ancora pubblicata in *Racc.*, par. 29 e del 26 febbraio 2013, *Åkerberg Fransson*, causa C-617/10, non ancora pubblicata in *Racc.*, paragrafi 21 e da 25 a 30).

[262] V. paragrafi 52-72 delle conclusioni dell'Avvocato generale.

ordinamenti nazionali (v. art. 1, par. 1).

La Corte di giustizia, al termine di tali considerazioni, ha concluso che il legislatore UE, nell'adottare la direttiva 2006/24 , aveva ecceduto i limiti imposti dalla necessità di rispettare il principio di proporzionalità, alla luce degli articoli 7, 8 e 52, par. 1 della Carta, dichiarando così l'invalidità della direttiva questione.

È interessante rilevare come, a differenza dell'avvocato generale, la Corte di giustizia non abbia fornito delle indicazioni riguardo agli effetti nel tempo della dichiarazione d'invalidità della direttiva 2006/24 . Infatti, nel testo della sentenza, la Corte non fornisce alcuna indicazione riguardo tali effetti, confermando così l'efficacia *ex tunc* della sentenza di invalidità, quindi risalente alla data in cui la direttiva è entrata in vigore.

L'avvocato generale, invece, nelle sue conclusioni, aveva suggerito una soluzione differente, vale a dire la sospensione degli effetti della costatazione d'invalidità della direttiva per dar tempo al legislatore UE di adottare le misure necessarie per porre rimedio all'invalidità accertata[263].

La scelta della Corte di giustizia di non prevedere sospensione degli effetti della dichiarazione d'invalidità, nelle more dell'adozione dei provvedimenti che l'esecuzione della sentenza comporta per le istituzioni che hanno emanato l'atto annullato (ex art. 266, par. 1 TFUE) è stata probabilmente dettata dalla gravità della violazione accertata e dalla conseguente necessaria pressione che ha inteso esercitare nei confronti delle istituzioni UE competenti a porvi rimedio.

5. Prima della comparsa di internet il diritto all'oblio secondo la dottrina civilistica si riferiva al diritto di un soggetto a non vedere ripubblicate notizie già legittimamente pubblicate a distanza di molto tempo. Con l'utilizzo di internet, il tempo da considerare è quello della durata della pubblicazione che resta immutata. Non si tratta del diritto a dimenticare, ma del diritto a contestualizzare. L'esigenza è quella di attribuire un peso all'informazione nell'ambito dell'identità del soggetto coinvolto[264].

La sentenza *Google Spain*[265] si esprime, in via pregiudiziale, sull'interpretazione degli articoli 12[266] e 14[267] della direttiva 95/46/CE sull'accesso ai dati e

[263] V. punto 158 delle conclusioni dell'Avvocato generale.

[264] V. G. PINO, *Teorie e dottrine dei diritti della personalità Uno studio di meta-giurisprudenza analitica*, in *Materiali per una storia della cultura giuridica*, 2003/1, p. 237 ss.; F. DI CIOMMO, R. PARDOLESI, *Dal diritto all'oblio in Internet alla tutela dell'identità dinamica. È la Rete, bellezza!*, in *Danno e responsabilità*, 7/2012, p. 701 ss.; G. FINOCCHIARO, *Il diritto all'oblio nel quadro dei diritti della personalità*, in *Dir. Inf.*, 2014, p. 591 ss.

[265] Sentenza della Corte di giustizia del 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, non ancora pubblicata in *Racc*.

[266] Nell'art. 12, lett. b) si dispone che "gli Stati membri garantiscono a qualsiasi persona interessata il diritto di ottenere dal responsabile del trattamento: (…) a seconda dei casi, la rettifica, la

l'opposizione al trattamento dei medesimi.

