Dipartimento di Giurisprudenza

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Dottorato in Discipline giuridiche

CORSO DI DOTTORATO DI RICERCA IN

DISCIPLINE GIURIDICHE

CURRICULUM

DISCIPLINE PRIVATISTICHE E DIRITTO PRIVATO PER L'EUROPA

CICLO DEL CORSO DI DOTTORATO

XXXI CICLO

Titolo della tesi

LA "NUOVA" *PRIVACY* DEL LAVORO ED I CONTROLLI AZIENDALI

Nome e Cognome del dottorando:

Andrea Ippoliti

Docente Guida/Tutor:

Prof. Giampiero Proia

Coordinatore:

Prof. Giuseppe Grisi

LA "NUOVA" *PRIVACY* DEL LAVORO ED I CONTROLLI AZIENDALI

CAPITOLO I

L'EVOLUZIONE NORMATIVA DELLA TUTELA DELLA *PRIVACY*

CAPITOLO II

I NUOVI CONTROLLI DIFENSIVI

CAPITOLO III

I CONTROLLI SUGLI STRUMENTI DI LAVORO E L'UTILIZZABILITÀ DEI DATI

CAPITOLO I

L'EVOLUZIONE NORMATIVA DELLA TUTELA DELLA *PRIVACY*

1.1 Il diritto alla riservatezza nella Costituzione

Il diritto alla riservatezza dei dati personali, oggi comunemente inteso come diritto alla *privacy*, ha avuto una propria "sede normativa" soltanto a partire dalla metà degli anni 90, ovvero con la Direttiva 95/46/Ce (c.d. Direttiva madre), recepita in Italia con la legge n. 675/1996.

Tale *corpus* normativo, che avrebbe dovuto essere il punto di riferimento per la disciplina della *privacy* per gli anni successivi, non aveva introdotto per la prima volta nell'ordinamento italiano il diritto alla *privacy*, che a ben vedere, trovava il proprio fondamento giuridico già nella Carta Costituzionale stessa, dal combinato disposto di alcuni articoli.

Ed infatti, la Corte di Cassazione negli anni '70[1], interrogandosi sull'esistenza in Italia di un "diritto alla riservatezza" ne ha trovato il fondamento all'interno dell'art. 2 Cost. relativamente ai diritti inviolabili dell'uomo, affermandone l'esistenza quale "*autonomo diritto soggettivo tra i diritti della personalità"*.

A ben vedere, il diritto alla *privacy* non poteva che trovare la propria base giuridica costituzionale all'interno dell'art. 2 Cost. inteso

[1] Cass. Civ., 27 maggio 1975, n. 2129.
A ben vedere tale sentenza oltre a individuare nell'art. 2 Cost. il fondamento giuridico costituzionale del diritto alla riservatezza, compie una ricostruzione giuridica del quadro normativo costituzionale ed internazionale del diritto alla *privacy*, richiamando gli art. 3, 13, 14, 15, 27, 29 e 41 Cost., nonché la dichiarazione universale sui diritti dell'uomo del 10 dicembre 1948, l'artt. 8 e 10 della Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali del 4 novembre 1950 ed il Patto internazionale relativo ai diritti civili e politici del 16 dicembre 1966.

come norma "aperta" idonea a consentire alla Carta Costituzionale di adattarsi nel tempo all'evolvere dei "nuovi" valori e delle "nuove questioni" poste dal mutare della società senza dover procedere al complesso *iter* di revisione costituzionale per darvi un fondamento nella norma fondamentale[2]. L'apertura dell'art. 2 Cost. a "nuovi" diritti[3], come ad esempio il diritto alla *privacy*, è ritenuto possibile poiché tale norma, piuttosto che affermare la tutela di un diritto o un valore, eleva la persona umana all'interno delle gerarchie dei valori giuridici costituzionali stabilendone la priorità rispetto agli altri[4].

Il legame intrinseco del diritto della *privacy* con la persona umana assume una chiara evidenza nel momento in cui si prova a definire il diritto alla riservatezza dei propri dati. La *privacy* può così definirsi come il diritto a che le informazioni personali più intime non sia comunicate a terzi o diffuse[5]. Un diritto che evidenza la "*necessità addirittura biologica dell'uomo*"[6] a mantenere uno spazio proprio, riservato, nella società in cui si colloca per sua natura in quanto "animale sociale".

In buona sostanza, la collocazione "naturale" dell'uomo è in un gruppo, ma ad esso deve appartenere il diritto inviolabile di sottrarre a tale gruppo una parte della propria sfera personale, rendendola sfera giuridica privata. Ed infatti, tale diritto ha una duplice accezione: una positiva ed una negativa.

---

[2] Ed infatti, in moltissime occasioni in cui la Corte Costituzionale ha dovuto pronunciarsi su "nuove questioni" afferenti ai diritti fondamentali della persona, essa ha fatto riferimento all'art. 2 Cost per elevarli a valori di rango costituzionale.
[3] R. BIFULCO, A. CELOTTO, M. OLIVETTI, *Commentario alla Costituzione*, vol. I, Torino, UTET 2006.
[4] A. GHIRIBELLI, *Il diritto alla privacy nella Costituzione italiana*, in *Teutas* (sito istituzionale – *www.teutas,it*), 30 novembre 2007.
[5] T. A. AULETTA, *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978.
[6] A. CATAUDELLA, *Scritti giuridici*, Padova, Cedam, 1991.

L'accezione positiva consente al soggetto titolare del diritto di *privacy* di controllare i propri dati e le proprie informazioni[7] che sempre di più con la *"New Economy"*[8] sono diventati dei beni giuridici molto rilevanti anche dal punto di vista patrimoniale[9], ma soprattutto di disporne[10], dal momento che, salvo particolari casi[11], la *privacy* è un diritto disponibile.

L'accezione negativa invece attribuisce il diritto alla persona di tenere i terzi al di fuori della propria sfera privata e di evitare quindi illegittime intromissioni nella propria riservatezza.

Ovviamente, il rapporto tra accezione negativa e positiva del diritto alla riservatezza definisce la *privacy* stessa ed è un rapporto dinamico[12] che si adatta al cambiamento della società; ad esempio è evidente che oggi, sempre di più, si riservi maggiore rilevanza all'aspetto positivo di tale diritto rispetto al passato, dal momento che nell'odierna "società della condivisione" dei *social network* e dei sistemi informatici è anche molto più semplice disporre dei propri dati personali.

---

[7] S. RODOTA', *Intervista su privacy e libertà*, Bari, Laterza, 2005.

[8] Con tale termine deve intendersi la nascita e diffusione di una nuova economia grazie all'introduzione di nuove tecnologie che determinano dei cambiamenti rilevanti a livello economico e sociale con un incremento della ricchezza, dello sviluppo sociale, della produttività e trasformazione degli stili di vita.

[9] Si pensi a tal proposito ai grandi flussi di dati personali che "viaggiano" tramite pacchetti di dati nella rete e che vengono venduti, molto spesso dopo essere profilati, per finalità commerciali o di altro tipo senza alcun arricchimento da parte del legittimo titolare al quale deve essere sempre garantita la libera disposizione dei propri dati, sebbene appunto tramite i sistemi informatici la "disponibilità" del dato viene resa sempre più difficile.

[10] Si ritiene la *privacy* un diritto così disponibile al punto da teorizzarne un sistema di pagamento alla cui base ci sarebbero proprio i dati personali come moneta: il c.d. "*Data Dollar"* ovvero una forma di pagamento che prevede lo scambio di beni e servizi per informazioni personali; nel Regno Unito già oggi esistono dei negozi fisici che utilizzano esclusivamente tale forma di pagamento, ma ciò non è nulla di diverso da quanto già oggi avviene su piattaforme *online* che per far utilizzare dei servizi gratuiti richiedono la disposizione dei dati personali, rendendo accessibili alcune informazioni personali come controprestazione del servizio "gratuito".

[11] Fattispecie in cui il titolare dei dati non è in grado di prestare liberamente il consenso alla disposizione dei dati per un particolare stato psico-fisico o a causa di una situazione di pericolo.

[12] A. TROJSI, *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli, Torino, 2013

Chiarita l'inclusione del diritto alla *privacy* tra i diritti fondamentali di cui all'art. 2 Cost., va rilevato come sia necessario richiamare anche l'art. 3 Cost. con particolare riferimento all'uguaglianza sostanziale. Tale norma, affermando il dovere dello Stato di rimuovere gli ostacoli che possono impedire il pieno sviluppo della persona, di fatto, si impegna alla tutela della *privacy* dell'individuo dal momento che, come evidenziato pocanzi, la *privacy* rientra tra i diritti inviolabili dell'uomo e solo assicurando a tutti una sfera privata libera e inviolabile lo Stato rende i cittadini veramente uguali tra loro.

Oltre agli articoli 2-3 Cost. di carattere generale, la Carta Costituzionale tutela la riservatezza della persona, e quindi il diritto alla *privacy* in specifici contesti e fattispecie che hanno consentito di teorizzare il diritto alla riservatezza dei dati personali.

In primo luogo, rientra in tali norme l'art. 13 Cost. in cui si afferma l'inviolabilità della libertà personale nella quale va ricompresa sicuramente la libera disposizione della propria sfera privata, da intendersi anche come libertà negativa di impedire l'intromissione di altri nella propria riservatezza, il c.d. "*right to be alone"* di matrice statunitense[13].

In secondo luogo, gli artt. 14-15 Cost. si riferiscono a due fattispecie ancora più specifiche, ovvero l'inviolabilità del domicilio e la libertà e segretezza dei mezzi di comunicazione. In entrambe le norme assume valore costituzionale il diritto di escludere i terzi dal proprio domicilio e dalle proprie comunicazioni, sancendo in due ipotesi specifiche e distinte, l'esistenza di un diritto alla riservatezza dell'individuo legato al luogo (domicilio) oppure al mezzo di

[13] S. WARREN e L. BRANDEIS, *The Right to privacy*, Harvard Law Review, 1890.

comunicazione (posta o corrispondenza) e quindi al messaggio in esso contenuto.

L'inviolabilità del domicilio o della segretezza del mezzo di comunicazione però non sono valori assoluti dal momento che la stessa Carta Costituzionale ai commi successivi dei medesimi articoli citati stabilisce che, in alcuni casi previsti dalla legge, il diritto alla riservatezza può essere compresso in favore dell'interesse pubblico.

L'accordare maggior tutela all'interesse pubblico rispetto alla *privacy* è il primo bilanciamento di valori che viene compiuto a livello normativo in ordine al diritto alla riservatezza dei dati personali che, come si vedrà, viene sempre contrapposto ad un altro interesse comunque meritevole di tutela.

A ben vedere infatti, il rapporto tra il diritto alla *privacy* e l'interesse che gli si contrappone di volta in volta definisce il livello di tutela che un ordinamento riconosce in un dato momento storico alla riservatezza dei dati personali.

Dal punto di vista giuslavoristico, la norma fondamentale in tema di impresa è l'art. 41 Cost. nel quale viene elevata a valore di rango costituzionale l'iniziativa economica privata anche per il particolare valore sociale che ha nel nostro ordinamento. Anche con riferimento alla libertà di iniziativa economica però, la norma fondamentale non attribuisce un valore assoluto, ma stabilisce che deve essere compiuto un bilanciamento con altri valori costituzionali ovvero la sicurezza, la libertà e la dignità umana.

Ovviamente, il richiamo alla dignità umana, che non può essere compressa dall'iniziativa economica, determina la base primaria per la

tutela della *privacy* nel rapporto di lavoro[14] dal momento che, come è già evidenziato, il diritto riservatezza personale rientra tra i diritti inviolabili della persona umana tutelati dall'art. 2 Cost. In tale norma assume chiaramente rilievo quella che è l'essenza del diritto alla *privacy* ovvero il bilanciamento tra valori: viene assicurata la libertà di iniziativa economica, ma entro il limite invalicabile della dignità della persona e quindi del lavoratore.

Poiché la norma fondamentale tutela l'iniziativa economica (art. 41 Cost.) e al successivo art. 42 Cost. la proprietà privata (quindi anche la proprietà dei beni aziendali), l'imprenditore-datore di lavoro ha il proprio diritto costituzionalmente garantito di preservare la propria attività ed i beni aziendali anche con controlli sui lavoratori, che però non devono valicare il limite dell'inviolabilità della dignità della forza lavoro. Tale bilanciamento tra diritto alla dignità della persona – quindi anche diritto alla *privacy* – e libertà d'impresa ha generato la disciplina giuslavoristica sulla *privacy*, la quale accorda maggior tutela ad una piuttosto che ad un'altra in ragione della peculiarità della fattispecie che si presenta, in applicazione dei principi generali vigenti in materia.

Prima di soffermarsi sull'impianto normativo più specifico della *privacy* nel rapporto di lavoro, va rilevato come il riconoscimento del diritto alla riservatezza dei dati personali all'interno della Costituzione Italiana avvenga anche indirettamente dal combinato disposto degli artt. 10-11 Cost. ed alcuni trattati internazionali. Ed infatti, in tali articoli l'ordinamento italiano riconosce valore costituzionale di matrice

[14] E. BARRACO, A. SITZIA*, La tutela della privacy nei rapporti di lavoro*, in *Monografie di diritto del lavoro*, dirette da M. MISCIONE, Milano, Ipsoa, 2008.

internazionale sia a norme di origine pattizia sia ad atti di provenienza comunitaria.

A tal proposito, un primo esempio è costituito dalla Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (4 novembre 1950), ove all'art. 8 viene tutelato il diritto al rispetto della vita familiare e privata[15]. Ed ancora, la Convenzione internazionale sui diritti civili e politici (16 dicembre 1966), in cui all'art. 17 si prevede un divieto generalizzato di interferenza, tra le altre cose, nella vita privata, familiare, nel domicilio e nella corrispondenza[16] oppure la Carta dei diritti fondamentali dell'Unione Europea c.d. Carta di Nizza (18 dicembre 2000), recepita all'interno del Trattato di Lisbona e quindi tra le fonti primarie del diritto dell'Unione Europea, che afferma anch'essa all'art. 7 il diritto alla riservatezza dell'individuo in generale ed in particolare nel domicilio e nelle comunicazioni[17].

[15] Convenzione per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali, 4 novembre 1950 – Art. 8: "*Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza.*
Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute e della morale, o alla protezione dei diritti e delle libertà altrui".

[16] Convenzione internazionale sui diritti civili e politici (16 dicembre 1966) - Art. 17: "*Nessuno può essere sottoposto ad interferenze arbitrarie o illegittime nella sua vita privata, nella sua famiglia, nella sua casa o nella sua corrispondenza, né a illegittime offese al suo onore e alla sua reputazione.*
Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze od offese".

[17] Carta dei diritti fondamentali dell'Unione Europea c.d. Carta di Nizza del 18 dicembre 2000 – Art. 7: "*Ogni individuo ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e delle sue comunicazioni*".

1.2 L'impianto normativo dello Statuto dei lavoratori

La legge n. 300 del 1970 c.d. Statuto dei lavoratori si caratterizza per essere il primo *corpus* giuridico a riconoscere un nucleo irriducibile di tutele ai lavoratori nei confronti del datore di lavoro nell'intento proprio della disciplina giuslavoristica di equilibrare le posizioni di disparità economica in cui si trovano naturalmente datore e prestatore di lavoro.

Con l'entrata in vigore dello Statuto dei lavoratori, "*al potere direttivo del datore di lavoro è stato posto un limite, di carattere esterno, ed assistito da sanzione penale, consistente nel divieto di indagini sulle opinioni politiche religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore"*[18]. Il potere "naturale" del datore di lavoro è stato così giuridicamente arginato dettagliatamente al fine di rendere inviolabile in aspetti più concreti del rapporto di lavoro la dignità della persona-lavoratore, così come sancito in astratto ed a livello generale dalle norme costituzionali[19]. In questo modo il diritto del lavoro passa dalla tutela del "contraente debole" alla tutela del lavoratore "persona"[20].

Relativamente alla riservatezza del lavoratore, rimangono legittimamente conoscibili dal datore di lavoro solo le informazioni personali strettamente collegate con l'oggetto del contratto di lavoro, che

[18] A. SITZIA, *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova CEDAM, 2013, pag. 10.

[19] Va rilevato infatti, come l'intento del Legislatore dello Statuto dei lavoratori non fosse quello di attribuire "nuovi" diritti ai lavoratori, ma riconoscere anche in ambito lavorativo quei diritti che la Costituzione riserva a livello generale. Nella relazione al disegno di legge infatti viene evidenziato come con tale impianto normativo si voglia assicurare "*l'effettivo godimento di taluni diritti e libertà fondamentali che, pur trovando nella Costituzione una disciplina e una garanzia complete sul piano dei principi, si prestano tuttavia, in carenza di disposizioni precise di attuazione, ad essere compressi nel loro libero esercizio*". La *ratio* dello Statuto dei lavoratori è quindi quella di disciplinare in concreto e puntualmente le libertà ed i diritti dei lavoratori al fine di rendere possibile in concreto la loro attuazione e pieno esercizio.

[20] M. GRANDI, *Persona e contratto di lavoro. Riflessioni storico critiche sul lavoro come oggetto del contratto di lavoro*, in *Arg. dir. lav*., 1999, 309.

si rendono indispensabili per lo svolgimento del rapporto[21]. In questo modo viene così introdotto per la prima volta il concetto di proporzionalità del trattamento del dato personale, che giustifica la compressione o l'apertura della sfera privata del lavoratore, soltanto quando ciò si renda indispensabile.

La tutela della riservatezza nel rapporto di lavoro si realizza pertanto attraverso la sottrazione di alcune aree di verificabilità da parte del datore di lavoro, assegnando al diritto alla *privacy* "*natura di vero e proprio diritto indisponibile in tutti i casi in cui si supera la soglia di ciò che è legittimamente verificabile e/o conoscibile*"[22]. Il potere di controllo del datore di lavoro in tal modo non viene soppresso, bensì regolato nelle sue modalità e nel suo oggetto "*al fine esclusivo di tutelare la dignità del lavoratore e di depurare l'attività di vigilanza dagli aspetti più odiosi, subdoli e polizieschi*"[23].

Nonostante siano quasi passati 50 anni dall'entrata in vigore dello Statuto dei lavoratori, esso rappresentata ancora il fondamento delle garanzie rivolte alla persona del lavoratore, realizzate tramite la "positivizzazione" di divieti al potere del datore di lavoro[24]. Ed infatti, se da un lato la legge n. 300 del '70 nel tempo si è dimostrata insufficiente ed inidonea a garantire adeguatamente la protezione della liberà e dignità umana, in particolare in tutte le aree del rapporto di lavoro caratterizzate da forte innovazione tecnologica, dall'altro costituisce ancora oggi il punto

[21] P. ICHINO, *Il contratto di lavoro*, in *Trattato di diritto civile e commerciale*, Tomo III, Milano, Giuffrè, 2003.
[22] P. CHIECO, *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*, Bari, Cacucci, 2000, pag. 12.
[23] F. TOFFOLETTO, *Nuove tecnologie informatiche e tutela del lavoratore*, Milano, 2006, pag. 5.
[24] A. BELLAVISTA, *Sorveglianza, privacy e rapporto di lavoro*, in *Dir. internet*, 5, 2006.

di riferimento e di partenza della disciplina della *privacy* nel rapporto di lavoro[25].

Le prime due norme relative alla riservatezza dei lavoratori nello Statuto dei lavoratori sono gli artt. 2-3 che disciplinano rispettivamente l'uso di guardie giurate e personale di vigilanza da parte del datore di lavoro.