Il contenuto del diritto all'oblio in discussione riguarda il diritto alla cancellazione, al congelamento dei dati e all'opposizione al trattamento nei confronti del motore di ricerca, che costituisce un titolare di trattamento. Quest'ultimo non potrà evidentemente cancellare i dati personali che si trovano presso il titolare di trattamento che ha pubblicato l'informazione (ad esempio, sul sito dell'editore del giornale, nei molti casi verificatisi), ma soltanto il collegamento a detti dati (de–indicizzazione). In altri termini, secondo il contenuto della domanda pregiudiziale se "l'interessato può rivolgersi ai motori di ricerca per impedire l'indicizzazione delle informazioni riguardanti la sua persona pubblicate su pagine web di terzi, facendo valere la propria volontà che tali informazioni non siano conosciute dagli utenti di Internet, ove egli reputi che la loro divulgazione possa arrecargli pregiudizio o desideri che tali informazioni siano dimenticate, anche quando si tratti di informazioni pubblicate da terzi lecitamente".

In primo luogo, la Corte afferma che il motore di ricerca è titolare del trattamento dei dati.

Soprattutto la Corte afferma il diritto a cancellare i dati se essi sono inadeguati, non pertinenti o non più pertinenti in rapporto alle finalità del trattamento[268]. Non si tratta di un diritto *ad nutum* ma di un diritto a cancellare che va ponderato ed esercitato in ragione delle caratteristiche dei dati costituite dall'adeguatezza, dalla pertinenza o dalla non pertinenza del trattamento rispetto alle finalità. Non viene

---

cancellazione o il congelamento dei dati il cui trattamento non è conforme alle disposizioni della presente direttiva, in particolare a causa del carattere incompleto o inesatto dei dati".

[267] Nell'art. 14, primo comma, lett. a) si dispone che "gli Stati membri riconoscono alla persona interessata il diritto: (…) almeno nei casi di cui all'articolo 7, lettere e) e f), di opporsi in qualsiasi momento, per motivi preminenti e legittimi, derivanti dalla sua situazione particolare, al trattamento di dati che la riguardano, salvo disposizione contraria prevista dalla normativa nazionale".

[268] Vale la pena di riportare per intero il passaggio rilevante della sentenza: "quanto all'articolo 12, lettera b), della direttiva 95/46/CE, la cui applicazione è subordinata alla condizione che il trattamento di dati personali sia incompatibile con la direttiva stessa, occorre ricordare che, come si è rilevato al punto 72 della presente sentenza, un'incompatibilità siffatta può derivare non soltanto dal fatto che tali dati siano inesatti, ma anche segnatamente dal fatto che essi siano inadeguati, non pertinenti o eccessivi in rapporto alle finalità del trattamento, che non siano aggiornati, oppure che siano conservati per un arco di tempo superiore a quello necessario, a meno che la loro conservazione non si imponga per motivi storici, statistici o scientifici". E aggiunge che pertanto "anche un trattamento inizialmente lecito di dati esatti può divenire, con il tempo, incompatibile con la direttiva suddetta qualora tali dati non siano più necessari in rapporto alle finalità per le quali sono stati raccolti o trattati. Tale situazione si configura in particolare nel caso in cui i dati risultino inadeguati, non siano o non siano più pertinenti, ovvero siano eccessivi in rapporto alle finalità suddette e al tempo trascorso" e conclude che "l'inclusione nell'elenco di risultati – che appare a seguito di una ricerca effettuata a partire dal suo nome – dei link verso pagine web, legittimamente pubblicate da terzi e contenenti informazioni veritiere relative alla sua persona, è, allo stato attuale, incompatibile con il citato articolo 6, paragrafo 1, lettere da c) a e), a motivo del fatto che tali informazioni appaiono, alla luce dell'insieme delle circostanze caratterizzanti il caso di specie, inadeguate, non pertinenti o non più pertinenti, ovvero eccessive in rapporto alle finalità del trattamento in questione realizzato dal gestore del motore di ricerca, le informazioni e i link in parola di cui al suddetto elenco di risultati devono essere cancellati".

affermato un generale diritto all'oblio sui dati trattati dai motori di ricerca, ma l'applicabilità anche a questi di quanto disposto nella direttiva. Non si tratta del diritto a cancellare i dati *tout court*. "Di per sé, una preferenza soggettiva non costituisce un motivo preminente e legittimo ai sensi dell'art. 14, lett. a), della direttiva".

È in rapporto alle finalità del motore di ricerca che va effettuata la valutazione sull'adeguatezza, la pertinenza dei dati e conseguentemente assunta la decisione di cancellare. Gli interessi legittimi perseguiti dai motori di ricerca sono quelli di facilitare l'accesso alle informazioni per gli utenti di Internet, migliorare l'efficacia della diffusione delle informazioni su internet, consentire diversi servizi della società dell'informazione. Questi interessi corrispondono a tre diritti fondamentali tutelati dalla Carta dei diritti fondamentali dell'Unione europea: libertà di informazione, libertà di espressione e libertà di impresa.

Nell'effettuare il trattamento, il motore di ricerca deve rispettare i principi di qualità dei dati dettati dalla direttiva. In particolare "i dati personali debbono essere adeguati, pertinenti e non eccedenti rispetto alle finalità perseguite, ed aggiornati, vale a dire non obsoleti per i fini per i quali sono stati rilevati". Alla luce del principio della qualità dei dati sopra menzionato va interpretata l'affermazione della Corte, secondo la quale "la constatazione di un diritto siffatto non presuppone che l'inclusione dell'informazione in questione nell'elenco di risultati arrechi un pregiudizio all'interessato".

La dottrina si chiede se il diritto all'oblio costituisca un nuovo diritto della personalità. Il bene giuridico che si vuole tutelare è quello dell'identità. Il dato personale è, in ultima analisi, inadeguato o non pertinente rispetto all'identità di un soggetto. Il motore di ricerca è, infatti, idoneo a generare una vera e propria immagine *on line*. La tesi sostenuta è che non sembra che il diritto all'oblio costituisca un diritto in sé e che si debba ampliare il catalogo dei diritti della personalità, dal momento che esso appare comunque strumentale, o al diritto all'identità personale o al diritto alla protezione dei dati personali.

Sia che il diritto all'oblio costituisca un diritto a non vedere ripubblicata l'informazione rispetto alla cui prima pubblicazione è trascorso un rilevante periodo di tempo (qualora la riproposizione della notizia non sia di attuale interesse), sia che si tratti della contestualizzazione dell'informazione, il bene giuridico tutelato è quello dell'identità personale, vale a dire il diritto a non vedere travisata la propria immagine sociale. Il motore di ricerca crea l'immagine *on line* di un soggetto anche se la finalità del trattamento dei dati effettuato dal motore di ricerca è costituita dal rendere l'informazione reperibile su internet. Tuttavia la creazione di un'immagine *on line* è certamente un effetto dell'attività svolta dal motore di ricerca.

In caso di diritto all'oblio nel senso del diritto alla cancellazione dei dati, il bene giuridico tutelato è costituito dai dati personali: il diritto a cancellare è strumentale

al diritto alla protezione dei dati personali. Il dato personale può essere cancellato, come afferma la Corte, se non è più adeguato, aggiornato o pertinente. Infatti, lo scenario e la prospettiva non sono quelli del dato personale contenuto nel singolo archivio, bensì quelli della tutela della persona nella rete internet, che non è un archivio ma un deposito, la quale crea, attraverso i motori di ricerca l'immagine della persona. Indipendentemente dalla constatazione che le informazioni sulla persona on line siano state lecitamente pubblicate, l'immagine complessiva può dare luogo ad un travisamento della sua immagine sociale.

La Corte decide, in sostanza, che il bilanciamento tra i diritti confliggenti (da una parte diritto all'oblio, dall'altra libertà di informazione e espressione) può essere operato in modo soddisfacente nelle specifiche situazioni individuali sulla base di una valutazione caso per caso.

Prima ancora che in *Google Spain*, è nella sentenza che annulla la direttiva in materia di *data retention* che la Corte innova rispetto alla giurisprudenza rilevante. Da una parte, la rilevanza autonoma dei due diritti previsti dagli articoli 7 e 8 della Carta; dall'altra, una distinzione netta tra il profilo del contenuto essenziale di tali diritti e, per altro verso, quello relativo all'accertamento della proporzionalità delle misure in discussione in relazione gli obiettivi previsti di tutela dell'ordine pubblico e lotta contro il terrorismo. Se il primo profilo non è giudicato intaccato nella fattispecie, la Corte di giustizia giudica le misure eccessivamente intrusive nei confronti dei diritti al rispetto alla vita privata ed alla protezione dei dati personali.