Alle guardie giurate viene assegnato esclusivamente lo scopo di tutelare i beni aziendali senza alcuna ingerenza nel controllo dei lavoratori (salvo contestazioni relative alla tutela dei beni aziendali[26]), al punto che le stesse non possono recarsi nei luoghi dove i lavoratori svolgono la propria prestazione lavorativa, se non per particolari esigenze di tutela dei beni aziendali stessi.

Il personale di vigilanza invece viene incaricato del controllo dell'attività lavorativa a differenza delle guardie giurate. L'art. 3 dello Statuto però richiede, ai fini della legittimità del controllo, che i nominativi e le mansioni del personale di vigilanza siano resi noti ai lavoratori interessati, per evitare forme di controllo occulto ritenuto lesivo della dignità del lavoratore-persona. Il controllo del personale di vigilanza pertanto è un controllo palese che si pone in contrasto ed in antitesi con i compiti di vigilanza affidati al personale non inserito nel ciclo produttivo aziendale e non conosciuto dai prestatori di lavoro[27].

Nella rassegna delle norme dello Statuto dei lavoratori relative alla *privacy,* l'art. 4 assume sicuramente ruolo centrale oggi più che in passato.

---

[25] M. NAPOLI, *Lo Statuto dei lavoratori ha quarant'anni, ben portati*, in *Lav. dir.*, 2010.

[26] Le contestazioni compiute da parte delle guardie giurate però hanno carattere peculiare, dal momento che non possono essere considerate in senso stretto "contestazioni disciplinari", dal momento che le guardie giurate per tali "contestazioni" non devono rispettare neppure la procedura prevista dall'art. 7 della legge n. 300 del 1970, cfr. Cass., 17 gennaio 1990 n. 205, in Dir. prat. lav., 1990, p. 838.

[27] A. VALLEBONA, *Istituzioni di diritto del lavoro. Il rapporto di lavoro*, Padova, Cedam, 2012

Tale norma disciplina l'uso di impianti audiovisivi per finalità di controllo, pertanto, a differenza dell'art. 3, che disciplina il controllo tramite personale a ciò preposto, regola i controlli tecnologici realizzati a distanza, ossia quelli che per l'elevato grado di informatizzazione e sviluppo tecnico raggiunto sono gli strumenti più utilizzati ed idonei a realizzare un controllo totalizzante.

Al di là della rubrica dell'art. 4 (impianti audiovisivi), che inevitabilmente soffre quasi 50 anni di vigenza della norma (oggi sostituita da impianti audiovisivi e altri strumenti di controllo), tale articolo si riferisce a tutti gli strumenti di controllo a distanza che la tecnica ha prodotto. La redazione dell'art. 4 come norma aperta, ossia idonea a recepire le novità tecnologiche in materia di controlli a distanza ("*altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori*") ne ha consentito la "sopravvivenza" nel testo originario sino al 2015, quando si è resa necessaria la modifica legislativa di cui al D.Lgs. n. 151/2015, che riformulando il vecchio testo ha risolto il problema pratico e non teorizzabile dal legislatore del '70 dei mezzi di lavoro che diventano anche mezzi di controllo.

L'art. 4 al momento della sua prima formulazione[28], nell'affrontare il problema del monitoraggio ininterrotto del comportamento, "*aveva*

[28] Art. 4. (Impianti audiovisivi) – testo originario:
"È vietato l'uso di impianti audiovisivi e di altre apparecchiature per finalità di controllo a distanza dell'attività dei lavoratori.
Gli impianti e le apparecchiature di controllo che siano richiesti da esigenze organizzative e produttive ovvero dalla sicurezza del lavoro, ma dai quali derivi anche la possibilità' di controllo a distanza dell'attività dei lavoratori, possono essere installati soltanto previo accordo con le rappresentanze sindacali aziendali, oppure, in mancanza di queste, con la commissione interna. In difetto di accordo, su istanza del datore di lavoro, provvede l'Ispettorato del lavoro, dettando, ove occorra, le modalità per l'uso di tali impianti.
Per gli impianti e le apparecchiature esistenti, che rispondano alle caratteristiche di cui al secondo comma del presente articolo, in mancanza di accordo con le rappresentanze sindacali aziendali o con la commissione interna, l'Ispettorato del lavoro provvede entro un anno dall'entrata in vigore della presente legge, dettando all'occorrenza le prescrizioni per l'adeguamento e le modalità di uso degli impianti suddetti.

avvertito molto chiaramente il rischio di una possibile lesione della dignità e della riservatezza del lavoratore subordinato, eventualità da far evidentemente prevalere sull'esigenza di controllo dell'imprenditore"[29]. Il legislatore del '70 al momento del bilanciamento tra riservatezza del lavoratore ed esigenza di controllo del datore di lavoro, almeno limitatamente a questo tipo di controlli, scelse di favorire il lavoratore sancendo il divieto di controlli a distanza, salvo prevedere, in subordine, per alcune esigenze, delle ipotesi di utilizzo comunque eccezionali e possibili solo al termine di una procedura di garanzia svolta con le rappresentanze sindacali, con le commissioni interne o infine con l'ispettorato del lavoro. Ed infatti, la *ratio* originaria dell'art. 4, così come emerse chiaramente all'interno dei lavori della Commissione preparatoria allo Statuto dei lavoratori, era quella di circoscrivere il poter di controllo del datore di lavoro, legittimandolo in casi specifici e soltanto quanto esso non era tale da minacciare gravemente i diritti alla dignità e alla riservatezza dei lavoratori[30]. In tale quadro il legislatore del '70 necessariamente riservò solo a casi eccezionali l'impiego delle nuove tecnologie ai fini di monitoraggio dei lavoratori dal momento esse ritenute fortemente invasive ed ignote.

Il sospetto nutrito dal legislatore nei confronti di tali strumenti, al punto da stabilirne un divieto generale (salvo ipotesi particolari di utilizzo), è dovuto al fatto che nell'art. 4 il bene protetto è il lavoratore-

Contro i provvedimenti dell'Ispettorato del lavoro, di cui ai precedenti secondo e terzo comma, il datore di lavoro, le rappresentanze sindacali aziendali o, in mancanza di queste, la commissione interna, oppure i sindacati dei lavoratori di cui al successivo art. 19 possono ricorrere, entro 30 giorni dalla comunicazione del provvedimento, al Ministro per il lavoro e la previdenza sociale".

[29] A. LEVI, *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli, 2013.

[30] R. DE LUCA TAMAJO, *Nuove tecnologie e tutela della riservatezza dei lavoratori*, F. Angeli, 1988.

persona, mentre negli artt. 2-3 il bene protetto è soltanto la prestazione lavorativa[31].

In tale quadro normativo vi potevano essere due tipi di controlli: (i) quelli in cui le apparecchiature sono destinate unicamente al controllo a distanza dell'attività del lavoratore e (ii) quelli in cui gli strumenti di controllo vengono installati per esigenze organizzative, produttive o per la sicurezza sul lavoro. I primi dovevano considerarsi sempre vietati, mancando un'esigenza meritevole di tutela per legittimare il controllo, mentre i secondi, in quanto il controllo dell'attività del lavoratore non era la ragione dell'installazione né l'oggetto di verifica degli stessi, erano consentiti, ma solo previo accordo con la parte sindacale oppure con l'autorizzazione dell'ispettorato del lavoro[32].

L'accordo con la compagine sindacale, oppure l'autorizzazione della parte amministrativa è condizione di liceità per l'esercizio del potere di controllo[33] e, una volta raggiunto, vincola tutti i lavoratori alle dipendenze del datore di lavoro, poiché procedimentalizza il potere di lavoro del datore[34].

Pertanto, il controllo a distanza nel quadro normativo pre-*Jobs Act* è considerato da utilizzare come *extrema ratio* soltanto "*quando esso sia indispensabile, vale a dire quando non esista altra possibilità, meno*

[31] E. BARRACO, *La tutela della privacy: la riservatezza del lavoratore*, in *Diritto e Pratica del Lavoro*, 19/2018.
[32] La procedura di garanzia dell'installazione delle apparecchiature nel luogo di lavoro deve essere sempre seguita anche quanto astrattamente tali impianti non sono idonei astrattamente neanche indirettamente al controllo dell'attività dei lavoratori, in quanto secondo la giurisprudenza "*la potenzialità di controllo a distanza deve ritenersi innata negli impianti audiovisivi, ragion per cui la norma dell'art. 4 comma 2 l. n. 300 del 1970, deve essere applicata a prescindere dalla prova della concreta idoneità dell'impianto al controllo dei posti di lavoro*" (Cass. 16 settembre 1997, n.9211).
[33] B. VENEZIANI, *Sub art. 4, in Lo Statuto dei lavoratori*, Commentario diretto da G. Giugni, Milano, 1979.
[34] La violazione della procedura dell'art. 4 SL determina l'applicazione di una sanzione penale che riguarda non solo il datore di lavoro bensì anche gli addetti alle apparecchiature di controllo.

restrittiva per la libertà e dignità del lavoratore, per realizzare uno scopo del datore ritenuto nel caso concreto meritevole di tutela"[35].

Alla luce di quanto sopra, risulta che il legislatore del '70 attraverso l'art. 4 ha manifestato la diffidenza verso un'utilizzazione indiscriminata dei prodotti tecnologici, maggiormente pericolosi per la libertà e la dignità dei lavoratori, decidendo così di limitarli e consentirli soltanto in ipotesi necessarie e giustificate[36].

Nell'impresa 2.0[37] così come definita da McAfee, gli strumenti informatici sono sempre più protagonisti dell'attività lavorativa e nel tempo, da possibili strumenti di controllo sono divenuti prima strumenti di lavoro ed oggi, in alcun casi, l'automazione ha consentito che essi diventassero dei "lavoratori" automatizzati perfettamente sostituibili alla persona fisica lavoratore.

E' evidente che in tale contesto storico-sociale, il bilanciamento di valori compiuto dall'art. 4 SL doveva essere rivisto poiché ritenuto sempre più obsoleto "*sia da parte di chi ha più a cuore la posizione dei lavoratori, e rimarca come esso possa rivelarsi inadeguato ad aggredire efficacemente tutte le potenzialità lesive delle nuove tecnologie, sia da parte di chi è più sensibile alle ragioni imprenditoriali, e paventa che le sue rigidità possano rallentare o impedire l'utilizzazione in chiave produttiva dell'innovazione tecnologica*"[38]. Pertanto sulla base di tale contesto socio-normativo si è resa necessaria la modifica normativa di cui al D.Lgs. n. 151 del 2015.

---

[35] A. BELLAVISTA, *I poteri dell'imprenditore e la privacy del lavoratore*, in *Il diritto del lavoro*, fasc. 3, 2002.
[36] A. BELLAVISTA*, Il controllo sui lavoratori*, Torino, Giappichelli, 1995.
[37] A. MCAFEE, *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*,
Harvard Business Review Press, 2009.
[38] L. GAETA*, La dignità del lavoratore e i turbamenti dell'innovazione* in *Lav. Dir*., 203, 1990.

L'art. 4 dello Statuto, nella nuova formulazione[39], continua a consentire l'installazione di impianti audiovisivi e di altri strumenti di controllo a distanza soltanto per ragioni specifiche ((i)esigenze organizzative e produttive, (ii) sicurezza del lavoro, circostanze alle quali viene aggiunta l'esigenza di (iii) tutela del patrimonio aziendale) e comunque previo accordo con le rappresentanze aziendali o unitarie oppure in assenza di accordo con l'autorizzazione della sede territoriale dell'ispettorato nazionale del lavoro.

La grande novità normativa però è la previsione del II comma del medesimo articolo secondo cui l'accordo sindacale o "*l'iter* autorizzativo" non è necessario per "*gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze*". In questo modo l'art. 4 dello Statuto trova un nuovo equilibrio nel bilanciamento tra la riservatezza del lavoratore e l'esigenza di controllo del datore di lavoro rispetto alla vecchia formulazione normativa. Ed infatti, gli strumenti informatici non vengono più visti dal legislatore come strumento di controllo indiretto della prestazione, bensì

[39] Art. 4. (Impianti audiovisivi e altri strumenti di controllo) – nuova formulazione:
"*Gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori possono essere impiegati esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e possono essere installati previo accordo collettivo stipulato dalla rappresentanza sindacale unitaria o dalle rappresentanze sindacali aziendali. In alternativa, nel caso di imprese con unità produttive ubicate in diverse province della stessa regione ovvero in più regioni, tale accordo può essere stipulato dalle associazioni sindacali comparativamente più rappresentative sul piano nazionale. In mancanza di accordo, gli impianti e gli strumenti di cui al primo periodo possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro o, in alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, della sede centrale dell'Ispettorato nazionale del lavoro. I provvedimenti di cui al terzo periodo sono definitivi.*
La disposizione di cui al comma 1 non si applica agli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze. Le informazioni raccolte ai sensi dei commi 1 e 2 sono utilizzabili a tutti i fini connessi al rapporto di lavoro a condizione che sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196".

come strumento di lavoro, che pertanto attiene alla prestazione lavorativa e non più alla persona-lavoratore e quindi controllabile, in quanto bene aziendale che il datore di lavoro mette a disposizione del lavoratore per rendere la propria prestazione.

L'erosione della riservatezza del lavoratore in favore del controllo degli strumenti di lavoro da parte del datore di lavoro non è stata però indiscriminata. Ed infatti, per la prima volta nell'ordinamento giuridico italiano, in una norma giuslavoristica al III comma, è stato introdotto un richiamo alla disciplina generale di tutela alla *privacy* contemperando così dal punto di vista della forma del controllo la compressione della sfera privata cui è stata sottoposta la sfera privata del lavoratore su questo tipo di controlli. In ogni caso, si vedrà più diffusamente del tema sul capitolo seguente.

Riprendendo il testo dello Statuto dei lavoratori le altre norme relative alla tutela della riservatezza del lavoratore all'interno dell'azienda sono gli artt. 5-6 e 8.

L'art 5 dello Statuto disciplina i controlli sanitari stabilendo il divieto di controlli diretti del datore di lavoro sui propri dipendenti. A differenza dello schema dell'art. 4 statutario, il divieto ai controlli sanitari diretti non ammette eccezioni che consentano il controllo diretto al datore di lavoro. Ed infatti, nei due commi successivi sono indicati i soggetti abilitati a svolgere tale tipo di controlli, ma tra essi non è mai incluso il datore di lavoro.

I soggetti ritenuti idonei a svolgere i controlli sanitari sono quindi i servizi ispettivi degli istituti previdenziali, enti pubblici ed istituti specializzati di diritto pubblico. La ragione del divieto di controllo da parte del datore di lavoro e la conseguente possibilità di controllo soltanto a

particolari soggetti abilitati vede la propria *ratio* sia dalla necessità dell'imparzialità dell'accertamento sanitario, ma anche nella tutela della riservatezza del lavoratore con particolare riferimento al suo stato di salute. Ciò non significa che il datore di lavoro non possa valutare il contenuto della documentazione medica risultante dagli accertamenti medici eseguiti dai predetti soggetti, né che egli stesso possa richiederli, rispettando la cornice normativa dell'art. 5 in esame, che impone di rivolgersi soltanto ad alcuni soggetti abilitati.

Pertanto, nel rispetto della norma in questione è comunque consentito al datore di lavoro di verificare indirettamente lo stato di salute del lavoratore e prendere conoscenza dei suoi comportamenti persino quando essi sono estranei allo svolgimento dell'attività lavorativa, ma rilevanti dal punto di vista del corretto adempimento della propria prestazione lavorativa oppure, in caso di lavoratore in stato di malattia, non gli consentano il recupero della propria integrità psico-fisica o ne rallentino i tempi[40].

L'art. 6 dello Statuto invece si occupa delle visite personali di controllo, ovvero le verifiche che investono direttamente il lavoratore-persona al fine di tutelare il patrimonio aziendale, senza andare ad indagare lo stato di salute del lavoratore. Anche in questa forma di controlli risulta il bilanciamento operato dal legislatore[41] tra valori di pari rilevanza costituzionale quale il diritto alla riservatezza del lavoratore (art. 2 Cost.) e l'interesse del datore di lavoro al corretto andamento della propria attività imprenditoriale, soprattutto attraverso la tutela del proprio

[40] Cass. 19 settembre 2017, n. 21667; Cass. 2 dicembre 2016, n. 24671; Cass. 18 gennaio 2018, n. 1173.
[41] L. MONTUSCHI, *Potere disciplinare e rapporto di lavoro*, Milano, Giuffré, 1973.

patrimonio aziendale (artt. 41-42 Cost.)[42]. Ed infatti, se da un lato è consentito il controllo del lavoratore da parte del datore di lavoro, le verifiche possono avvenire soltanto previo consenso del prestatore d'opera che, laddove si rifiuti ingiustificatamente, è esposto alla responsabilità disciplinare, sino ad arrivare ai casi estremi di configurazione della giusta causa di licenziamento[43].

Pertanto, ove vi siano ragioni giustificatrici e venga rispettata la cautela dell'effettuazione delle verifiche all'uscita dei luoghi di lavoro, salvaguardando la dignità e la riservatezza del lavoratore, le visite personali possono essere legittimamente svolte da parte del datore di lavoro[44]. L'indispensabilità del controllo è la *condicio sine qua non* per l'effettuazione di tale tipo di controlli. Così come per i controlli a distanza, la norma stabilisce che le ipotesi nonché le modalità in cui le visite potranno essere effettuate siano determinate tramite accordo con le rappresentanze sindacali aziendali oppure con la commissione interna ed ancora, in assenza di accordo, su istanza del datore di lavoro, provveda l'Ispettorato del lavoro.

Il bilanciamento operato dal legislatore in favore del controllo datoriale rispetto alla persona-lavoratore, però non arriva al punto di consentire anche il controllo dei beni personali poiché da una interpretazione letterale della norma in esame la disciplina statutaria sembra riferirsi soltanto alle ispezioni corporali. Anche nel controllo in

---

[42] Sulla correttezza del bilanciamento tra valori costituzionali si è pronunciata la Corte Costituzionale con la sentenza n. 99 del 25 giugno 1980, rilevando come l'art. 6 SL sia un norma regolatrice dei rapporti tra datore di lavoro e lavoratori, concorrendo a disciplinare l'attività collettiva dei facenti parte dell'organizzazione aziendale per dare un carattere impersonale alle visite salvaguardando la serenità e tranquillità dell'ambiente di lavoro per proteggere i beni aziendali, ma anche quelli personali degli stessi lavoratori.

[43] Pretura Milano, 2 gennaio 1996, in Lav. Giur., 1996.

[44] L. TEBANO, *Le visite di controllo "in uscita" nel diritto vivente*, in *Diritto Lavori e Mercati*, 2010, 3.

esame la disciplina statutaria, così come per gli altri controlli esaminati, prevede in caso di violazione della forma di controllo o delle ipotesi in cui esso sarebbe stato utilizzabile la sanzione penale[45], assistita dall'inutilizzabilità delle risultanze acquisite ad ogni fine, anche disciplinare.

Un altro articolo specifico dello Statuto dei Lavoratori è riservato alla tutela della libertà di pensiero dei lavoratori: si tratta dell'articolo 8. Tale norma può essere considerata la declinazione giuslavoristica dell'art. 21 Cost. tutelando la libertà di pensiero della persona anche quando essa assume le vesti di prestatore di lavoro all'interno di una realtà aziendale.