Forse è il par. 69 della pronuncia quello che illustra meglio di altri la dichiarazione di intenti dei giudici comunitari in merito alla volontà di leggere le disposizioni rilevanti della direttiva alla luce delle previsioni della Carta a tutela della c.d. "privacy digitale". La Corte osserva infatti che "l'art. 7 della Carta garantisce il diritto al rispetto della vita privata, mentre l'articolo 8 della Carta proclama espressamente il diritto alla protezione dei dati personali. I paragrafi 2 e 3 di quest'ultimo articolo precisano che i dati suddetti devono essere trattati secondo il principio di lealtà, per finalità determinate e in base al consenso della persona interessata o a un altro fondamento legittimo previsto dalla legge, che ogni persona ha il diritto di accedere ai dati raccolti che la riguardano e di ottenerne la rettifica, e che il rispetto di tali regole è soggetto al controllo di un'autorità indipendente. Tali prescrizioni ricevono attuazione in particolare mediante gli articoli 6, 7, 12, 14 e 28 della direttiva 95/46/CE".

A differenza dell'Avvocato generale, che aveva citato le disposizioni in tema di libertà di espressione ed accesso all'informazione (art. 11 Carta) e di libertà di iniziativa economica (art. 16 Carta), la Corte qui si riferisce solo agli articoli 7 ed 8 della Carta.

Il bilanciamento tra diritti contrastanti è realizzato a priori a tutela della privacy digitale. Pur affermando che la soppressione di link dall'elenco di risultati potrebbe

avere ripercussioni sul legittimo interesse degli utenti ad avere accesso a quest'ultima, occorre ricercare "un giusto equilibrio segnatamente tra tale interesse e i diritti fondamentali della persona di cui trattasi derivanti dagli articoli 7 e 8 della Carta", nel senso della presunzione di prevalenza. "Indubbiamente, i diritti della persona interessata tutelati dagli articoli da ultimo citati, prevalgono di norma, anche sull'interesse degli utenti di Internet, tale equilibrio può nondimeno dipendere, in casi particolari, dalla natura dell'informazione di cui trattasi e dal suo carattere sensibile per la vita privata della persona suddetta, nonché dall'interesse del pubblico a disporre di tale informazione, il quale può variare, in particolare, a seconda del ruolo che tale persona riveste nella vita pubblica".

La regola è la soccombenza del diritto (derubricato in mero interesse) all'accesso all'informazione a favore dei diritti che riguardano la protezione della sfera privata e dei dati personali degli utenti. L'eccezione è la possibile prevalenza, in determinati casi ed a certe condizioni, del primo sui secondi[269].

Nella giurisprudenza rilevante della Corte di Strasburgo, ad esempio nella citata sentenza *Węgrzynowski* e *Smolczewski*, la prevalenza della libertà di espressione costituisce la regola e le restrizioni a tale libertà sono le eccezioni, che debbono essere interpretate in modo restrittivo. E ciò anche nel caso in cui il conflitto, come nella fattispecie, sia tra accesso all'informazione sul web e interesse del soggetto ricorrente a fare in modo che informazioni pregiudizievoli per la sua reputazione non siano rintracciabili sul web.

Se vi fossero ancora dei dubbi sul ruolo giocato dagli articoli 7 e 8 della Carta nella estensione delle maglie normative della disciplina rilevante, fino ad includere nella nozione di responsabile del trattamento anche i motori di ricerca, qualche paragrafo più avanti la Corte ribadisce il concetto argomentando che "nella misura in cui l'attività di un motore di ricerca può incidere, in modo significativo e in aggiunta all'attività degli editori di siti web, sui diritti fondamentali alla vita privata e alla protezione dei dati personali, il gestore di tale motore di ricerca quale soggetto che determina le finalità e gli strumenti di questa attività deve assicurare, nell'ambito delle sue responsabilità, delle sue competenze e delle sue possibilità, che detta attività soddisfi le prescrizioni della direttiva 95/46/CE, affinché le garanzie previste da quest'ultima possano sviluppare pienamente i loro effetti e possa essere effettivamente realizzata una tutela efficace e completa delle persone interessate, in particolare del loro diritto al rispetto della loro vita privata".