Il potere di controllo nelle "mani del datore di lavoro" è fisiologicamente funzionale all'esercizio del potere direttivo che, come tale, può essere rivolto soltanto alla prestazione lavorativa. Pertanto il datore di lavoro ha il diritto nei confronti del lavoratore di vedere eseguita la prestazione lavorativa, ma ciò non può consentirgli di indagare sulle opinioni della propria forza lavoro poiché non collegate allo svolgimento del rapporto di lavoro, neanche indirettamente[46].

La possibilità di controllo sulle opinioni del prestatore di lavoro "*anche su fatti concernenti la vita privata del lavoratore è legittima solo quando abbiamo una immediata e diretta correlazione con le mansioni dedotte o deducibili in contratto*"[47].

[45] La sanzione penale è quella prevista dall'art. 38 del medesimo Statuto dei Lavoratori, così come già analizzato per gli artt. 2 e 5 della L. n. 300/1970.
[46] Ciò non può dirsi invece per le organizzazioni di tendenza ove le opinioni ed i convincimenti personali investono necessariamente anche l'esecuzione della prestazione lavorativa, rendendole quindi controllabili da parte del datore di lavoro e tale da configurare in casi estremi persino il c.d. "licenziamento ideologico".
[47] A. BELLAVISTA, *Dignità e riservatezza*, in P. Lambertucci (a cura di), *Dizionari del diritto privato. Diritto del lavoro*, Milano, Giuffré, 2010

L'art. 8 dello Statuto tutela il lavoratore non solo nella fase del rapporto ma anche nella costituzione dello stesso. Ed infatti, l'indagine datoriale non può investire la sfera personale del lavoratore neanche nella fase di selezione[48], che anch'essa deve essere mirata alla valutazione della capacità professionale del lavoratore e la sua idoneità a rendere correttamente la propria prestazione lavorativa.

Tale impianto normativo di tutela della riservatezza del lavoratore nei diversi ambiti che possono essere minacciati nel normale svolgimento del rapporto di lavoro è a sua volta garantito da una norma di chiusura ossia dall'art. 38 dello Statuto dei Lavoratori, il quale rende penalmente rilevanti le condotte del datore di lavoro che viola gli articoli 2, 4-6, 8, 15 dello Statuto stesso.

[48] G. AMOROSO, V. DI CERBO e A. MARESCA, *Diritto del lavoro vol. 1, sub art. 8*, Milano, Giuffré, 2013.

1.3 Dalla direttiva UE 95/46 al D.Lgs. n. 196/03 c.d. "*codice della privacy*"

Se da un lato nello Statuto dei lavoratori si trova la traccia di una "primordiale" disciplina di tutela della *privacy* nell'ambito del rapporto di lavoro, l'introduzione a livello generale di una normativa di protezione dei dati personali nel nostro ordinamento è tardata ad arrivare.

A livello europeo il principale punto di riferimento in materia di protezione dei dati personali è stata la Convenzione per la protezione delle persone in relazione all'elaborazione automatica dei dati a carattere personale del Consiglio d'Europa del 1981, che ha delineato per la prima volta i principi cardine del trattamento legittimo[49] e una prima chiara individuazione di categorie speciali di dati[50].

Successivamente sono stati emanati due strumenti di *soft law,* quindi non vincolanti, caratterizzati da "*un'eminente importanza pratica, giacché entrambe contemplano l'uso di tali strumenti internazionali come mezzi per superare il persistente gap regolativo*"[51] quali la Raccomandazione n. R(89)2 del Consiglio d'Europa sull'uso dei dati personali nel rapporto di lavoro e il *Code of practice on the protection of workers' personal data*, adottato dall'Organizzazione Internazionale del lavoro (OIL) nel novembre 1996.

[49] All'interno di tale Convenzione si afferma che i dati devono essere (i) ottenuti ed elaborati legalmente, (ii) registrati per fini determinati e legittimi, (iii) adeguati, pertinenti e non eccessivi in rapporto alla finalità di raccolta, (iv) esatti ed aggiornati e (v) conservati per un periodo non superiore a quello necessario.

[50] Tali categorie speciali di dati diventeranno poi i c.d. dati sensibili. Esse si riferivano a dati personali idonei a rivelare l'origine razziale, le opinioni politiche, le convinzioni religiose o di altro genere, nonché dei dati relativi alla salute, alla vita sessuale e riguardanti la vita sessuale.

[51] S. SIMITIS, *Reconsidering the premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data*, in *European Law Journal*, 1999.

La raccomandazione R(89)2 aveva l'obiettivo di fornire un quadro di principi ai nuovi problemi nei luoghi di lavoro posti dal crescente impiego delle tecnologie, cercando di porre un vincolo di trasparenza alle sconfinate possibilità di intrusione ed elaborazione dei dati proprie delle nuove tecnologie[52]. Facendo propri i principi della Convenzione del 1981, la Raccomandazione specifica che per evitare la perdita del controllo delle proprie informazioni da parte dei lavoratori in favore dei sistemi di automazione, i dati vadano raccolti direttamente presso il soggetto interessato e, quando sia necessario acquisire i dati direttamente da terzi, gli interessati debbano comunque essere informati.

Il *Code* dell'OIL invece prevede un maggior coinvolgimento della compagine sindacale nella gestione della *privacy* in azienda, che dovrebbe essere consultata almeno per l'introduzione e la modificazione dei sistemi automatizzati di trattamento dei dati personali dei lavoratori, prima dell'introduzione di qualsiasi forma di monitoraggio o controllo elettronico sul lavoratore ed infine per la predisposizione dei questionari e test relativi ai dati personali dei prestatori di lavoro[53].

L'atto di impulso per la predisposizione del primo testo normativo italiano in tema di *privacy* è però dell'Unione Europea con la direttiva 95/46 CE recepita in Italia attraverso la legge n. 675/1996. La legge italiana non ha aggiunto nulla alla direttiva europea (che dovrebbe contenere soltanto principi e non norme di dettaglio), ma si limitava

[52] H. NISSENBAUM, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

[53] In sostanza, le linee direttive del Codice dell'OIL escludono il monitoraggio diretto e continuo del lavoratore, potendo essere eccezionalmente ammesso per esigenze di tutela della salute o sicurezza ed eseguito comunque nel rispetto delle regole di trasparenza e di consultazione con le rappresentanze sindacali. A ben vedere quindi, le linee del *Code of practice* dell'OIL convergono sulle direttive interpretative fornite dal Garante per la protezione dei dati personali e dalla giurisprudenza relativamente all'art. 4 dello Statuto dei lavoratori.

soltanto a recepirne il contenuto con un atto di diritto interno[54], disciplinando così la protezione dei dati personali delle persone fisiche e la circolazione di tali dati ed approvando contemporaneamente la legge n. 676/1996, recante la delega al Governo per l'emanazione di disposizioni integrative e correttive della legislazione in tema di *privacy*[55].

Un grande elemento di novità di tale disciplina, senza soffermarsi su aspetti non strettamente collegati al diritto del lavoro, è certamente l'istituzione di un'autorità di controllo in ogni Stato membro con il compito di assumere il ruolo di garanti della novella normativa sulla protezione dei dati personali. Come si vedrà, tali autorità indipendenti, oltre a costituire un canale alternativo all'autorità giudiziaria tendenzialmente più celere dove azionare i propri diritti in materia di protezione dei dati personali, si caratterizzano per grande capacità ermeneutica ed indirizzo in merito alla materia della *privacy*, fornendo molto spesso delle linee guida o degli indirizzi autorevoli[56] agli operatori del settore ed a volte al legislatore stesso.

[54] Tale mera ricezione da parte dello Stato Italiano senza alcuna modifica o apporto proprio alla disciplina comunitaria è dovuta al fatto che la L. n. 675/96 venne emanata il 31 dicembre 1996, ovvero l'ultimo giorno utile per l'attuazione della Direttiva con un atto interno da parte dello Stato membro per scongiurare l'applicazione da parte dell'UE della sanzione dell'esclusione dei benefici legati agli accordi Schengen per la libera circolazione delle persone.

[55] Si pensi che nell'esercizio di tale delega sono stati emanati numerosi decreti legislativi:
(i) D.Lgs. 9 maggio 1997, n. 123; (ii) D.Lgs. 28 luglio 1997, n. 255 – notificazioni dei trattamenti; (iii) D.Lgs. 8 maggio 1998, n. 135; (iv) D.Lgs. 13 maggio 1998 n. 171 – disposizioni in materia di vita privata nel settore delle telecomunicazioni ed in tema di attività giornalistica; (v) il D.Lgs. 6 novembre 1998, n. 389; (vi) il D.Lgs. 26 febbraio 1999, n. 51 – personale dell'ufficio del Garante; (vii) D.Lgs. 11 maggio 1999, n. 135; (viii) D.Lgs. 30 luglio 1999, n. 281 – trattamento dati personali per finalità storiche, statistiche e ricerca scientifica; (ix) D.Lgs. 30 luglio 1999, n. 282 – riservatezza dati personali in ambito sanitario; D.Lgs. 28 dicembre 2001, n. 467.

[56] Alcuni esempi in materia di *privacy* nel rapporto di lavoro sono costituiti dalle (i) linee guida sulla videosorveglianza del 29 novembre 2000, (ii) linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati del 23 novembre 2006, (iii) linee guida per la posta elettronica e internet del 1° marzo 2007 solo per citarne alcune.

Ad esempio, in tema di rapporto di lavoro, il Garante ha affermato che il consenso è "vincolato" in quanto, quando i trattamenti vengono effettuati dal datore di lavoro nel rispetto dei principi di legge, il consenso del lavoratore non è altro che la manifestazione della generale lealtà e correttezza che deve improntare i comportamenti delle parti contrattuali[57].

Con riferimento al rapporto di lavoro, il Garante per la protezione dei dati personali è intervenuto più volte per assicurare un maggior grado di tutela della riservatezza dei lavoratori, oppure per semplificare le procedure da attivare da parte dei datori di lavoro.

Ad esempio, il Garante ha emanato numerose autorizzazioni generali[58] al trattamento per i datori di lavoro, al fine di evitargli gli obblighi di notificazione o altri oneri formali per ogni trattamento dei dati dei propri dipendenti.

La prima autorizzazione rilasciata dal Garante per la protezione dei dati personali ha riguardato il trattamento dei dati sensibili nel rapporto di lavoro[59] ed è stata emanata con "*l'intento di facilitarne la gestione da parte dei datori relativamente al trattamento dei dati dei propri dipendenti*

[57] Garante per la protezione dei dati personali in *Dir. Prat. Lav*., 1999, pag. 3133. In particolare, il Garante precisa che il consenso del lavoratore è "dovuto" soltanto entro i limiti della gestione del rapporto di lavoro, mentre qualora i trattamenti richiesti eccedessero tale cornice operativa, non solo sarebbe giustificabile il rifiuto al consenso, ma la richiesta da parte del datore di lavoro sarebbe persino tale violare la normativa sulla protezione dei dati personali laddove subordini la conclusione del contratto al consenso del lavoratore, oppure venga anche solo minacciato l'uso del potere disciplinare.

[58] Le autorizzazioni generali sono il mezzo attraverso il quale il Garante permette il trattamento di dati sensibili o giudiziari a determinate condizioni, per determinati fini, e per certe categorie di titolari. Pertanto, l'autorizzazione costituisce una condizione di liceità del trattamento che rilascia il Garante dopo valutazione di pericolosità così acconsentendolo.

[59] Autorizzazione n. 1/99 al trattamento dei dati sensibili nei rapporti di lavoro. Seguita poi in altri ambiti dalla autorizzazione n. 2/99 al trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale; autorizzazione n. 3/99 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni; autorizzazione n. 4/99 al trattamento dei dati sensibili da parte dei liberi professionisti; autorizzazione n. 5/99 al trattamento dei dati sensibili da parte di diverse categorie di titolari; autorizzazione n. 6/99 al trattamento di dati sensibili da parte degli Investigatori privati; autorizzazione n. 7/99 al trattamento dei dati a carattere giudiziario da parte di privati, di enti pubblici economici e di soggetti pubblici.

necessario ad adempiere (o per esigere l'adempimento di) specifici obblighi posti dalla legge interna e comunitaria, da regolamenti o da contratti collettivi anche aziendali – specie se a fini retributivi, fiscali, previdenziali e assistenziali -, oppure dalla normativa in materia di igiene e sicurezza del lavoro, di tutela della salute, di ordine e di sicurezza pubblica"[60].

La legge n. 675/96 non contempla però alcuna previsione specifica per la tutela della riservatezza dei lavoratori né un coordinamento con la disciplina giuslavoristica in generale. A ben vedere l'unico riferimento, comunque marginale, si trova nell'art. 43, nel quale dopo aver previsto l'abrogazione delle disposizioni di legge o regolamentari in contrasto con la nuova normativa, vengono confermate le disposizioni della legge n. 300/1970[61]. Tale previsione apparentemente senza alcuna portata innovativa, afferma invece la compatibilità delle norme statutarie con il nuovo impianto normativo della disciplina di protezione dei dati personali; la L. n. 675/96 appare così "*compatibile con la con la contestuale vigenza e applicabilità della l. n. 300 e delle altre disposizioni che stabiliscono regole specificamente indirizzate nell'area del lavoro e sindacale*"[62]

Alla legge n. 675/96, emanata più per il rispetto degli accordi di Schengen che per disciplinare concretamente la materia della *privacy*, sono seguiti nel tempo molti interventi disorganici[63] da parte del

---

[60] C. TACCONI, *La disciplina della privacy e la tutela del lavoratore*, in V. CUFFARO R. D'ORAZIO V. RICCIUTO (a cura di), *Il codice di trattamento dei dati personali*, Torino, Giappichelli, 2007.

[61] Art. 43, II comma, L. n. 675/96: "*Restano ferme le disposizioni della legge 20 maggio 1970 n. 300, e successive modificazioni […]. Restano altresì ferme le disposizioni di legge che stabiliscono divieti o limiti più restrittivi in materia di trattamento di taluni dati*".

[62] G. BUTTARELLI, *Banche dati e tutela della riservatezza, La privacy nella società dell'informazione*. *Commento analitico alle Leggi 31 dicembre 1996 n. 675 e 676*, Milano, Giuffré, 1997.

[63] Oltre ai decreti attuativi della L. n. 676/96 già citati, si pensi al D.P.R. n. 318/99, oppure il D.P.R. n. 501/98.

legislatore italiano che hanno fatto venire meno la presenza di un unico testo legislativo di riferimento per la tutela della *privacy*[64].

Tale contesto normativo ha richiesto l'esigenza di un *corpus* normativo unitario che potesse contenere in un atto di riferimento l'intera disciplina per la riservatezza dei dati personali. Il nuovo testo di riferimento "*avrebbe costituito lo strumento più adatto a compiere il necessario ripensamento della disciplina, a realizzare l'auspicato obiettivo di norme di complessiva regolazione della materia, mettendo a posto i dati sparsi qua e là nelle varie fonti regolatrici, contribuendo così a rendere la normativa più unitaria, organica e, soprattutto, sistematica, e facendo ordine in un campo nel quale anche l'esperto faticava ormai a ritrovarsi*"[65].

E' per rispondere a tale esigenza che è stato emanato il D.Lgs. n. 196/2003, il c.d. "Codice della *privacy*". Senza procedere ad un'analisi della normativa di carattere generale, va rilevato come il principio che permea l'intera disciplina in esame sia quello della centralità dell'informativa sulle finalità e le modalità di gestione dei dati personali e del conseguente necessario consenso libero ed autodeterminato[66]. Il trattamento dei dati, per essere lecito, deve inoltre avvenire previo consenso dell'interessato e secondo la finalità precisa per cui il consenso è stato conferito; i dati trattati devono essere esatti, pertinenti, completi e conservati per un periodo non superiore a quanto necessario per raggiungere la finalità del trattamento (c.d. principio di necessità).

---

[64] F. CARDARELLI, S. SICA, V. ZENO-ZENCOVICH*, Il codice dei dati personali - temi e problemi*, Milano, Giuffrè, 2004.
[65] A. TROJSI, *op. cit.*
[66] AA. VV., *La nuova disciplina della privacy*, commentario diretto da S. SICA E P. STANZIONE, Bologna, Zanichelli, 2004;

Dal punto di vista giuslavoristico, il codice della *privacy* riserva un intero titolo (Titolo VIII – Lavoro e previdenza sociale) alla protezione dei dati personali in ambito lavorativo, ciononostante nessuna delle norme in esso contenute stabilisce una disciplina dettagliata e puntuale della tutela della riservatezza nel rapporto di lavoro.

Ed infatti, esse si riferiscono a "*codici di deontologia e di buona condotta"* (art. 111) per il trattamento dei dati per finalità previdenziali o per la gestione dei rapporti di lavoro, oppure l'inclusione tra le finalità di interesse pubblico di rapporti di lavoro, o altre forme di impiego in presenza di particolari circostanze ed esigenze (art. 112) ed ancora specifiche norme relative alla riservatezza nel telelavoro o nel lavoro domestico[67] (art. 115) oppure nell'attività degli istituti di patronato o assistenza sociale[68] (art. 116). Gli artt. 113-114 invece creano un rinvio[69] rispettivamente ai fini del divieto di indagine sulle opinioni dei lavoratori e sui controlli a distanza agli artt. 8 e 4 dello Statuto dei lavoratori[70]. Tale normativa richiamando per specifiche ipotesi la disciplina dello Statuto dei lavoratori, lascia intendere che oltre a mantenere il sistema previgente in ipotesi ben individuate e già disciplinate compiutamente (artt. 4 e 8 L. n. 300/70), al rapporto di lavoro si aggiungono le nuove prescrizioni previste

[67] La dottrina ha ipotizzato che in tale articolo con la previsione del lavoro domestico in luogo del lavoro a domicilio, il legislatore sia incorso in un errore terminologico dal momento che la presenza nella stessa norma del telelavoro fa intendere che ci si riferisca al lavoro a domicilio che non è altro che una delle modalità di svolgimento del telelavoro, diversamente al lavoro domestico che riguarda invece la prestazione resa nell'abitazione del datore di lavoro e relativa ai servizi di carattere domestico per la vita familiare.

[68] Rispetto alla precedente normativa in materia (art. 12 L. n. 152/2001) viene precisato che l'accesso alle banche di dati degli enti eroganti le prestazioni può avere luogo soltanto relativamente a tipi di dati individuati dall'interessato mediante l'espressione del proprio consenso.

[69] Art. 113 del D.Lgs. n. 196/03: "*Resta fermo quanto disposto dall'art. 8 della legge 20 maggio 1970 n. 300.*"
Art. 114 del D.Lgs. n. 196/03: "*Resta fermo quanto disposto dall'art. 4 della legge 20 maggio 1970 n. 300.*"

[70] In realtà la versione pubblicata degli artt. 113-114 è diversa da quella contenuta nella bozza di decreto legislativo che invece riproduceva integralmente gli articoli statutari.

in generale dal D.Lgs. n. 196/03, creando un sistema di grande tutela per il lavoratore a fronte di maggiori oneri per i datori di lavoro. In tal modo i principi generali propri del Codice della *privacy* diventano degli elementi di immediata portata precettiva, idonei a modificare ed incidere concretamente e specificamente all'interno delle dinamiche aziendali.

In un siffatto quadro normativo "duplice", sia nella fonte normativa (Statuto dei lavoratori e Codice della *privacy*) che dal punto di vista "giudiziario" (autorità giudiziaria "tradizionale" ed Autorità Garante per la protezione dei dati personali), per realizzare un controllo legittimo, è quindi necessario il rispetto sia delle norme statutarie che dei principi generali del D.Lgs. n. 196/03.

Secondo parte della dottrina[71] il titolo del codice della *privacy* relativo a lavoro e previdenza sociale è però oscuro ed ambiguo al punto da non comprendersi le ragioni per il richiamo all'interno del D.Lgs. n. 196/03 soltanto di alcune disposizioni giuslavoristiche, né un eventuale criterio selettivo utilizzato per includere alcune piuttosto che altre. Secondo tale parte della dottrina il titolo in esame del codice della *privacy* "*risulta persino fuorviante, per chi, in questo caso, non abbia adeguata dimestichezza con il diritto del lavoro: perché, ponendo, in risalto soltanto poche disposizione del complesso sistema normativo in materia, non dà la dimensione della capillarità della disciplina del regime giuridico delle informazioni dei lavoratori, contenuta invece appunto in una miriade di disposizioni sparse qua e là nei provvedimenti normativi più disparati, e spesso celate all'interno dei provvedimenti destinati ad altro*"[72].

[71] A. TROJSI, *op. cit.*
[72] A. TROJSI, *op. cit.*

Pertanto, nonostante un titolo specifico sul lavoro e la previdenza sociale, l'apporto innovativo del *corpus* normativo del 2003, anche in ambito giuslavoristico, risiede quasi esclusivamente nella parte generale. La tutela del codice della *privacy*, tramite l'applicazione dei principi generali, è una tutela più formale rispetto alle norme giuslavoristiche che invece riguardano "l'oggetto" della conoscenza datoriale, distinguendo fino a che punto può spingersi l'indagine del datore di lavoro e quali informazioni può acquisire tramite gli strumenti di controllo.

La parte generale del codice della *privacy*, invece, è principalmente diretta a disciplinare le modalità di raccolta e di trattamento dei dati, ergendo la forma del controllo al medesimo livello di tutela che fin tale momento era riservata al merito.

La maggior tutela approntata anche per i lavoratori dal D.Lgs. n. 196/03 è garantita da un proprio apparato sanzionatorio costituito principalmente da quattro tipi di sanzioni: (i) divieto di utilizzo dei dati personali trattati in modo illegittimo[73]; (ii) tutela risarcitoria specifica[74]; (iii) sanzioni amministrative[75]; (iv) sanzioni penali[76].

La normativa comunitaria non ha terminato però l'impulso legislativo in tema di riservatezza dei dati personali con la direttiva 95/46, ma ha continuato la sua opera in materia con altre direttive, in particolare sul tema delle nuove tecnologie. Ed infatti, nella nostra società dell'informazione, la società della "quarta rivoluzione industriale" ogni nuova tecnologia è idonea ad essere diffusa immediatamente e su larga

[73] Art. 11, II comma, D.Lgs. n. 196/03: "*i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati*".
[74] Art. 15, D.Lgs. n. 196/03: "*Chiunque cagiona danno ad altri per effetto del trattamento dei dati personali è tenuto al risarcimento ai sensi dell'articolo 2050 del codice civile. Il danno non patrimoniale è risarcibile anche in caso di violazione dell'art. 11*".
[75] Titolo III - Capo I – Violazioni amministrative artt. 161-166.
[76] Titolo III – Capo II – Illeciti penali artt. 167-172.

scala ed è sempre più capace astrattamente di intromettersi nella sfera privata dell'individuo e raccogliere informazioni.

Per ovviare al problema di questa capacità di intrusione delle nuove tecnologie, il legislatore europeo ha preferito emanare singole direttive per le specifiche fattispecie. Emblematiche in tal senso sono le Direttive n. 2006/24 per individuare (o renderlo rintracciabile tramite le c.d. "tracce elettroniche"), anche in rete, un titolare del trattamento dei dati e renderlo responsabile nei confronti degli interessati e n. 2009/140, altrimenti nota come *cookies law* che in ambito di *software* di profilazione a fini commerciali ed operativi ha introdotto l'obbligo del consenso per l'installazione di questi strumenti sul dispositivo dell'interessato, mentre prima di tale normativa esso avveniva in automatico e senza possibilità di controllo, se non postumo.

1.4 Le linee guida del Garante per la protezione dei dati personali

La difficoltà nel disciplinare settori specifici da parte del D.Lgs. n. 196/03 ha generato la necessità da parte del Garante per la protezione dei dati personali di intervenire tramite atti di controversa portata normativa[77] per declinare i principi generali contenuti nella parte generale del Codice della *privacy* all'interno di fattispecie specifiche ed in ambiti che richiedono una disciplina più puntale o perché particolarmente idonei a ledere la riservatezza personale o perché sono il frutto dell'evoluzione tecnica e non erano stato presi in esame da legislatore del 2003.

Il Garante interviene in tale ambito attraverso le sue decisioni che però prendono le mosse da fattispecie particolari o in generale tramite le c.d. "linee guida", che invece forniscono delle indicazioni di carattere generale sul corretto trattamento dei dati in ambiti specifici al fine di garantire l'applicazione dei principi del Codice della *privacy*[78].

A ben vedere però quella che potrebbe sembrare una mera attività interpretativa, dal momento che le "linee guida" che, anche a livello terminologico, dovrebbero soltanto indirizzare l'interprete, può assumere

[77] La dottrina è divisa sul riconoscergli portata normativa o solo interpretativa.

[78] Ad esempio di seguito si riportano le più recenti tra le linee guida emanate da parte del Garante per la protezione dei dati personali: (i) Linee guida in materia di Dossier sanitario del 4 giugno 2015; (ii) Linee guida in materia di trattamento di dati personali per profilazione on line del 19 marzo 2015; (iii) Linee guida in materia di riconoscimento biometrico e firma grafometrica del 12 novembre 2014; (iv) Linee guida in materia di trattamento di dati personali, contenuti anche in atti e documenti amministrativi, effettuato per finalità di pubblicità e trasparenza sul web da soggetti pubblici e da altri enti obbligati del 15 maggio 2014; (v) Linee guida in materia di attività promozionale e contrasto allo spam del 4 luglio 2013; (vi) Linee guida in materia di attuazione della disciplina sulla comunicazione delle violazioni di dati personali del 26 luglio 2012; (vii) Linee guida in materia di trattamento di dati personali per finalità di pubblicazione e diffusione nei siti web esclusivamente dedicati alla salute del 25 gennaio 2012; (viii) Linee guida in materia di trattamento di dati per lo svolgimento di indagini di *customer satisfaction* in ambito sanitario del 5 maggio 2011; (ix) Linee guida in materia di trattamento di dati personali contenuti anche in atti e documenti amministrativi, effettuato da soggetti pubblici per finalità di pubblicazione e diffusione sul web del 2 marzo 2011; (x) Linee guida in materia di trattamento di dati personali nella riproduzione di provvedimenti giurisdizionali per finalità di informazione giuridica del 2 dicembre 2010.

un valore normativo, con la portata precettiva propria di una normazione secondaria[79]. La conferma di tale ricostruzione è fornita dall'art. 154, comma I lett. c) del D.Lgs. n. 196/03[80], secondo il quale il Garante per la protezione dei dati personali può prevedere delle prescrizioni aggiuntive alla disciplina generale che si rendano necessarie[81].

Dal punto di vista giuslavoristico vi sono tre "linee guida" di notevole rilevanza: (i) Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati del 23 novembre 2006; (ii) Linee guida per posta elettronica ed internet del 1° marzo 2007; (iii) Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007.

Con le prime linee guida sopra riportate il Garante predispone una disciplina di dettaglio per indicare ai datori di lavoro gli accorgimenti e le misure più utili da adottare per la gestione del rapporto di lavoro. In ogni caso, però, il principio che permea tali linee guida è ancora una volta il principio di necessità, dal momento che si rende possibile trattare soltanto quelle informazioni "indispensabili" per poter rispettare le previsioni normative o contrattuali.

Relativamente ai dati personali di natura "sensibile" viene precisato che anche per essi si applica il principio di necessità, ossia la possibilità di raccolta del dato solo strettamente necessario per raggiungere la finalità

---

[79] Almeno relativamente alla sua sanzionabilità dinanzi al Garante per la protezione dei dati personali in sede di reclamo.

[80] Art. 154, comma I lett. c) del D.Lgs. n. 196/03: "*prescrivere anche d'ufficio ai titolari del trattamento le misure necessarie o opportune al fine di rendere il trattamento conforme alle disposizioni vigenti, ai sensi dell'articolo 143*".

[81] Sulla portata precettiva di tali provvedimenti si veda più diffusamente:
A. STANCHI, *Privacy, Le Linee Guida del Garante per Internet e posta elettronica*, in Guida Lav., n. 12/2007; ed ancora E.O. POLICELLA, *Le linee-guida del Garante sull'uso di internet e posta elettronica: conseguenze sanzionatorie*, in Lav. Giur. n. 4/2008.

del datore di lavoro compatibile con il contratto di lavoro, ma per tale categoria di dati vengono aggiunte delle cautele rafforzate in particolare in ordine alla sicurezza della modalità di conservazione. Inoltre, con le linee guida viene chiarito che sebbene il rapporto di lavoro rientri tra le ipotesi in cui il trattamento dei dati personali è possibile anche senza uno specifico consenso in virtù di un'altra base giuridica[82] legittimante il trattamento dei dati, il datore di lavoro è tenuto, prima di procedere al trattamento dei dati personali anche in tali ipotesi, a rendere comunque al

[82] La base giuridica è l'elemento che consente il trattamento legittimo dei dati personali. Il D.Lgs. n. 196/03 stabilisce in linea generale che per il trattamento dei dati personali è necessario il consenso della persona cui si riferiscono i dati, salvo prevedere all'art. 24 delle ipotesi eccezionali (esecuzione di un contratto), ovvero delle basi giuridiche, che in virtù di condizioni particolari consentono il trattamento anche in assenza del consenso dell'interessato. Art. 24 del D.Lgs. n. 196/03: "*Il consenso non è' richiesto, oltre che nei casi previsti nella Parte II, quando il trattamento: a) è necessario per adempiere ad un obbligo previsto dalla legge, da un regolamento o dalla normativa comunitaria; b) è necessario per eseguire obblighi derivanti da un contratto del quale è parte l'interessato o per adempiere, prima della conclusione del contratto, a specifiche richieste dell'interessato; c) riguarda dati provenienti da pubblici registri, elenchi, atti o documenti conoscibili da chiunque, fermi restando i limiti e le modalità che le leggi, i regolamenti o la normativa comunitaria stabiliscono per la conoscibilità e pubblicità dei dati; d) riguarda dati relativi allo svolgimento di attività' economiche, trattati nel rispetto della vigente normativa in materia di segreto aziendale e industriale; e) è necessario per la salvaguardia della vita o dell'incolumità fisica di un terzo. Se la medesima finalità riguarda l'interessato e quest'ultimo non può prestare il proprio consenso per impossibilità fisica, per incapacità di agire o per incapacità di intendere o di volere, il consenso è manifestato da chi esercita legalmente la potestà, ovvero da un prossimo congiunto, da un familiare, da un convivente o, in loro assenza, dal responsabile della struttura presso cui dimora l'interessato. Si applica la disposizione di cui all'articolo 82, comma 2; f) con esclusione della diffusione, è necessario ai fini dello svolgimento delle investigazioni difensive di cui alla legge 7 dicembre 2000, n. 397, o, comunque, per far valere o difendere un diritto in sede giudiziaria, sempre che i dati siano trattati esclusivamente per tali finalità e per il periodo strettamente necessario al loro perseguimento, nel rispetto della vigente normativa in materia di segreto aziendale e industriale; g) con esclusione della diffusione, è necessario, nei casi individuati dal Garante sulla base dei principi sanciti dalla legge, per perseguire un legittimo interesse del titolare o di un terzo destinatario dei dati, anche in riferimento all'attività di gruppi bancari e di società controllate o collegate, qualora non prevalgano i diritti e le libertà fondamentali, la dignità o un legittimo interesse dell'interessato; h) con esclusione della comunicazione all'esterno e della diffusione, è effettuato da associazioni, enti od organismi senza scopo di lucro, anche non riconosciuti, in riferimento a soggetti che hanno con essi contatti regolari o ad aderenti, per il perseguimento di scopi determinati e legittimi individuati dall'atto costitutivo, dallo statuto o dal contratto collettivo, e con modalità di utilizzo previste espressamente con determinazione resa nota agli interessati all'atto dell'informativa ai sensi dell'articolo 13; i) è necessario, in conformità ai rispettivi codici di deontologia di cui all'allegato A), per esclusivi scopi scientifici o statistici, ovvero per esclusivi scopi storici presso archivi privati dichiarati di notevole interesse storico ai sensi dell'articolo 6, comma 2, del decreto legislativo 29 ottobre 1999, n. 490, di approvazione del testo unico in materia di beni culturali e ambientali o, secondo quanto previsto dai medesimi codici, presso altri archivi privati".*

lavoratore una informativa individualizzata sebbene non vi sia appunto necessario il consenso del lavoratore al trattamento.

La portata precettiva di tale atto è dubbia, al punto che parte della dottrina[83] la ritiene soltanto una mera indicazione che non pregiudica l'applicazione di leggi o di regolamenti anche in contrasto con esso, riconoscendone comunque il grande valore ermeneutico ed operativo.

Successivamente sono state emanate le linee guida per posta elettronica ed internet del 1° marzo 2007 che, ribadendo ancora una volta i principi generali in materia di protezione dei dati personali, impongono al datore di lavoro l'onere di fornire ai propri dipendenti un'informativa specifica sulle modalità di utilizzo nel contesto aziendale della posta elettronica e di internet, includendo nella comunicazione anche le modalità dei controlli che potrebbero essere svolti[84].

Lo strumento individuato dalle Linee guida per permettere al datore di lavoro di assolvere gli adempimenti richiesti dalla normativa in materia di *privacy* nell'utilizzo di posta elettronica e internet (in generale poi di tutti gli strumenti tecnologici) da parte dei dipendenti è la "*policy* aziendale"[85].

La *policy* pertanto sarà un documento con il quale il lavoratore viene informato della "cornice d'uso" dello strumento che gli viene messo a disposizione e quali controlli possono verificarsi su di esso[86]. In ogni caso però, la *policy* di per sé non è sufficiente a liberare il datore di lavoro

[83] R. NUNIN, *Utilizzo di dati biometrici da parte del datore di lavoro: la prescrizione del garante per la privacy*, in *Lav. nella giur.*, 2007, Vol. n. 15 fasc. 2.
[84] Fermo restando in caso di controlli a distanza su tali strumenti informatici il rispetto da parte del datore di lavoro anche della procedura dell'art. 4 della L. n. 300/70.
[85] P. TULLINI, *Tecnologie informatiche in azienda: dalle Linee-guida del Garante alle applicazioni concrete*, in P. TULLINI (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, CEDAM, 2010.
[86] M. DEL CONTE, *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, in *Dir. Informatica*, vol. 23, n. 3, 2007.

da qualsiasi onere di informazione a meno che in essa vengano inseriti anche gli elementi propri della normativa generale in materia di protezione dei dati personali, che è evidentemente la soluzione preferibile[87].

Al fine di rendere il meno invasivo possibile il controllo della casella di posta elettronica aziendale e della navigazione Internet, che comunque non potrà essere un controllo sistematico da parte del datore di lavoro, il Garante indica delle buone pratiche[88] per evitare intromissioni altrimenti evitabili sui dispositivi informatici dei lavoratori, poiché, se dovesse rendersi necessario il controllo specifico, dovrebbe (o meglio doveva prima della riforma del Jobs Act del 2015) rispettare la procedura di cui all'art. 4 dello Statuto dei lavoratori. Pertanto, almeno nelle linee guida del 2007, l'indicazione operativa del Garante è quella di limitare "a monte" alcune modalità di utilizzo dei dispositivi al fine di diminuire la necessità di controlli.

Da ultimo, le Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007 seguono quanto già affermato dalle Linee guida del 2006 relative al settore privato, adattandole in parte al differente contesto del lavoro pubblico.

Il Garante rileva che il datore di lavoro pubblico così come quello privato può lecitamente trattare i dati personali dei propri dipendenti, ma solo nella misura strettamente necessaria per la gestione del rapporto di

[87] G. FAGGIOLI – A. ROZZA, *Privacy per posta elettronica e internet in azienda*, Roma, Cesi Professionale, 2008.

[88] Tra le buone pratiche vi rientrano: (i) inibizione del download dei files provenienti da siti web o caselle di posta elettronica non autorizzate; (ii) divieto di utilizzo di dispositivi esterni quali *hard disk* esterni o chiavi USB; (iii) abilitazione dell'invio di email soltanto ad alcuni domini; (iv) creazione di indirizzi di posta elettronica condivisi tra i lavoratori; (v) predisposizione di funzionalità in grado di comunicare i rifermenti di altro lavoratore durante l'assenza del titolare di una casella di posta elettronica aziendale.

lavoro, applicando anche in tale settore i principi di liceità, necessità, indispensabilità e pertinenza.

In tale settore vengono poste ancora più cautele da parte del Garante in ordine ai dati sanitari ed alle assenze per ragioni di salute. In particolare, con riferimento a quest'ultima fattispecie, il datore di lavoro in caso di assenza per malattia del proprio potrà conoscerne soltanto l'inizio e la durata della presunta infermità, senza poter invece aver accesso alla diagnosi. Laddove, anche per mero errore del lavoratore, venga offerta a giustificazione dell'assenza della documentazione attestante anche la diagnosi, il datore di lavoro pubblico, salvo casi eccezionali tassativi[89], dovrà astenersi dal loro utilizzo e richiedere al lavoratore di produrre altra documentazione senza quelle caratteristiche.

Le linee guida del Garante però non sono gli unici provvedimenti di carattere generale ad essere emanati in materia di riservatezza dei dati personali. Ed infatti, già con la Direttiva 95/46 si prevede all'art. 29 l'istituzione di un gruppo di lavoro comune composto dai rappresentanti di tutte le Autorità nazionali di vigilanza in materia di *privacy*[90] con compiti consultivi e punto di riferimento per l'emanazione di provvedimenti di carattere generale a livello comunitario nell'interpretazione della Direttiva, nonché per la promozione dell'applicazione della disciplina di tutela della *privacy*. Tale gruppo di lavoro prende il nome proprio dall'articolo che lo istituisce: *Article* 29 *Working party* o WP29 (Gruppo di lavoro art. 29).

[89] A titolo esemplificativo si veda l'art. 61 del D.P.R. n. 782/85 relativo alla malattia per il personale della Polizia di Stato.

[90] Era un organismo consultivo indipendente composto dal Garante europeo per la protezione dei dati personali, da un rappresentante della Commissione e da un rappresentante di ognuna delle autorità nazionali indipendenti in materia di *privacy*. Inoltre, tra i membri del Gruppo di lavoro veniva nominato il presidente con un mandato di due anni.

A seguito dell'entrata in vigore del Regolamento UE n. 2016/679 (GDPR[91]) il Gruppo è stato sostituito dal Consiglio (anche noto come Comitato) Europeo per la protezione dei dati (EDPB)[92], ma prima dello scioglimento ha fornito importanti indicazioni interpretative anche sul GDPR allora di prossima entrata in vigore.