La Corte, come anticipato, ha il compito di valutare se i diritti riconosciuti agli interessati dalla direttiva, agli articoli 12, lett. b) e 14, c. 1, lett. b), conferiscano a questi ultimi la possibilità di ottenere dal motore di ricerca la rimozione dai risultati dei collegamenti a pagine web ove siano presenti dati personali, ancorché senza

[269] Il rapporto regola/eccezione non è quello proposto dall'Avvocato generale Jääskinen, nè dall'Avvocato generale Kokott nel caso *Satamedia*.

alcuna modifica del sito Internet interessato e senza che la pubblicazione abbia di per sé carattere illecito. Qui viene in gioco in modo diretto l'equilibrio tra, da un lato, la libertà di espressione dei gestori di siti internet; dall'altro, il diritto degli interessati alla tutela dei propri dati personali, ed ai nostri fini è rilevante, in particolare, la forzatura della disciplina prevista dall'art. 12, lett. b) , funzionale a piegarla alle esigenze di massima protezione della privacy digitale degli interessati.

Ai sensi dell'art. 12, lett. b), l'interessato ha diritto di ottenere la cancellazione, la rettifica o il congelamento dei dati, ove il loro trattamento non sia conforme ai principi della direttiva, in particolare a causa del carattere inesatto e incompleto dei dati. La Corte interpreta quest'ultimo inciso a titolo esemplificativo e non esclusivo (come invece sembra emergere da un'interpretazione letterale della disposizione), così ponendo le basi perché qualsiasi difformità nel trattamento in contrasto con la direttiva sia in grado di attribuire all'interessato il diritto di attivarsi come previsto dalla disposizione. Così operando, la sentenza finisce per allargare le maglie della previsione, snaturando il senso del diritto di ottenere la rettifica o la cancellazione dei dati personali, attraverso un richiamo generale alle ipotesi di cui agli articoli 6 e 7 della direttiva.

Al riguardo, tra l'altro, si impone di ricordare che una cosa è un trattamento illecito di dati personali, rispetto al quale i rimedi sono contemplati dalla direttiva; altra è il trattamento senz'altro lecito di dati che l'interessato manifesti l'interesse a non vedere più diffusi in modo incondizionato, che corrisponde specificamente al diritto all'oblio. Tuttavia, i due piani paiono confondersi nell'esame della Corte.

E la ragione della confusione sembra essere, come più volte evidenziato, la volontà dei giudici comunitari, attraverso una lettura orientata della disciplina rilevante alla luce dell'art. 7 e, specialmente, dell'art. 8 della Carta, di allargare al massimo l'ambito di applicazione della direttiva, fino ad includervi fattispecie abbastanza chiaramente escluse in forza di una interpretazione tanto letterale quanto sistematica della stessa e che possono rientrarvi soltanto grazie ad un'operazione ermeneutica molto simile ad un'attribuzione di un'efficacia diretta ed orizzontale degli articoli della Carta prima citati.

Infine, ultimo ambito applicativo della direttiva la cui interpretazione, da parte della Corte, sembra essere stata fortemente influenzata dall'intento di attribuire la massima protezione possibile agli articoli della Carta che compongono lo statuto della privacy digitale, è quello relativo all'ipotesi, prevista dall'art. 9 della direttiva, di possibile deroga ai principi generali in essa fissati nell'ipotesi in cui il trattamento dei dati sia finalizzato a scopi giornalistici o di espressione artistica o letteraria. In particolare, la Corte ricorda che, ai sensi del trentasettesimo considerando della direttiva, l'art. 9 della stessa persegue la finalità di conciliare due diritti fondamentali, vale a dire, da un lato, la tutela della vita privata e, dall'altro, la libertà di espressione, quanto che, ai sensi dello stesso art. 9, le deroghe ammesse sono

esclusivamente quelle risultino necessarie per conciliare il diritto alla vita privata con le norme che disciplinano la libertà d'espressione. Ciò nonostante, i giudici comunitari arrivano alla conclusione, non del tutto convincente, secondo cui "il trattamento da parte dell'editore di una pagina web, consistente nella pubblicazione di informazioni relative a una persona fisica, può, eventualmente, essere effettuato "esclusivamente a scopi giornalistici" e beneficiare così, a norma dell'articolo 9 della direttiva 95/46/CE , di deroghe alle prescrizioni dettate da quest'ultima, mentre non sembra integrare tale ipotesi il trattamento effettuato dal gestore di un motore di ricerca".