In particolare, tra le ultime linee guida emanate dal WP29, vi rientrano le linee guida sul trattamento dei dati sul posto di lavoro secondo il GDPR emanate l'8 giugno 2017: *Opinion on data processing at work 2/17*. Le principali indicazioni del WP29 in merito all'applicazione dei principi generali GDPR in ambito lavorativo possono essere riassunte come di seguito:

(i) obbligo di rispettare la vita privata, la dignità e la libertà del lavoratore a prescindere dal tipo di contratto applicato comunicando ad esso in modo chiaro, semplice e completo come i suoi dati personali sono trattati; (ii) proporzionalità del trattamento dei dati ed il suo scopo[93], pertanto in caso di utilizzo da parte del dipendente di dispositivi ad uso promiscuo, al fine di impedire il monitoraggio di informazioni private, devono essere adottate misure adeguate per distinguere tra uso privato e aziendale del dispositivo; (iii) possibilità di monitoraggio della rete informativa e dei

[91] Sigla con la quale si intende comunemente il Regolamento europeo n. 2016/679 (GDPR – *General data protection regulation*).

[92] L'EPBD istituito dall'art. 68 del GDPR è composto dalla figura di vertice di ciascuna autorità indipendente nazionale oppure da un loro rappresentante e dal Garante europeo della protezione dei dati, nonché da una rappresentanza della Commissione europea che partecipa alle riunioni ma senza diritto di voto. Come già previsto per il Gruppo di lavoro dell'art. 29, i compiti dell'EPBD saranno rivolti a garantire l'applicazione uniforme del GDPR e la cooperazione tra le autorità indipendenti nazionali. Inoltre, conserverà il ruolo interpretativi già avuto dal Gruppo di lavoro dell'art. 29 tramite la pubblicazione di provvedimenti generali e linee guida di applicazione del GDPR, alle quali si affiancherà la possibilità di pronunciarsi con decisioni vincolanti sulle controversie relative al trattamento dei dati transfrontaliero.

[93] In applicazione di tale principio, ad esempio in tema di geolocalizzazione, il WP29 indica che tali dispositivi possono essere utilizzati per fini strettamente professionali e che il lavoratore dovrebbe essere autorizzato a disabilitare il dispositivo di localizzazione, se necessario.

dispositivi aziendali ad essa collegati al fine di evitare attacchi *hacker* o altri rischi informatici, senza però incorrere in controllo sistematico di ogni attività online dei dipendenti; (iv) divieto di indagine da parte del datore di lavoro sui profili social dei dipendenti se non limitatamente ai profili professionali; (v) abilitazione di spazi privati su pc o servizi cloud per consentire al dipendente anche un uso privato di tali servizi, rendendo però gli spazi al di fuori di essi controllabili in quanto strettamente professionale; (vi) consenso rafforzato del lavoratore in alcuni ambiti dal momento che la differenza di posizione tra le parti non sempre consente un consenso libero ed autodeterminato.

Al pari dell'opera ermeneutica del Garante per la protezione dei dati personali, l'attività del WP29 ed ora del EDPB ha il compito di declinare in particolare i principi generali prima della Direttiva ed ora del GDPR al fine di consentire agli operatori l'applicazione più uniforme e corretta del diritto alla *privacy* in ogni settore, incluso quello aziendale.

1.5 Il "*Jobs Act*" – le modifiche apportate dal D.Lgs. n. 151/2015

Nel capitolo precedente si è visto che, nonostante i numerosi interventi normativi di carattere transnazionale (il D.Lgs. n. 196/03 e qualche altro atto normativo emanato successivamente) la disciplina principale in materia di controlli sul luogo di lavoro e più in generale in materia di *privacy* dei lavoratori fosse ancora contenuta nella L. 300/70. Nonostante i quasi cinquanta anni di vigenza, si riteneva che tale testo fosse comunque in grado di bilanciare correttamente anche in una società informatizzata l'esigenza di controllo del datore di lavoro e la richiesta di riservatezza dei lavoratori, tranne che in relazione ai controlli a distanza nel suo art. 4 dello Statuto del quale, da più parti[94], ormai se ne richiedeva una riforma di adeguamento al nuovo contesto sociale e lavorativo, in parte per le nuove tecnologie, ma anche per l'evoluzione della normativa generale in materia di tutela della riservatezza.

Per rispondere a tale esigenza di adeguamento della normativa del '70 è intervenuto il legislatore con il D.Lgs. n. 151/2015, nell'ambito della riforma del "*Jobs Act*" (Legge n. 183/2014 che ha previsto diverse deleghe al Governo per la riforma della disciplina giuslavoristica), modificando in gran parte l'art. 4 della L. n. 300/70, realizzando un nuovo bilanciamento tra il "legittimo interesse" (al trattamento dei dati) del datore di lavoro e la "ragionevole aspettativa" di *privacy* del lavoratore[95].

In particolare, l'art. 23 del D.Lgs. n. 151/2015 ha mutato notevolmente la disciplina dei controlli a distanza generando almeno

[94] L. SERRANI, *Moderne soluzioni di registrazione audio-visiva: ambito di applicazione e limiti dell'art. 4 dello statuto dei lavoratori*, in *Dir. rel. ind*., 2010, 529; C. ZOLI, *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Riv. it. dir. lav.*, 2009; M.T. SALIMBENI, *Il controllo a distanza sull'attività dei lavoratori: la sopravvivenza dell'art. 4 sugli impianti audiovisivi*, in *Dir. lav. merc*., 2010, pp. 795 ss..

[95] G. PROIA, *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza, in Rivista Italiana di diritto del lavoro*, 2016, pag. 547 e ss.

quattro grandi novità in merito alla disciplina dei controlli a distanza: (i) eliminazione del divieto di controllo diretto; (ii) rideterminazione della disciplina dei controlli preterintenzionali con l'inclusione della categoria della tutela del patrimonio; (iii) esenzione dalla procedimentalizzazione dei controlli gli strumenti di lavoro[96] e quelli di rilevamento accessi e presenza[97]; (iv) vincolo dei dati raccolti alla disciplina *privacy* con uno specifico richiamo, pena l'inutilizzabilità dei dati acquisiti.

Da tale quadro emerge immediatamente come "*il sistema definito dal nuovo art. 4, legge n. 300/1970, da un lato destruttura e depotenzia quel quarantennale divieto di controlli a distanza dell'attività del lavoratore, dall'altro riporta il controllo a distanza nella più ampia categoria dei trattamenti dei dati personali assoggettandolo alla disciplina generale in materia di privacy*"[98].

Si passa dal ruolo del sindacato quale garante della riservatezza del lavoratore, tramite la stipulazione di un accordo sindacale, alla tutela della *privacy* del lavoratore tramite il sistema di tutela di ordine generale attinti dal codice sulla protezione dei dati personali e dal GDPR.

Procedendo con ordine all'esame delle principali novità normative introdotte dalla riforma del 2015 va rilevato come, nonostante nel nuovo testo dell'art. 4 L. n. 300/70 manchi una norma di divieto dei controlli a distanza, salvo per gli strumenti di lavoro e registro presenza, essi restano ammessi soltanto in via eccezionale in presenza di esigenze ben

[96] Definiti dalla dottrina come gli "strumenti impiegati dal lavoratore per rendere la prestazione". Si veda tra gli altri: I. ALVINO, *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour law issues*, 2/2016; R. DEL PUNTA, *La nuova disciplina dei controlli a distanza sul lavoro* (art. 23 D.Lgs. n. 151/2015), in *Ridl*, 1/2016.

[97] Rientrano in tale categoria tutti gli strumenti, ivi inclusi i badges, idonei a rilevare l'accesso e la permanenza nei luoghi di lavoro.

[98] E. BARRACO, *Strumenti di lavoro e controllo a distanza*, in *Diritto & Pratica del Lavoro*, 31/2018 pag. 1943.

specifiche, consentendo quindi il solo controllo preterintenzionale e comunque non diretto[99].

I controlli a distanza, sempre ad eccezione di quelli realizzati tramite gli strumenti di lavoro e registro presenza, ai fini della validità dovranno rispettare tre requisiti: (i) sussistenza di una delle esigenze che consentono l'impiego di strumenti di controllo a distanza, idonea anche al controllo dei lavoratori (esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale); (ii) installazione degli strumenti di controllo soltanto a seguito di accordo con il sindacato o con l'ispettorato del lavoro; (iii) rispetto delle prescrizione della normativa generale in materia di *privacy* richiamata nel nuovo III comma dell'art. 4 L. n. 300/70.

Oltre alla nuova esigenza legittimante il controllo preterintenzionale della "tutela del patrimonio aziendale", una novità attiene ai soggetti coinvolti nella procedura di installazione degli impianti. Ed infatti, per le imprese con unità produttive ubicate in diverse province oltre che dalle rappresentanze aziendali o unitarie già previsti dal vecchio testo normativo, l'accordo sindacale può essere stipulato con le associazioni sindacali comparativamente più rappresentanti sul piano nazionale.

Tale previsione consente alle grandi aziende plurilocalizzate di evitare la moltiplicazione di accordi, uno in ognuna unità produttiva, peraltro con possibili esiti diversi, bensì di concludere un unico accordo

[99] Diversamente opinando, ovvero ritenendo che con l'eliminazione del divieto del I comma del vecchio testo dell'art. 4 L. n. 300/70 sia possibile il controllo diretto dei lavoratori in presenza delle esigenze richiamate dall'art. 4, significherebbe non operare alcun bilanciamento tra interesse del datore di lavoro a verificare compiutamente la prestazione lavorativa ed il lavoratore che invece per la sua condizione di subordinazione ricerca spazi di sfera privata anche nel luogo di lavoro.

applicabile in tutti le sue sedi. Sullo stesso piano si pone la possibilità per le imprese plurilocalizzate di rivolgersi all'Ispettorato nazionale del lavoro[100] per richiedere un'unica autorizzazione all'installazione degli impianti di controllo a distanza in mancanza di un accordo con la parte sindacale.

Nello schema normativo delineato dal nuovo testo dell'art. 4 L. n. 300/70 sembra delinearsi, da un lato, nel I comma, una presunzione relativa di divieto di controllo a distanza tramite impianti audiovisivi ed altri strumenti di controllo superabile tramite la verificazione di esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e, dall'altro lato, nel II comma, una presunzione assoluta di legittimità del controllo svolto sugli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze.

Ai fini dell'applicazione del II comma dell'art. 4 L. n. 300/70 è sufficiente che il controllo riguardi uno strumento lavorativo (oppure strumenti di registrazione di accessi e presenze), ma per individuare quando ci si trovi dinanzi a tale categoria, il presunto strumento lavorativo deve essere analizzato focalizzandosi sulla funzione che riveste all'interno dell'organizzazione aziendale e non alle caratteristiche intrinseche che lo rendono o meno astrattamente uno strumento di lavoro[101]. Pertanto, uno

[100] L'ispettorato nazionale del lavoro con riferimento agli strumenti di controllo a distanza ha una funzione simile alla giurisprudenza che con i suoi precedenti condizionerà l'operato e l'interpretazione delle altre sedi territoriali, imprese e sindacati. Per le aziende plurilocalizzate avere un unico soggetto con cui relazionarsi eviterà altresì di interfacciarsi con diverse sedi territoriali che potrebbero avere orientamenti diversi tra loro tali da portare a autorizzazioni o dinieghi per la medesima questione, con ovvie conseguenze negative dal punto di vista pratico per le imprese.

[101] Sul punto è intervenuta la circolare dell'Ispettorato Nazionale del lavoro n. 2 del 7 novembre 2016 che, pronunciandosi sui sistemi di geolocalizzazione ha chiarito che sono considerabili strumenti di lavoro quei dispositivi/apparecchi/congegni che costituiscono il mezzo indispensabile al lavoratore per adempiere la prestazione lavorativa. Dello stesso avviso è il Garante per la protezione dei dati personali il quale con il provvedimento n. 138 del 16 marzo

stesso strumento, in ragione di come viene inserito nel processo produttivo aziendale può ricadere o meno nel II comma dell'art. 4 L. n. 300/70.

Nonostante la norma indichi soltanto gli "strumenti di lavoro" è chiaro che essa si riferisca agli strumenti tecnologico-informatici poiché dagli stessi deve derivare il controllo che non è invece possibile tramite i tradizionali strumenti di lavoro.

Per quanto concerne gli strumenti per la registrazione degli accessi e delle presenze, mentre nella vigenza del vecchio testo dell'art. 4 L. n. 300/70 era stata la giurisprudenza[102] a ritenere applicabile la disciplina dei controlli a distanza anche a tali strumenti, il legislatore ha superato tale problematica esentandoli dalla procedura sindacale o amministrativa.

La registrazione degli accessi e delle presenze è limitata soltanto in entrata (anche in specifiche aree piuttosto che all'ingresso aziendale) ed in uscita nei confronti del lavoratore, non potendosi ritenere sostenibile la possibilità in tempo reale della localizzazione del lavoratore anche all'interno dei locali aziendali. Una diversa interpretazione sul punto, non sarebbe "*coerente con la ratio della norma che accomuna la registrazione degli accessi a quella delle presenze, evidenziando che si tratta di due situazioni per le quali ricorre la medesima esigenza, cioè quella di acquisire un dato preciso relativo alla posizione del dipendente nel momento dell'accesso o di inizio o fine del lavoro*"[103].

Come anticipato, altro elemento di novità è l'inserimento del richiamo alla disciplina generale in materia di protezione dei dati personali

---

2017, sempre in tema di geolocalizzazione che se un dispositivo/apparecchio/congegno "*non è direttamente preordinato all'esecuzione della prestazione lavorativa,* [vi è la] *conseguente applicazione dell'art. 4, comma 1*".

[102] Tra le altre, Cass. 13 maggio 2016, n. 9904 e Cass. 17 luglio 2007, n. 15892.

[103] A. MARESCA, *Controlli tecnologici tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori, in Rivista Italiana di diritto del lavoro*, 2016, pag. 513 e ss.

all'interno del III comma dell'art. 4 L. n. 300/1970, dalla cui inosservanza discende l'inutilizzabilità dei dati acquisiti. Ed infatti, il legislatore "*prendendo atto che l'uso delle tecnologie nell'ambiente di lavoro (primo comma) e nella prestazione di lavoro (secondo comma) determina inevitabilmente la possibilità della raccolta di dati personali del lavoratore, il legislatore ha inteso distinguere l'atto in sé, della "raccolta" da quello della eventuale, successiva, "utilizzazione" dei dati raccolti, legittimando la prima e subordinando, invece, la seconda a specifiche condizioni*"[104].

Ed infatti, anche laddove il dato personale venga correttamente raccolto ai fini della sua spendibilità e della sua utilizzazione "a qualsiasi fine connesso al rapporto di lavoro", è necessario che, nel rispetto dei principi generali della normativa *privacy,* venga fornita ai lavoratori un'adeguata informazione[105] (necessaria anche per la conservazione, selezione e comunicazione dei dati personali). L'adeguata informazione esplicita il bilanciamento effettuato dal legislatore del 2015 tra interesse del datore di lavoro al trattamento ed aspettativa di *privacy* del lavoratore.

Ed infatti, fornire ai lavoratori un'"adeguata informazione" gli consente di stabilire i margini della loro aspettativa di *privacy* all'interno del luogo di lavoro, evincendo quali strumenti lavorativi nel corso dell'esecuzione della loro prestazione lavorativa sono idonei a rivelare anche dei loro dati personali. L'adeguata informazione sulle modalità di utilizzo e del controllo derivabile di uno strumento di lavoro, magari

[104] G. PROIA, *op. cit.*
[105] L'obbligo di informazione non è una duplicazione dell'informativa prevista dalla disciplina generale in materia di *privacy*, ma ha una finalità diversa e richiede un controllo più puntuale. Ed infatti, oltre ad essere un'informazione adeguata essa deve essere in grado di chiarire al lavoratore la conoscenza e le modalità attraverso le quali può essere svolto il controllo, nonché gli adempimenti che gli possono essere richiesti.

attraverso specifiche *policy* aziendali[106], impedisce al lavoratore di formare una specifica aspettativa di riservatezza legittimando così i controlli *ex ante.*

L'utilizzabilità dei dati personali acquisiti tramite controlli a distanza, era controversa[107]. In particolare, non vi era uniformità di posizioni sulla possibilità o meno di adoperare tali informazioni per sanzionare inadempimenti accertati tramite dei sistemi di controllo a distanza[108], ma con il nuovo testo e con la previsione "a tutti i fini connessi al rapporto di lavoro" potrebbe sembrare essere superato qualsiasi dubbio interpretativo in ordine alla loro spendibilità.

Pertanto, la norma giuslavoristica si limita a consentire l'utilizzabilità del dato raccolto rispettando i requisiti da lei posti, mentre le norme di tutela generale in materia di *privacy* (Codice *privacy* e GDPR) che nulla prevedono in termini di raccolta del dato in ambito lavorativo dettano la disciplina da rispettare ai fini della adoperabilità dei dati acquisiti. Pertanto, con il richiamo della normativa generale in materia di *privacy*, all'interno della norma giuslavoristica, si integrano i due sistemi assicurando la protezione della riservatezza del lavoratore persona propria della normativa generale e l'eliminazione di forme odiose e squilibrate di controllo che astrattamente sarebbero ipotizzabili per la disparità economica delle parti contrattuali del rapporto di lavoro propria della norma giuslavoristica.

---

[106] La *policy* aziendale è un insieme di norme adottate dall'azienda per regolare la condotta dei propri dipendenti in specifiche materie oppure nell'utilizzo di strumenti di lavoro (*smartphones* aziendali, PC, navigazione web e posta elettronica).

[107] M.L. VALLAURI, *E' davvero incontenibile la forza espansiva dell'art. 4 dello Statuto dei lavoratori?*, in *Orient. giur. lav*., 2008.

[108] G. DOSSI, *Controlli a distanza e legalità della prova: tra esigenze difensive del datore di lavoro e tutela della dignità del lavoratore,* in *Dir. Rel. Ind.*, 2010.

Nel quadro così delineato dal combinato disposto della norma giuslavoristica e quella di carattere generale emerge che in ambito lavorativo non sia necessario il consenso dei prestatori di lavoro ai fini del trattamento dei dati personali[109] essendo sufficiente l'adeguata informazione degli stessi, risiedendo la legittimazione al trattamento nel contratto di lavoro e la possibilità di controllo nel novellato art. 4 L. n. 300/70, che ben si coordina con la normativa *privacy* di carattere generale.

A ben vedere, non potrebbe peraltro concludersi diversamente, dal momento che il consenso per essere una valida base giuridica del trattamento dei dati non dovrebbe essere rilasciato in presenza di grandi squilibri contrattuali[110] che non garantirebbero un consenso pienamente autodeterminato[111].

Dal nuovo testo dell'art. 4 L. 300/70 emerge l'importanza anche in ambito giuslavoristico della disciplina generale *privacy*, oggi rappresentata dal GDPR e dal decreto di adeguamento del codice della *privacy* di cui si dirà più avanti, la quale, una volta raccolti i dati nelle fattispecie individuate dalle norme speciali di settore (giuslavoristico) disciplina come effettuare il trattamento anche dei dati raccolti in tale ambito.

[109] Di diverso avviso è parte della dottrina rappresentata da A. SITZIA, *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo art. 4 st. lav. e il consenso del lavoratore*, in *Labour&Law Issues,* vol. 2stanc n. 1, 2016.

[110] A tal proposito, la normativa giuslavoristica affida il ruolo di interlocutore con il datore di lavoro per consentire il trattamento dei dati per i controlli a distanza agli organismi sindacali che si reputano soggetti idonei a diminuire lo squilibrio contrattuale di partenza tra lavoratori e datore di lavoro. Il consenso dei lavoratori è necessario invece per fini non strettamente lavorativi che esulano dal confine del rapporto di lavoro, come ad esempio nel caso di comunicazione all'esterno dei dati personali dei lavoratori.