La Corte, in altre parole, esclude che il motore di ricerca possa in qualche modo avvalersi della deroga prevista dall'art. 9 della direttiva e, citando la decisione *Satamedia* in cui tale deroga è stata oggetto di specifica interpretazione da parte degli stessi giudici comunitari, dimentica però di menzionare quel passaggio in cui quest'ultimi avevano chiarito come il riferimento a trattamenti per scopi giornalistici dovesse essere inteso nel modo più ampio possibile, includendovi qualsiasi "attività diretta a divulgare al pubblico informazioni, opinioni o idee, indipendentemente dal mezzo di trasmissione".

Bibliografia generale

Manuali e monografie

F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH, *Il codice dei dati personali*: *temi e problemi*, Milano, 2004;
T. M. UBERTAZZI, *Il diritto alla privacy: natura e funzione giuridiche*, Padova, 2004;
G. CASSANO, *Diritto dell'Internet: il sistema di tutele della persona*, Milano, 2005;
S. RODOTÀ, *Intervista su privacy e libertà*, Bari, 2005;
G. SANTANIELLO (a cura di), *La protezione dei dati personali*, Padova, 2005;
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, 2006;
R. BOCCHINI (a cura di), *Codice delle comunicazioni*: *privacy, telefonia fissa e mobile, internet, firma elettronica, televisione, informatica nella P.A*, Milano, 2006;
S. NIGER, *Le nuove dimensioni della privacy: dal diritto alla riservatezza alla protezione dei dati personali*, Padova, 2006;
C. M. BIANCA (a cura di), *La protezione dei dati personali: commentario al D.lgs. 30 giugno 2003, n. 196*, *Codice della privacy*, Padova, 2007, vol. 2;
V. CUFFARO, R. D'ORAZIO, V. RICCIUTO (a cura di), *Il codice del trattamento dei dati personali*, Torino, 2007;
P. PERRI, *Protezione dei dati e nuove tecnologie: aspetti nazionali, europei e statunitensi*, Milano, 2007;
G. FIORIGLIO, *Il diritto alla privacy: nuove frontiere nell'era di internet*, Bologna, 2008;
R. RAZZANTE, *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2008;
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;
S. GUTWIRTH (ed.), *Reinventing data protection?*, Dordrecht, 2009;
S. SICA, V. ZENO-ZENCOVICH (a cura di), *Manuale di diritto dell'informazione e della comunicazione*, Padova, 2009;
A. M. GAMBINO, A. STAZI, *Diritto dell'informatica e della comunicazione*, Torino, 2009;
Article 29 Working Party (A29WP), *The Future of Privacy – Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, Brussels, 2009;
E. BRIBOSIA, *In search of a balance between the right to equality and other fundamental rights*, Luxembourg, 2010;
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS (a cura di), *Data protection in the European Union: the role of national data protection authorities. Strengthening the fundamental rights architecture in the EU*, Wien, 2010;
L. COUDRAY, *La protection des données personnelles dans l'Union européenne: naissance et consécration d'un droit fondamental*, Sarrebruck, 2010;
E. GUILD, *The area of freedom, security and justice ten years on: successes and future challenges under the Stockholm Programme*, Brussels, CEPS, 2010;
S. GUTWIRTH, *Data protection in a profiled world*, Dordrecht, 2010;
R. ZACCARIA, *Diritto dell'informazione e della comunicazione*, 7 ed., Padova, 2010;
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, 2011;
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;
E. KOSTA, *Consent in European data protection law*, Leiden, 2013;
W. BENEDEK, M.C. KETTEMANN, *Liberté d'expression et internet*, Strasbourg, Conseil de l'Europe, 2014;
LEE A. BYGRAVE, *Data privacy law: an international perspective*, Oxford, 2014;
G. GONZÁLEZ FUSTER, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Berlin, 2014;