[111] G. PROIA, *op. cit.*

1.6 Il Regolamento UE n. 2016/679 (GDPR – "*General Data Protection Regulation"*)

In data 15 dicembre 2015 è stata raggiunta l'intesa sul testo del nuovo Regolamento Europeo in materia di *privacy*, d'ora in avanti, GDPR (*General Data Protection Regulation*) che avrebbe sostituito la direttiva 95/46/CE e conseguentemente, in Italia avrebbe determinato la necessità di una modifica della normativa interna di diretta attuazione della direttiva.

Successivamente, il 4 maggio 2016, è stato pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il testo del Regolamento Europeo n. 2016/679 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati. Il GDPR è così entrato in vigore il 25 maggio 2016 e, a differenza della Direttiva, ha portata generale ed è direttamente applicabile in tutti gli Stati membri. Al fine di consentire un migliore coordinamento con la normativa interna dei Paesi membri dell'UE con il GDPR è stata differita di due anni la sua applicabilità, portandola al 25 maggio 2018, anche per consentire ad imprese, pubbliche amministrazioni ed a qualsiasi altro operatore di adattarsi alle nuove prescrizioni in materia di *privacy* entro la scadenza di maggio 2018.

La scelta dell'Unione Europea di disciplinare la materia della *privacy* tramite il Regolamento, a differenza del passato ove invece era stata utilizzata la Direttiva, rappresenta la necessità di fornire ai cittadini europei ed alle imprese, che sempre più si muovono all'interno dell'Unione Europea, una regolamentazione unica e comune, non essendo più sufficienti delle linee guida indicate dalla Direttiva, dal momento che l'esperienza ha dimostrato che non in tutti gli Stati membri, a prescindere

dagli strumenti normativi utilizzati, si era riuscito a raggiungere un livello di tutela della *privacy* sufficiente[112].

Pertanto, l'esigenza di certezza giuridica, di predisposizione di diritti minimi per gli interessati[113], coordinamento e semplificazione della *privacy* anche con riferimento al trasferimento dei dati personali al di fuori dell'Unione Europea ed alla necessità di disciplinare le nuove tecnologie, ha reso indispensabile ed indifferibile l'emanazione del GDPR.

Senza voler elencare ed analizzare tutte le novità ed i tratti distintivi della nuova disciplina rispetto a quella prevista dalla Direttiva e, conseguentemente, dal Codice della *privacy*, le principali novità apportate in materia di *privacy* possono riassunte come segue:

(i) Ambito di applicazione della disciplina: il GDPR si applica sia ai trattamenti effettuati all'interno dell'UE sia all'esterno quando riguardano l'offerta di beni e servizi all'interno dell'UE oppure si riferiscono al monitoraggio ed alla profilazione di un operatore all'interno dell'UE;

(ii) Informativa: in attuazione dei principi di *privacy by design* e *privacy by default* al fine di rendere l'informativa ancora più chiara sarà preferibile far uso di icone per facilitare la comprensione delle modalità del trattamento dei propri dati e si dovrà inoltre indicare anche indirettamente la durata del trattamento stesso;

[112] In controtendenza rispetto alla *ratio* dell'emanazione del Regolamento sono le disposizioni che hanno dato la possibilità agli Stati membri di legiferare per precisare le norme generali contenute nel GDPR rischiando così di compromettere l'uniformità della disciplina comune.
[113] Il GDPR attribuisce notevoli diritti all'interessato nel corso del trattamento dei dati personali. In particolare: (i) diritto di accesso (art. 15 GDPR); (ii) diritto di rettifica e all'oblio (art. 16-17 GDPR); (iii) diritto alla limitazione del trattamento (art. 18 GDPR); (iv) diritto alla portabilità dei dati (art. 20 GDPR); (v) diritto di opposizione (art. 21 GDPR).

(iii) Diritto all'oblio: diritto dell'interessato di chiedere la cancellazione dei propri dati laddove questi non siano più necessari a realizzare la finalità del trattamento per cui erano stati raccolti;

(iv) Diritto alla portabilità: diritto dell'interessato di ricevere in un formato di uso comune e leggibile tramite dispositivo elettronico i dati personali che lo riguardano e di trasmetterli ad un altro titolare del trattamento senza impedimenti (al fine di favorire la libera circolazione dei dati personali);

(v) Consenso: il consenso dovrà essere preventivo ed espresso in maniera inequivocabile, pertanto non potranno più ritenersi idonee tutte le forme di consenso tacito;

(vi) *Data breach*: in caso di violazione della normativa *privacy*, il titolare del trattamento dovrà comunicare prontamente l'accaduto al Garante per la protezione dei dati personali e laddove tale violazione coinvolga anche delle persone, queste dovranno essere adeguatamente informate dei rischi e dei comportamenti utili da adottare per limitare conseguenze negative;

(vii) DPO – *Data Protection Officer*[114]: è una nuova figura che viene coinvolta nel trattamento dei dati personali in qualità di specialista della normativa e delle pratiche in materia *privacy* e che deve garantire "nell'interesse della norma" la corretta applicazione del GDPR.

Queste sono alcune delle principali novità che ha comportato il GDPR. Di conseguenza, dal periodo di entrata in vigore del GPDR (25 maggio 2016) sino alla sua data di applicazione (25 maggio 2018) è partita

[114] Tale figura risulta essere facoltativa o obbligatori in base al soggetto che svolge il trattamento dei dati o il tipo di attività che esso svolge. Ed infatti, la nomina di un DPO risulta essere obbligatoria nelle seguenti fattispecie: (i) trattamento dei dati personali effettuato da un'autorità pubblica o da un organismo pubblico; (ii) titolare del trattamento che svolge delle attività che per loro natura per ambito di applicazione e/o finalità richiedono il monitoraggio regolare e sistematico degli interessati su larga scala; (iii) titolare del trattamento che svolge le attività di trattamento su larga scala oppure relativo a dati personali sensibili o comunque giudiziari.

una corsa contro il tempo per rispettare gli adempimenti delle imprese e più in generali di tutti gli addetti per rendere la propria organizzazione conforme alle nuove norme.

Lo stesso processo di adattamento al GDPR è stato svolto dai datori di lavoro, i quali, nonostante il Regolamento n. 2016/679 così come la precedente Direttiva non abbia disciplinato la materia giuslavoristica rimettendola alla disciplina speciale di settore[115], devono adattare la loro struttura aziendale, i processi produttivi e la gestione del rapporto di lavoro ai nuovi principi affermati dal GDPR.

Sul punto è di grande utilità interpretativa il provvedimento n. 2/2017 emanato dal WP29[116]. Prima di procedere all'analisi dei nuovi oneri imposti al datore di lavoro dal GDPR va rilevato che tale atto normativo ha stabilito in via generale che "*i datori di lavoro nel trattare i dati dei lavoratori devono tenere ben presenti i loro diritti fondamentali, ivi incluso il diritto alla riservatezza e solo dopo individuare le basi giuridiche di tale trattamento"* che possono alternativamente distinguersi

[115] Ad esempio, l'art. 88 GDPR, fermi restando i principi generali della nuova normativa in materia di *privacy* rimette agli Stati membri la possibilità di prevedere norme che possano assicurare meglio la protezione e la libertà del trattamento dei dati personali dei lavorati:
1. Gli Stati membri possono prevedere, con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, in particolare per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro.
2. Tali norme includono misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro.
3. Ogni Stato membro notifica alla Commissione le disposizioni di legge adottate ai sensi del paragrafo 1 entro 25 maggio 2018 e comunica senza ritardo ogni successiva modifica".
[116] Come anticipato nei paragrafi precedenti è un organismo indipendente che emana provvedimenti di interpretazione della normativa in materia di *privacy*.

in "*(i)l'adempimento di obblighi derivanti da un contratto di lavoro (ad. es. finalità retributive); (ii) adempimento di obbligazioni previste dalla legge (ad es. per effettuare il conguaglio delle imposte); (iii) interesse legittimo del datore di lavoro (ad. es. miglioramento della produttività aziendale)*"[117].

Il GDPR impone al datore di lavoro (i) un maggiore onere di informazione nei confronti dei lavoratori (art. 10 GDPR – principio di trasparenza), (ii) l'implementazione delle misure di sicurezza nella gestione dei dati dei lavoratori, specie se dati sensibili (art. 32 GDPR – sicurezza del trattamento), (iii) la minimizzazione del rischio sin dal momento di avvio del trattamento dei dati (art. 25 – *privacy by default*), (iv) la predisposizione della valutazione di impatto sulla protezione dei dati[118] quando il trattamento dei dati svolto verso i lavoratori preveda l'uso di nuove tecnologie e, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, possa presentare un rischio elevato per i diritti e le libertà dei prestatori di lavoro.

Il WP29 nel provvedimento n. 2/2017, declinando il GDPR nel rapporto di lavoro, evidenzia come esso debba essere applicato anche nella prima fase di contatto tra datore di lavoro e lavoratore, ossia nella fase preassuntiva. In tale fase, il trattamento dei dati personali non può essere ritenuto legittimato dal contratto di lavoro, non essendovene ancora

[117] V. DE LUCA, E. CANNONE, A. IACOBELLIS, L. VELLA, L. PORTARO, *Privacy in azienda. La nuova disciplina dal 25 maggio 2018*, Studio Legale De Luca & Partners (a cura di), in *Guida al Lavoro* n. 17 del 20 aprile 2018.

[118] L'art. 35 del GDPR stabilisce che la valutazione di impatto *privacy* c.d. PIA (*Privacy Impact Assessment*) sia lo strumento attraverso il quale viene assicurata la trasparenza di quei trattamenti dei dati personali che in astratto possono presentare dei rischi maggiori. La redazione di tale documento impone al titolare del trattamento di operare in via preventiva, prefigurandosi e risolvendo in anticipo i possibili *data breaches* che possono avvenire nei singoli trattamenti. Ed infatti, nella redazione di tale documento dovranno essere indicati: (i) la complessiva descrizione dei trattamenti previsti e delle loro finalità; (ii) una valutazione dei rischi per i diritti e le libertà degli interessati; (iii) le misure predisposte *ex ante* per affrontare i rischi, includendo misure di sicurezza ed ogni garanzia atta a dimostrare la *compliance* con il GDPR.

alcuno, né tantomeno dal consenso del lavoratore, ma da un legittimo interesse del datore di lavoro a procedere ad una assunzione.

Nel corso del rapporto di lavoro invece, il GDPR chiarisce definitivamente come non sia necessario il consenso del lavoratore, da un lato poiché il trattamento avverrebbe in esecuzione di un contratto (altra condizione di liceità del trattamento – art. 6 GDPR) dall'altro per espressa previsione del GDPR in materia di dati sensibili in materia di diritto del lavoro[119].

Alla luce del quadro normativo delineato è evidente che in ambito di rapporto di lavoro, neanche il GDPR è riuscito, o meglio non ha voluto stabilire la disciplina completa del diritto alla riservatezza della persona che pertanto resta, almeno nel rapporto di lavoro una tutela multilivello[120] (GDPR, normativa interna, CEDU, ecc…). In ogni caso, il GDPR intervenendo in un contesto sociale fortemente informatizzato, ha cercato di porre un freno ad una raccolta ed utilizzo indiscriminato dei dati personali sempre più facili da ottenere tramite gli strumenti tecnologici, sacrificando in ambito aziendale la riservatezza del lavoratore soltanto quando strettamente necessario per i fini aziendali.

Pertanto, se da un lato il GDPR non detta una disciplina specifica in materia di *privacy* nel rapporto di lavoro, il combinato disposto dei suoi principi aggiunti alle sue norme di carattere generale sono invece in grado di comportare un notevole cambiamento nella gestione della *privacy*

[119] Art. 9 paragrafo 2, lettera b) GDPR: "*l'interessato ha prestato il proprio consenso esplicito al trattamento di tali dati personali per una o più finalità specifiche, salvo nei casi in cui il diritto dell'Unione o degli Stati membri dispone che l'interessato non possa revocare il divieto di cui al paragrafo 1*".
[120] C. OGRISEG, *GDPR and Personal Data Protection in the Employment context,* in *Labour Law Issues*, vol. 3, n. 2, 2017.

all’interno dell’azienda. Cambiamento al quale il datore di lavoro deve adattarsi con una serie di nuovi adempimenti.

1.7 Gli adempimenti del datore di lavoro nella "nuova *privacy*" aziendale

Il datore di lavoro quale soggetto principale della gestione della *privacy* e titolare dei trattamenti all'interno dell'azienda riceve una notevole responsabilizzazione (principio della *accountability*). Spetta a lui infatti l'adozione di tutti i comportamenti proattivi idonei a dimostrare la corretta e concreta adozione di misure finalizzate alla *compliance* con il GDPR nel rispetto dei principi della *privacy by default* e *privacy by design*, nonché compiendo una puntuale valutazione dei rischi inerti dei trattamenti dei dati in corso di svolgimento.

Il datore di lavoro, assicurando ai propri lavoratori la salvaguardia e la disponibilità di tutti quei diritti che il GDPR prevede per gli interessati, dovrà procedere ai nuovi numerosi adempimenti che impone la nuova disciplina, tra cui i più significativi sono:

1) analisi della situazione *privacy* sul luogo di lavoro e predisposizione di una valutazione di impatto *privacy* con la quale dimostrare la corretta progettazione dei trattamenti dei dati personali all'interno dell'azienda;

2) definizione dei ruoli dei soggetti coinvolti nel trattamento dei dati personali dal titolare del trattamento, al responsabile del trattamento sino alla nomina del responsabile della protezione dei dati personali;

3) in caso di dubbio sulla gestione del trattamento dei dati personali ricorrere alla consultazione preventiva del Garante per la protezione dei dati personali;

4) adottare misure tecniche appropriate a garantire la sicurezza dei dati personali trattati;

5) redazione del registro del trattamento dei dati (obbligatorio per imprese con almeno 250 dipendenti o che trattano dati sensibili), nel quale riportare compiutamente la descrizione dei trattamenti effettuati ed i soggetti in essi coinvolti;

6) notifica al Garante per la protezione dei dati personali di eventuali violazioni dei dati personali entro 72 dal loro verificarsi.

Come già anticipato, dal momento che il GDPR non prevede una disciplina specifica per la *privacy* nel rapporto di lavoro, al datore di lavoro non sono richiesti adempimenti particolari, oltre a quelli già previsti per la normativa nazionale, ma il rispetto delle previsioni di carattere generale le cui violazione vengono previste con relative sanzioni.

A ben vedere le sanzioni previste dal GDPR sono un altro elemento di novità in materia. Ed infatti, rispetto al passato, esse sono molto più afflittive e proporzionate al fatturato dell'impresa che vanno a colpire.

Principalmente vi sono due tipi di sanzioni: (i) sanzioni fino a € 10.000.000,00 o al 2% del fatturato aziendale per violazioni relative ad obblighi del titolare, del responsabile, dell'organismo di certificazione e dell'organismo di controllo; (ii) sanzioni fino a € 20.000.000,00 o al 4% del fatturato aziendale per violazioni che si riferiscono a diritti degli interessati e le condizioni del trattamento.

Nonostante l'afflittività di tale quadro sanzionatorio il processo di adeguamento alla "nuova *privacy*" è tutt'altro che concluso, sul punto sarà interessante valutare nelle prime pronunce delle autorità di controllo la discrezionalità con cui definiranno le sanzioni in concreto.

1.8 L'adeguamento della disciplina italiana in materia di protezione dei dati personali al GDPR – il D.Lgs. n. 101/2018

Nel paragrafo precedente si è rilevato come, nonostante la *ratio* del GDPR fosse quella di stabilire un'unica disciplina normativa in materia di *privacy* per tutti i Paesi dell'Unione Europea, il Regolamento UE n. 2016/679 abbia rimesso la possibilità di legiferare in specifici settori (incluso il rapporto di lavoro) ai singoli ordinamenti interni. Prima di legiferare negli spazi normativi lasciati dal GDPR, i singoli Stati membri però dovranno adattare la loro disciplina interna ai principi del nuovo Regolamento per evitare possibili contrasti tra atti normativi nazionali e comunitari.

A tal fine dopo 3 mesi dall'applicazione del GDPR, il legislatore italiano ha emanato il D.Lgs. n. 101 del 10 agosto 2018[121] per l'armonizzazione della legislazione italiana con la nuova normativa contenuta nel Regolamento UE n. 2016/679.

Nell'adeguamento della disciplina italiana, il legislatore doveva compiere una scelta: abrogare integralmente il D.Lgs. n. 196/03 (codice della *privacy*) che fino ad oggi aveva rappresentato il *corpus* normativo di riferimento in materia, oppure procedere ad una modificazione del D.Lgs. n. 196/03 rendendolo compatibile con il Regolamento. La scelta del legislatore è ricaduta su quest'ultima opzione, rendendo di fatto più difficile per l'interprete la ricognizione della disciplina *privacy*, contenuta in molteplici atti normativi.

[121] Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento UE n. 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati).

Ed infatti, il D.Lgs. n. 101/2018 modifica ed integra il D.Lgs. n. 196/03 "*eliminando le parti incompatibili, specificando alcuni aspetti del reg. 2016/679 e aggiungendo alcune regole non previsto allo scopo di semplificare maggiormente gli adempimenti, fermo restando che nell'eventuale incompatibilità tra le due discipline, prevarrebbe quella europea*"[122].

Senza riportare ancora una volta le novità del GDPR, va rilevato che le principali novità del D.Lgs. n. 101/2018 riguardano:

(i) la conferma del potere del Garante di emanare autorizzazioni generali per semplificare la gestione dei dati personali, anche in ambito lavorativo, che invece non erano state previste dal GDPR;

(ii) la revisione del sistema sanzionatorio;

(iii) la previsione di codici deontologici per specifiche categorie[123];

(iv) la specificazione di aspetti del GDPR relativi a dati sensibili o categorie particolari di dati;

(v) l'introduzione di una sorta di *class action* in tema di *privacy* relativamente alla quale gli interessati conferendo mandato ad un ente del terzo settore possano ricorre al Garante o all'autorità giudiziaria;

(vi) l'abrogazione delle disposizioni del codice della *privacy* in contrasto con il GDPR.

Per quanto concerne il rapporto di lavoro, il D.Lgs. n. 101/2018 individua quali sono i casi in cui vi è un interesse pubblico di cui all'art. 9

[122] P. GREMIGNI, *La normativa italiana sulla privacy si adegua a quella europea*, in *Guida al Lavoro*, n. 36/2018.
[123] La previsione dei codici deontologici con alcune differenze era già presente nel D.Lgs. n. 196/03, ma non ha mai trovato attuazione.

lett. g) che consente il trattamento di dati particolari (dati sensibili) ai fini della gestione del lavoro e della previdenza, ossia:

(i) attività di controllo e ispettive;

(ii) attività sanzionatorie e di tutela in sede amministrativa e giudiziaria;

(iii) instaurazione, gestione ed estinzione, di rapporti di lavoro di qualunque tipo, anche non retribuito o onorario, e di altre forme di impiego, materia sindacale, occupazione e collocamento obbligatorio, previdenza e assistenza, tutela delle minoranze e pari opportunità nell'ambito dei rapporti di lavoro, adempimento degli obblighi retributivi, fiscali e contabili, igiene e sicurezza del lavoro o di sicurezza o salute della popolazione, accertamento della responsabilità civile, disciplinare e contabile, attività ispettiva.