Articoli

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, 2005, p. 365 ss.;
M. MAES, *La refonte du règlement (CE) n° 1049/2001 relatif à l'accès du public aux documents du Parlement européen, du Conseil et de la Commission*, in *Revue du droit de l'Union européenne*, 2007, p. 411 ss.;
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 ss.;
E. HERLIN–KARNELL, *Is there more to it than the fight against "dirty money"?: Article 95 EC and the Criminal Law*, in *European Business Law Review*, 2008, p. 557 ss.;
H. KRANENBORG, *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 ss.;
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 ss.;
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 ss.;
P. DE HERT, S GUTWIRTH, *'Data Protection in the case law of Strasbourg and Luxemburg: Constitutionalisation in Action*', in S. GUTWIRTH, Y. POULLET, P. DE HERT, S. NOUWT, C. DE TERWANGNE (eds), *Reinventing Data Protection*? Berlin, 2009, p. 5 ss.;
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*, 2009, p. 53 ss.;
E. HERLIN–KARNELL, *Case C–301/06, Ireland v. Parliament and Council, Judgment of the Court (Grand Chamber) of 10 February*, *2009*, in *Common Market Law Review*, 2009, p. 1167 ss.;
E. HERLIN–KARNELL, *Subsidiarity in the area of EU Justice and Home Affairs law: a lost cause?*, in *European Law Journal*, 2009, p. 351 ss.;
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 ss.;
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 ss.;
V. MITSILEGAS, *The third wave of third pillar law: which direction for EU criminal justice?* in *European Law Review*, 2009, p. 523 ss;
P. OLIVER, The *Protection of Privacy in the Economic Sphere before the European Court of Justice*, in *Common Market Law Review*, 2009, p. 1443 ss.;
S. 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*, in *Revue française de droit administratif*, 2009, p. 741 ss.;
V. PAPAKONSTANTINOU, P. DE HERT, *The PNR Agreement and transatlantic anti-terrorism cooperation: no firm human rights framework on either side of the Atlantic*, in *Common Market Law Review*, 2009, p. 885 ss.;
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 ss.;
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 ss.;
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 ss.;
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 ss.;
O. DE SCHUTTER, *Les droits fondamentaux dans l'Union européenne*, in *Journal de droit européen*, 2010, pp. 120-127;
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 ss.;
H. HIJMANS, *Recent developments in data protection at European Union level* in *ERA-Forum: scripta iuris europaei*, 2010, p. 219 ss.;
W. HINS, *Case C–73/07, "Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia O", judgment of the Grand Chamber of 16 December 2008, not yet reported*, in *Common Market Law Review*, 2010, p. 215 ss.;
J-P. JACQUE, *Communauté des internautes et protection des libertés individuelles dans l'Union européenne*, in *Revue trimestrielle de droit européen*, 2010, p. 271 ss.;
L. KONG, *Data protection and transborder data flow in the European and global context*, in *European Journal of International Law*, 2010, p. 441 ss.;
T. KONSTANDINIDES, *Analysis and reflections: wavering between centres of gravity: comment on Ireland v. Parliament and Council,* in *European Law Review*, 2010, p. 88 ss.;
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 ss.;
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", nyr*, in *European Constitutional Law Review*, 2010, p. 137 ss.;
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;
M. AILINCAI, *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 ss.
I. BROWN, *Keeping our secrets?: Designing Internet technologies for the public good*, in *European Human Rights Law Review*, 2014, n. 4, p. 369 ss.;
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 ss.;
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 ss.;
J. P. JACQUÉ, *Protection des données personnelles, internet et conflits entre droits fondamentaux devant la CJUE*, in *Revue trimestrielle de droit européen,* 2014, p. 283 ss.;
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 ss.;
E. KELSEY, *Gogle 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 ss.;
H. KRANENBORG, *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 (eds.), Oxford, 2014;
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*, in *Common Market Law Review*, 2014, p. 1789 ss.;
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, p. 569 ss.