Pertanto, il D.Lgs. n. 101/2018 consente il trattamento dei dati sensibili in tutte gli aspetti del rapporto di lavoro anche quando non esiste una specifica norma di legge legittimante il trattamento di tali dati purché venga rispettato il principio di proporzionalità ed equilibrio nel trattamento (principio dell'*accountability*)[124].

Il D.Lgs. n. 101/2018 prevede altresì che i dati personali di carattere penale possano essere trattati da parte del datore di lavoro laddove vi sia una norma di legge a consentirlo, mentre non può affermarsi lo stesso negli altri casi. Ed infatti, sebbene nella vigenza della precedente normativa, in virtù delle autorizzazioni generali del Garante per la protezione dei dati personali fosse pratica frequente quella di richiedere l'acquisizione del casellario penale, nella vigenza del GDPR e del D.Lgs. n. 101/2018 non è

[124] Tale norma rende possibile ad esempio la redazione di un fascicolo personale del lavoratore per fini valutativi dove vengano indicati degli elementi utili alla valutazione (quindi connessi all'esercizio di rapporti di lavoro) quali le relazioni con i colleghi, la puntualità, la percentuale di assenze, l'uso dei *social network*.

consentito il trattamento di dati personali di carattere penale (senza una specifica ragione giustificatrice oltre alla mera instaurazione del rapporto di lavoro), almeno fino all'emanazione di una nuova autorizzazione di carattere generale da parte del Garante.

Sempre in ambito lavorativo, va segnalata un'ulteriore previsione normativa contenuta nel D.Lgs. n. 101/2018 all'art. 9 che integra il D.Lgs. n. 196/03 inserendo l'art. 111 *bis* relativo ai *curriculum vitae*. In tale previsione normativa viene stabilito che il datore di lavoro in caso di ricezione di *curricula vitae* inviati spontaneamente e finalizzati all'instaurazione di un rapporto di lavoro può trattare i dati personali ivi contenuti e posticipare l'informativa di cui all'art. 13 GDPR, così come il consenso del candidato che devono essere fornite solo al momento del primo contatto utile successivo all'invio del *curriculum vitae*.

CAPITOLO II
I NUOVI CONTROLLI DIFENSIVI

2.1. La teorizzazione dei controlli difensivi

La nuova regolamentazione in materia di *privacy* e le nuove norme giuslavoristiche introdotte sul punto (D.Lgs. n. 151/2015) hanno comportato un nuovo bilanciamento di interessi tra esigenza di riservatezza del lavoratore e interesse del datore di lavoro alla verificazione dell'adempimento della prestazione lavorativa.

A ben vedere, però, il nuovo assetto normativo è in grado di alterare le modalità pratiche-operative attraverso le quali vengono svolti i controlli sulla prestazione lavorativa, ad esempio, non rendendo più necessaria la procedura per l'installazione di mezzi di controllo a distanza di cui all'art. 4 L. n. 300/70 se i controlli sono rivolti su strumenti di lavoro, modificando la regolamentazione in merito all'utilizzabilità dei dati acquisti nei controlli attraverso l'esplicito richiamo alla disciplina in materia di *privacy* di ordine generale ed infine richiedendo una revisione della teoria dei controlli difensivi[125].

Soffermandosi in particolare sui controlli difensivi, va rilevato come sin dai primi anni di vigenza dell'art. 4 L. n. 300/70, la dottrina[126] ha elaborato un controllo distinto da quello diretto alla mera verificazione dell'adempimento della prestazione lavorativa, bensì diretto all'accertamento di comportamenti illeciti ed estranei al normale

[125] A. STANCHI, *Apparecchiature di controllo, strumenti di comunicazione elettronica e controlli difensivi del datore di lavoro*, in *Lav. giur*., 2008, vol. 16, Fasc. 4, pp. 351 ss.
[126] F. LISO, *Computer e controllo dei lavoratori*, in *Dir. lav. rel. ind*., 1986.

svolgimento della prestazione lavorativa, anche di terzi[127], che possono o mirano a ledere il patrimonio aziendale[128].

Pertanto, in tali casi, l'interesse al controllo da parte del datore di lavoro non risiede più nella corretta esecuzione della prestazione lavorativa bensì nella tutela del patrimonio aziendale e quindi del proprio di diritto di proprietà tutelato a livello costituzionale (*ex* art. 42 Cost.).

La teorizzazione dei controlli difensivi da parte della dottrina[129] ha trovato un ostacolo nella previsione dell'art. 3 dello Statuto, in quanto tale norma non consente i cosiddetti controlli occulti. È evidente però che il controllo diretto alla verificazione di un illecito da parte di un dipendente è riscontrabile soltanto laddove esso non sia conosciuto da parte del lavoratore, altrimenti esso non sarebbe più riscontrabile.

La giurisprudenza[130] e la dottrina però hanno superato tale "ostacolo normativo" ritenendo che la norma citata non preveda nel suo ambito di applicazione la verificazione di condotte illecite dei dipendenti, dal momento che la sua finalità sarebbe soltanto quella di prevenire invasione della riservatezza personale mentre i lavoratori stanno eseguendo la propria prestazione lavorativa e non compiendo un illecito.

---

[127] P. TULLINI, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, RIDL 2009, I, 323 ss.

[128] R. DE LUCA TAMAJO, *I controlli sui lavoratori*, in *i poteri del datore di lavoro nell'impresa*, G. ZILIO GRANDI (a cura di), Atti del convegno di Studi Venezia 12 aprile 2002, Padova, 2002.

[129] G. SPINELLI, *La legittimità dei controlli datoriali c.d. "difensivi": certezze apparenti in una categoria dubbia*, in *Riv. It. Dir. lav*., 2013, n. 1.

[130] In particolare, la giurisprudenza di legittimità, nelle prime pronunce favorevoli ai controlli difensivi, nel 2002 ha ritenuto che le norme statutarie, che secondo alcuni ne impedivano il compimento, non si riferissero alla fattispecie del controllo della condotta illecita del lavoratore, che, pertanto, poteva essere verificata rispettando il principio di necessità e proporzionalità (Cass. 3 aprile 2002, n. 4746). In precedenza, non erano stati ritenuti ammissibili controlli difensivi compiuti direttamente dal datore di lavoro, ma erano già stati legittimati i controlli sugli illeciti dei lavoratori attraverso gli investigatori privati, in quanto da un'interpretazione letterale degli artt. 2-3 dello Statuto dei lavoratori, tali soggetti non rientravano nel divieto stabilito da le citate norme.

Compiendo un illecito, i lavoratori interromperebbero il vincolo lavorativo venendo meno al loro dovere di correttezza e diligenza, legittimando così i controlli difensivi del datore di lavoro[131]. Tale orientamento è stato perfezionato dalla giurisprudenza di legittimità[132] che ha ridotto l'ambito dei controlli difensivi, escludendoli dalla disciplina dello Statuto dei lavoratori soltanto se diretti esclusivamente ai beni estranei al rapporto di lavoro e pertanto non rivolti alla verifica dell'esatto adempimento delle obbligazioni lavorative, finendo così per restare al di fuori del perimetro dell'art. 4 (con l'applicazione della relativa procedura concertativa) soltanto le indagine dirette ad accertare comportamenti del lavoratore illeciti e lesivi del patrimonio o dell'immagine aziendale[133].

Tuttavia, sul punto, non mancano orientamenti di segno opposto[134], maggioritari in ordine ai controlli difensivi operati tramite sistemi di controllo a distanza, secondo i quali l'esigenza di evitare condotte illecite da parte del proprio dipendente non potrebbe essere comunque tale da giustificare l'eliminazione di qualsiasi forma di tutela alla sua riservatezza

[131] Tale ricostruzione è sostenuta anche dalla giurisprudenza penale che, anche in virtù della prevalenza dell'interesse pubblico, considera sempre ammissibili quei controlli difensivi diretti a riscontrare la commissione di illeciti penali, persino quando la relativa prova sia stata illegittimamente raccolta, dovendo così riconoscersi inferiore tutela al diritto di riservatezza e all'autonomia del lavoratore davanti ad interessi superiori. Sul punto si veda Cass. Pen. 12 novembre 2013, n. 4331 e Cass. Pen. 14 dicembre 2009, n. 47429.

[132] Cass. 17 luglio 2007, n. 15892 con nota di A. BELLAVISTA, *Controlli a distanza e necessità del rispetto della procedura di cui al comma 2 dell'art. 4 St. lav.*, in *Riv. giur. lav.*, 2008, II, pp. 358 ss.

[133] Da ultimo Cass. 13 maggio 2016, n. 9904 e Cass. 17 febbraio 2015, n. 3122.

[134] Sul punto le pronunce Cass. 17 luglio 2007, n. 15892 e Cass. 23 febbraio 2010, n. 4375 secondo cui i controlli difensivi realizzati tramite dei sistemi di controllo a distanza quando collegati anche indirettamente alla prestazione lavorativi, dovevano essere assoggettati alla disciplina dei controlli preterintenzionali di cui all'art. 4, II comma, L. n. 300/70 per non comportare "*un sostanziale annullamento di ogni forma di garanzia alla dignità e riservatezza del lavoratore*" (Cass. 17 luglio 2007, n. 15892).

e dignità, almeno tutte le volte che l'illecito sia in qualche modo connesso allo svolgimento della prestazione lavorativa[135].

L'orientamento contrario[136] ai controlli difensivi fonda le sue ragioni sulla difficoltà pratica di distinguere tra controlli sull'attività lavorativa e controlli difensivi, nonché su un'individuazione comune e condivisa di "patrimonio aziendale". Pertanto, dove i controlli difensivi siano compiuti tramite un sistema di controllo a distanza e possano preterintenzionalmente dare atto anche ad un controllo sulla prestazione lavorativa[137], anch'essi devono essere preceduti dalla procedura di cui all'art. 4 dello Statuto dei lavoratori[138].

A ben vedere però, un controllo difensivo compiuto con un impianto audiovisivo ritenuto poi illegittimo porterebbe al paradosso di sanzionare il datore di lavoro con una sanzione penale prevista dall'art. 38 S.L. e di salvaguardare un lavoratore che commette un illecito, possibilmente anche di rilievo penale, in ragione della tutela della *privacy*.

Pertanto, la giurisprudenza[139] ha legittimato sempre più spesso i controlli difensivi che venivano effettuati in modo occulto, purché a titolo occasionale e non continuativo e che siano indispensabili, come *extrema ratio*, per la tutela del patrimonio aziendale, specie quando abbiano ad

---

[135] R. SCORCELLI, *Ancora in tema di controlli a distanza ai sensi dell'art. 4 SL sui limiti di liceità dei cd controlli difensivi*, in *DL Rivista di diritto del lavoro privato e pubblico*, 2007 fasc. 4, pp. 1205 ss.

[136] P. LAMBERTUCCI, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act),* WP (*Working Papers*) C.S.D.L.E. "Massimo D'Antona" IT - 255/2015.

[137] M. MISCIONE, *I controlli intenzionali, preterintenzionali e difensivi sui lavoratori in contenzioso continuo,* in *Lav. giur.*, n. 8-9/2013.

[138] L. CAIRO, *Orientamenti della giurisprudenza in tema di controlli difensivi*, in *Guida Dir*. n. 37/2007; nonché M.L. VALLAURI, *op. cit.*.

[139] Cass. 23 febbraio 2012, n. 2722; Cass. 1° ottobre 2012, n. 16622, Cass. 27 maggio 2015, n. 10955.

oggetto condotte di rilevanza penale[140], prescindendo dalla sorveglianza della prestazione lavorativa dei dipendenti.

Il quadro delineato da dottrina e giurisprudenza finiva pertanto con il prevedere dei controlli difensivi "puri" quando non operati tramite sistemi di controllo a distanza o che comunque controllassero solo l'illecito e quelli che invece dovevano rispettare comunque la procedura ex art. 4 dello Statuto in quanto astrattamente idonei a controllare anche la prestazione lavorativa.

A ben vedere però, i controlli difensivi "puri" non potevano ritenersi liberi da qualsiasi vincolo normativo, dal momento che anche per essi restava vincolante il rispetto della normativa generale in materia di *privacy* secondo la quale nell'esecuzione del controllo e nell'acquisizione dei dati dovevano comunque essere rispettati i principi di proporzionalità, necessità, pertinenza e non eccedenza[141].

[140] L'accertamento di una condotta del lavoratore di rilevanza penale è di per sé idonea a legittimare i controlli difensivi da parte del datore di lavoro, anche in considerazione della finalità pubblicistica dell'accertamento dell'illecito penale.
[141] A. RUSSO, M. TUFO, *I controlli preterintenzionali: la nozione*, in A. LEVI (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei lavoratori dopo il Jobs Act*, Milano, Giuffrè, 2016.

2.2 La compatibilità ed il coordinamento dei controlli difensivi con la nuova *privacy* del lavoro

I controlli difensivi, come ogni teorizzazione giurisprudenziale-dottrinaria, hanno sofferto dell'incertezza in cui si naviga in assenza di un dato normativo preciso, rendendo per i datori di lavoro difficile comprendere la legittimità o meno delle loro condotte di controllo ai limiti.

Per garantire una maggiore chiarezza e certezza normativa, il legislatore del 2015, con l'art. 23[142] del D.Lgs. n. 151/2015 ha cercato di superare i problemi interpretativi connessi anche ai controlli difensivi. Ed infatti, il legislatore ha inserito nella previsione normativa per i controlli a distanza, esperibili previa procedura sindacale-amministrativa, oltre alle esigenze organizzative e produttive ed alla sicurezza sul lavoro anche la "tutela del patrimonio aziendale". In tal modo i controlli difensivi realizzati con strumenti di controllo a distanza vengono parificati per espressa previsione normativa ai controlli preterintenzionali[143].

L'esplicito riferimento del legislatore alla tutela del patrimonio aziendale ed alla normativa generale della *privacy* potrebbe far ritenere chiuso il dibattito sui controlli difensivi nel senso di ritenere estinta tale categoria, normativa inclusa nei controlli di cui al nuovo I comma dell'art. 4 statutario[144].

---

[142] Articolo rubricato "Disposizioni di razionalizzazione e semplificazione delle procedure e degli adempimenti a carico di cittadini e imprese e altre disposizioni in materia di rapporto di lavoro e pari opportunità, in attuazione della legge 10 dicembre 2014, n. 183".

[143] Sul punto si veda: L.A. COSATTINI, *Le modifiche all'art. 4 st. lav. sui controlli a distanza, tanto rumore per nulla?,* in *Lav. giur.* 2015, n. 11; M.T. SALIMBENI, *La riforma dell'art. 4 dello statuto dei lavoratori: l'ambigua risolutezza del legislatore,* in *Riv. It. Dir. lav*., 2015 n. 4.

[144] G.A. RECCHIA, *Controlli datoriali difensivi: note su una categoria in via di estinzione*, in Lavoro nella giurisprudenza, 4/2017.

Ed infatti, secondo larga parte della dottrina[145] e le prime pronunce della giurisprudenza di merito[146] (per fatti successivi all'entrata in vigore del nuovo testo dell'art. 4 della L. n. 300/1970), tale previsione non richiede più al datore di lavoro di verificare se dal controllo difensivo effettuato a distanza possa essere o meno astrattamente controllabile anche la prestazione lavorativa, dal momento che in ogni caso un controllo a distanza effettuato per tutela del patrimonio aziendale richiederebbe comunque l'espletamento della procedura autorizzativa sindacale-amministrativa stante la previsione della nuova esigenza legittimante il controllo a distanza.

L'inflessibilità della norma emerge ancora di più laddove si pensi che all'interno di patrimonio aziendale vi rientrino anche i beni immateriali[147], pertanto anche i controlli informatici svolti attraverso internet o un generico dispositivo informatico necessiteranno dell'espletamento della procedura di cui all'art. 4, comma I, L. n. 300/70[148].

Peraltro, i controlli difensivi svolti attraverso gli strumenti tecnologici sono visti con particolare sospetto poiché essi hanno più di altri la capacità di rivelare dati personali riservati dei lavoratori. Ed infatti,

---

[145] R. DEL PUNTA, *Op. cit.*., nonché P. LAMBERTUCCI, *I poteri del datore di lavoro nello Statuto dei lavoratori dopo l'attuazione del c.d. jobs act del 2015: primi spunti di riflessione,* in Arg. dir. lav., 2016, 530 ss.; A. ARBORE, *La nuova disciplina dei controlli ex art. 4 St. Lav.,* in E. GHERA – D. GAROFALO (a cura di), *Semplificazioni – sanzioni - ispezioni nel Jobs Act 2,* Bari, Cacucci, 2016, 161 ss.

[146] Tribunale di Roma, 13 giugno 2018, n. 57668.

[147] I. ALVINO*, L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica,* in *Diritto delle relazioni industriali*, 4, 2014.

[148] La giurisprudenza di legittimità si è recentemente pronunciata su controlli difensivi "tecnologici" (seppure per casi di specie avvenuti nella vigenza del vecchio testo) affermando il principio secondo il quale il controllo difensivo deve ritenersi illegittimo laddove seppur mirato ad accertare comportamenti illeciti dei lavoratori comporti la possibilità di verifica a distanza dell'attività di questi ultimi ed avvenga in assenza di acquisizione del consenso individuale, del rilascio dell'adeguata informativa e il conseguente trattamento possa determinare indagine sulle opinioni o vita personale del lavoratore. Sul punto si vedano Cass. 19 settembre 2016, n. 18302.

parte della dottrina[149], secondo un orientamento rigoroso del Garante per la protezione dei dati personali[150], ritiene che i controlli difensivi posti in essere con strumenti informatici, che in astratto sono idonei a rivelare persino dati sensibili del lavoratore, devono essere considerati illegittimi a prescindere.

La rigidità del nuovo testo normativo secondo parte della dottrina "*mette a rischio la possibilità di configurare controlli difensivi legittimi perché finalizzati a provare illeciti penali. Ciò in quanto è indubbio che, laddove il reato vada a ledere il patrimonio aziendale (come ad es. il caso della cassiera che sottragga il denaro incassato del supermercato datore di lavoro), l'eventuale controllo difensivo sarebbe finalizzato alla tutela del patrimonio aziendale stesso, e, allora, necessiterebbe l'espletamento della procedura sindacale amministrativa di cui all'art. 4 comma 1, st. lav.*"[151].

La nuova interpretazione restrittiva in merito ai controlli difensivi porterebbe poi all'impossibilità di verificare e sanzionare illeciti gravi soltanto perché il datore di lavoro non ha preventivamente ottenuto l'autorizzazione all'installazione del sistema di controllo, con la paradossale conseguenza che non verrebbe più garantito neanche il principio generale della legittima difesa nei rapporti inter-privati contro atti di aggressione del patrimonio altrui[152].

Inoltre, la necessità di procedere ad un'indagine per l'accertamento di un illecito richiede una tempestività che mal si coordina con la

[149] P. SALAZAR - L. FAILLA, *Controlli difensivi: quali limiti nel nuovo contesto dell'art. 4, L. n. 300/1970,* in *Il lavoro nella giurisprudenza*, 2/2017.
[150] Garante per la protezione dei dati personali provvedimento n. 303 del 13 luglio 2016 e provvedimento n. 350 dell'8 settembre 2016.
[151] A. RUSSO, M. TUFO, *op.cit.*
[152] V. MAIO, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. Dir. Lav*., 6/2015, pp. 1186 ss.

procedura di cui all'art. 4 dello Statuto. Ed infatti secondo parte della dottrina, "*l'installazione dell'impianto di controllo, e ciò sia ove si tenga conto dei tempi necessari per il normale svolgimento di tale procedura, sia ove si consideri che l'avvio del confronto sindacale priverebbe l'indagine della segretezza che è normalmente necessaria perché essa dare risultati*"[153].

Nell'interpretazione restrittiva della normativa in esame, al fine di realizzare il controllo difensivo, il datore di lavoro dovrebbe preventivamente raggiungere l'accordo sindacale oppure ottenere l'autorizzazione amministrativa per l'uso dei sistemi di controllo a tutela del patrimonio aziendale, in modo da "abilitare" il controllo ed azionarlo legittimamente in presenza di indizi di condotta illecita del dipendente. Ma v'è di più. Ed infatti, per utilizzare le informazioni acquisite in tale controllo anche a fini disciplinari, il datore deve dare atto di tale possibile uso nell'informativa con l'indicazione delle eventuali conseguenze disciplinari[154].

Ci si ritroverebbe quindi nella situazione in cui una norma restrittiva dei controlli difensivi porterebbe al paradosso della moltiplicazione esponenziale di accordi sindacali o richieste di autorizzazioni amministrative preventive, numerose informative su tutti i possibili controlli espletabili e rilevanza disciplinare delle condotte dei lavoratori, con la conseguente possibilità per i datori di lavoro di svolgere una casistica amplia di controlli, purché preventivamente autorizzati e rappresentati ai lavoratori.

---

[153] G. PROIA, *op. cit.*

[154] A. INGRAO*, Il controllo disciplinare e la "privacy" del lavoratore dopo il "Jobs act"***,** *nota a Cass. sez. I civ. 19 settembre 2016, n. 18302; Cass. sez. lav. 5 ottobre 2016, n. 19922*, in *Rivista italiana di diritto del lavoro,* 2017, fasc. 1, pt. 2, pp. 46-54.

È evidente quindi che l'interpretazione rigida del nuovo art. 4, comma I, L. n. 300/70 non possa essere sostenuta, in quanto, a livello operativo, determinerebbe l'impossibilità di accertare la maggior parte degli illeciti accertabili soltanto tramite controllo tecnologico. Inoltre, la recente novità normativa in tema di *whistleblowing*[155], nell'ipotesi in cui si ritenessero impediti i controlli difensivi senza opportuna autorizzazione, verrebbe svuotata nei propri effetti dal momento che il datore di lavoro non avrebbe gli strumenti per accertare l'illecito segnalato ed applicare le opportune conseguenze disciplinari.

Contrariamente alla tesi restrittiva, parte della dottrina[156] ha sostenuto che il nuovo testo dell'art. 4 statutario ha portato alla distinzione tra due tipi di controlli che nel vecchio testo normativo potevano invece essere ricompresi nel medesimo alveo dei controlli difensivi. Da un lato vi sarebbero i controlli a presidio del patrimonio aziendale i quali pacificamente, per espressa previsione normativa, devono avvenire nel rispetto delle previsioni di cui all'art. 4, comma I e III. Dall'altro lato "sopravvivrebbero" alla novella normativa quei controlli difensivi volti a salvaguardare il datore di lavoro da condotte illecite dei propri dipendenti, le quali non necessariamente potrebbero colpire il patrimonio aziendale.

---

[155] Il *whistleblowing* è un termine anglosassone per definire la segnalazione compiuta da un prestatore di lavoro che, nello svolgimento delle proprie mansioni, verifica un illecito, un rischio o comunque una situazione di pericolo che possa arrecare danno all'azienda per cui lavora direttamente o indirettamente. Tale fattispecie, che per esigenze di brevità non potrà essere oggetto di approfondimento nella presente opera, è stata recentemente disciplinata dal legislatore italiano con la L. n. 179/2017. Tale legge prevede che chi effettua le segnalazioni non possa essere licenziato, sanzionato o comunque colpito da qualsiasi misura organizzativa che possa avere effetto negativo sulle sue condizioni di lavoro per aver effettuato la segnalazione. La comunicazione per tutelare la riservatezza del segnalante viene persino sottratta al diritto di accesso di cui agli artt. 22 ss. della L. n. 241/90 fermo restando l'inapplicabilità della legge laddove sia accertata la responsabilità penale del segnalante per calunnia o diffamazione oppure la responsabilità civile per i medesimi reati nei casi di dolo e colpa grave. Per un approfondimento sul tema, tra gli altri M. FREDIANI, *La delazione protetta quale diritto-dovere alla segnalazione d'allarme*, in *Il lavoro nella giurisprudenza,* n. 3/2018.

[156] A. MARESCA, *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, in *Forum Tuttolavoro Ipsoa,* 2016.

Le indagini mirate all'accertamento della condotta illecita del lavoratore dovrebbero considerarsi ancora all'esterno dell'ambito di applicazione dell'art. 4 dello Statuto, privilegiando l'interesse datoriale al controllo piuttosto che l'esigenza di *privacy* di un lavoratore che ha posto in essere una condotta non meritevole, violando i suoi doveri di correttezza e diligenza.

In tal senso procedono alcune pronunce della giurisprudenza di legittimità[157] (seppure per casi di specie avvenuti nella vigenza del vecchio testo dell'art. 4 statutario) con le più recenti sentenze ha ribadito la legittimità dell'uso di sistemi di controllo a distanza a fini di prevenzione o investigazione di condotte del dipendente che integrano illeciti penali o illeciti civili sanzionabili con il licenziamento, non potendo essere tollerabile un siffatto comportamento lavorativo che altrimenti si renderebbe impossibile da accertare[158].

---

[157] Cass. del 29 aprile 2017, n. 10636 ("*è stata affermata la legittimità dei controlli in relazione ad illeciti non attinenti al mero inadempimento della prestazione lavorativa, ma incidenti sul patrimonio aziendale, si è precisato che non dovessero presupporre necessariamente illeciti già commessi, restando giustificato l'intervento in questione non solo per l'avvenuta perpetrazione di illeciti e l'esigenza di verificarne il contenuto, ma anche in ragione del solo sospetto o della mera ipotesi che illeciti siano in corso di esecuzione*"), Cass. 8 novembre 2016, n. 22662 ("*Nel caso in disamina la condotta della lavoratrice oggetto della ripresa video non solo non atteneva alla prestazione lavorativa ma non differiva in alcun modo da quella illecita posta in essere da un qualsiasi soggetto estraneo all'organizzazione del lavoro. Il c.d. controllo difensivo, pertanto, non atteneva all'esatto adempimento delle obbligazioni discendenti dal rapporto di lavoro, ma era destinato ad accertare un comportamento che poneva in pericolo la stessa sicurezza dei lavoratori, oltre al patrimonio aziendale, determinando la diretta implicazione del diritto del datore di lavoro di tutelare la propria azienda mediante gli strumenti connessi all'esercizio dei poteri derivanti dalla sua supremazia sulla struttura aziendale*") e Cass. 28 maggio 2018 n. 13266 ("*che nel caso di specie deve essere pertanto esclusa la violazione delle garanzie previste dall'art. 4 I. 300/1970, avendo la Corte territoriale, con esatta applicazione dei principi di diritto regolanti la materia (dall'ultimo capoverso di pag. 3 al terzo di pag. 4 della sentenza), accertato in fatto l'utilizzazione del controllo all'esclusivo fine di accertamento di mancanze specifiche del lavoratore nell'impiego del computer per finalità extralavorative (gioco a Free-Cell), nelle quali era stato sorpreso dal direttore tecnico e con avvio mirato della verifica informatica ex post, per giunta in base ad o autorizzazione scritta del lavoratore (così al penultimo e al terz'ultimo capoverso di pg. 4 della sentenza) e questa solo genericamente contestata dal lavoratore medesimo (al primo periodo di pag. 8 del ricorso)*").

[158] M. DI FRANCESCO, *Licenziamento per giusta causa e controlli difensivi occulti*, in *Diritto & Pratica del lavoro*, 34-35/2017.

In ogni caso, con la riforma del 2015 la categoria dei controlli difensivi "puri", ossia senza la preventiva procedura sindacale-amministrativa, si è notevolmente ristretta, o almeno questo è quello che traspare dall'interpretazione letterale della norma[159].

Ed infatti, se si intende rimanere fedeli "*al dato letterale della norma, qualsiasi installazione di impianti audiovisivi e di altri strumenti che siano preordinati a tutelare il patrimonio aziendale e controllare la commissione di illeciti, anche di rilevanza penale, da parte dei lavoratori, risulta oggi soggetta alla procedura codeterminativa sindacale o all'autorizzazione amministrativa*"[160].

Al di fuori di tale procedura rimarrebbero quei controlli difensivi che vengono espletati tramite gli strumenti di lavoro che potrebbero beneficiare dell'esenzione della procedura sindacale-amministrativa prevista dall'art. 4, II comma, L. n. 300/70, ma, anche ai controlli difensivi mirati esclusivamente all'accertamento dell'illecito dei lavoratori e non all'attività, intesa come attività lavorativa[161], laddove la giurisprudenza maggioritaria rimanga fedele al proprio orientamento anche di buon senso in un'interpretazione adeguatrice del nuovo testo dell'art. 4 dello Statuto.

Secondo tale interpretazione in linea con gli ultimi arresti della giurisprudenza di legittimità[162] anche penale[163] la norma statutaria sarebbe limitata al divieto di controllo, anche indiretto, della corretta esecuzione della prestazione lavorativa da parte dei dipendenti, ma non già

[159] M. MARAZZA, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in Arg. dir. lav., 2016, pp. 485 ss.
[160] M. LANOTTE, *La ridefinizione dei limiti al potere di controllo a distanza,* in A. LEVI (a cura di), *Il nuovo art. 4 sui controlli a distanza Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, Giuffré, 2016.
[161] A. TAMPIERI, *I controlli a distanza mediante impianti audiovisivi*, in R. PESSI (a cura di), Codice commentato del lavoro, Torino, 2011.
[162] Cass. 21 agosto 2018, n. 20879; Cass. 28 maggio 2018, n. 13266.
[163] Cass. pen. 16 gennaio 2015, n. 2890; Cass. pen. 4 giugno 2013 n. 30177.

all'impedimento di controlli esplicazione della legittima difesa del datore di lavoro a condotte illecite dei propri lavoratori.

Il quadro normativo appena delineato lascia però insoluto il problema dei controlli difensivi che astrattamente possono insistere anche sull'attività lavorativa lasciando all'interprete il dovere di individuare il perimetro dei controlli a distanza soggetti alla procedura autorizzatoria di cui all'art. 4, I comma, L. n. 300/70[164].

Ed infatti, è evidente che l'esistenza di una condotta illecita o meno richiede una verifica che può essere fatta solo *ex post* rispetto al controllo ed alle relative risultanze, pertanto il datore di lavoro una volta acquisite le informazioni ricercate, laddove individui e riscontri una condotta illecita del lavoratore, quest'ultima "sanerebbe" anche un'eventuale intromissione nella *privacy* del lavoratore (purché proporzionata), ma laddove invece all'esito del controllo non emergano illeciti ma rimanga soltanto un monitoraggio sull'attività lavorativa effettuato senza le opportune procedure previste dall'art. 4, l'operato del datore di lavoro non solo sarebbe illegittimo ma anche soggetto a sanzione penale.

La chiarezza interpretativa che il nuovo art. 4 statutario aveva nella sua finalità non può quindi dirsi raggiunta e dovrà continuare a valutarsi caso per caso se nello svolgimento del controllo difensivo si siano rispettati i principi generali elaborati dalla giurisprudenza in materia e quelli della disciplina generale in materia di *privacy*.

[164] C. CRISCULO, *Controlli difensivi e Codice della "privacy", Nota a Cass. sez. I civ. 19 settembre 2016, n. 18302; Cass. sez. lav. 5 ottobre 2016, n. 19922,* in *Rivista italiana di diritto del lavoro,* 2017, fasc. 1, pt. 2, pp. 39-46.

2.3 I controlli difensivi nella giurisprudenza della Corte europea dei diritti dell'uomo

Alla luce del quadro normativo delineato dalla nuova disciplina sui controlli a distanza e dalla vigenza del GDPR, non si può ritenere che oggi vi sia la chiarezza normativa auspicata dal legislatore al momento della Riforma del 2015.

Pertanto, l'opera interpretativa giurisprudenziale sarà fondamentale per fare chiarezza e dettare le linee guida per gli operatori, così come lo era stata nella vigenza del vecchio testo dell'art. 4 dello Statuto e del "vecchio" codice *privacy*.

Le prime pronunce in materia di controlli difensivi dopo l'emanazione del GDPR arrivano però dalla Corte Europea dei diritti dell'Uomo[165] per vicende radicate in altri Paesi dell'Unione Europea[166] riguardo all'interpretazione degli artt. 6 ed 8 della CEDU[167].

---

[165] Nonostante non sia un'istituzione dell'Unione Europea, la Corte Europea dei diritti dell'uomo ha sempre svolto un importante ruolo interpretativo nei confronti del quale i giudici nazionali hanno un obbligo conformativo "morale" dal momento che l'art. 46 CEDU stabilisce che le sentenze della Corte EDU vincolino soltanto le parti in causa. In particolare, per il giudice italiano le pronunce in materia di *privacy* sul lavoro sono necessarie per rileggere e reinterpretare il nuovo art. 4 dello Statuto alla luce dei principi elaborati dalla Corte Europea dei diritti dell'uomo.

[166] La Corte Europea dei diritti dell'uomo in più occasioni si è pronunciata in temi di *privacy* nel rapporto di lavoro limitando il potere datoriale di utilizzo anche difensivo dei controlli a distanza. Sul punto si veda tra le altre: Kopke c. Germania, n. 420/07; Copland c. Regno Unito, n. 62617/00; Halford c. Regno Unito, n. 20605/92.

[167] Art. 6 CEDU – diritto ad un equo processo: "1. *Ogni persona ha diritto a che la sua causa sia esaminata equamente, pubblicamente ed entro un termine ragionevole da un tribunale indipendente e imparziale, costituito per legge, il quale sia chiamato a pronunciarsi sulle controversie sui suoi diritti e doveri di carattere civile o sulla fondatezza di ogni accusa penale formulata nei suoi confronti. La sentenza deve essere resa pubblicamente, ma l'accesso alla sala d'udienza può essere vietato alla stampa e al pubblico durante tutto o parte del processo nell'interesse della morale, dell'ordine pubblico o della sicurezza nazionale in una società democratica, quando lo esigono gli interessi dei minori o la protezione della vita privata delle parti in causa, o, nella misura giudicata strettamente necessaria dal tribunale, quando in circostanze speciali la pubblicità possa portare pregiudizio agli interessi della giustizia. 2. Ogni persona accusata di un reato è presunta innocente fino a quando la sua colpevolezza non sia stata legalmente accertata. 3. In particolare, ogni accusato ha diritto di: (a) essere informato, nel più breve tempo possibile, in una lingua a lui comprensibile e in modo dettagliato, della*

La più importante di esse, anche perché emanata dalla Grande Camera della Corte EDU, è la pronuncia avvenuta all'esito del procedimento *Barbulescu c. Romania*.

Tale sentenza è stata denominata da alcuni[168] la sentenza cardine in tema di tutela della *privacy* sul luogo di lavoro, anche in ordine ai controlli difensivi.

Ed infatti, essa detta gli *standard* minimi di riservatezza dei dati personali che devono essere rispettati sul luogo di lavoro in tutti gli Stati europei[169]. La pronuncia in esame ha preso le mosse da un caso di

---

natura e dei motivi dell'accusa formulata a suo carico; (b) disporre del tempo e delle facilitazioni necessarie a preparare la sua difesa; (c) difendersi personalmente o avere l'assistenza di un difensore di sua scelta e, se non ha i mezzi per retribuire un difensore, poter essere assistito gratuitamente da un avvocato d'ufficio, quando lo esigono gli interessi della giustizia; (d) esaminare o far esaminare i testimoni a carico e ottenere la convocazione e l'esame dei testimoni a discarico nelle stesse condizioni dei testimoni a carico; (e) farsi assistere gratuitamente da un interprete se non comprende o non parla la lingua usata in udienza".
Art. 8 CEDU – diritto al rispetto della vita privata e familiare: "*1. Ogni persona ha diritto al rispetto della propria vita privata e familiare, del proprio domicilio e della propria corrispondenza. 2. Non può esservi ingerenza di una autorità pubblica nell'esercizio di tale diritto a meno che tale ingerenza sia prevista dalla legge e costituisca una misura che, in una società democratica, è necessaria alla sicurezza nazionale, alla pubblica sicurezza, al benessere economico del paese, alla difesa dell'ordine e alla prevenzione dei reati, alla protezione della salute o della morale, o alla protezione dei diritti e delle libertà altrui*".

[168] F. PERRONE, *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei diritti dell'Uomo e giurisdizione nazionale dopo la sentenza Barbulescu 2*, in *Labor – Il lavoro nel diritto* n. 3/2018.

[169] (i) *whether the employee has been notified of the possibility that the employer might take measures to monitor correspondence and other communications, and of the implementation of such measures. While in practice employees may be notified in various ways depending on the particular factual circumstances of each case, the Court considers that for the measures to be deemed compatible with the requirements of Article 8 of the Convention, the notification should normally be clear about the nature of the monitoring and be given in advance; (ii) the extent of the monitoring by the employer and the degree of intrusion into the employee's privacy. In this regard, a distinction should be made between monitoring of the flow of communications and of their BĂRBULESCU v. ROMANIA JUDGMENT 37 content. Whether all communications or only part of them have been monitored should also be taken into account, as should the question whether the monitoring was limited in time and the number of people who had access to the results (see Köpke, cited above). The same applies to the spatial limits to the monitoring; (iii) whether the employer has provided legitimate reasons to justify monitoring the communications and accessing their actual content (see paragraphs 38, 43 and 45 above for an overview of international and European law in this area). Since monitoring of the content of communications is by nature a distinctly more invasive method, it requires weightier justification; (iv) whether it would have been possible to establish a monitoring system based on less intrusive methods and measures than directly accessing the content of the employee's communications. In this*

licenziamento di un lavoratore romeno il quale aveva utilizzato i mezzi informatici aziendali per comunicazioni personali nonostante fosse stato edotto dell'uso esclusivamente a fini lavorativi di tali strumenti. L'illecito di rilevanza disciplinare (violazione delle norme interne e *policy* aziendale) ha azionato il controllo difensivo da parte della Società, che nella verifica degli strumenti informatici ad esso messi a disposizione ha raccolto anche dati personali del lavoratore[170].

La Corte EDU ha rilevato una intromissione nella vita privata e familiare, del domicilio e della corrispondenza (art. 8 Convenzione Europea dei diritti dell'uomo), ma allo stesso tempo ha ritenuto comunque legittimo il controllo compiuto dal datore di lavoro in quanto il comportamento illecito del lavoratore aveva fatto venire meno la sua

connection, there should be an assessment in the light of the particular circumstances of each case of whether the aim pursued by the employer could have been achieved without directly accessing the full contents of the employee's communications; (v) the consequences of the monitoring for the employee subjected to it (see, mutatis mutandis, the similar criterion applied in the assessment of the proportionality of an interference with the exercise of freedom of expression as protected by Article 10 of the Convention in Axel Springer AG v. Germany [GC], no. 39954/08, § 95, 7 February 2012, with further references); and the use made by the employer of the results of the monitoring operation, in particular whether the results were used to achieve the declared aim of the measure (see Köpke, cited above); (vi) whether the employee had been provided with adequate safeguards, especially when the employer's monitoring operations were of an intrusive nature. Such safeguards should in particular ensure that the employer cannot access the actual content of the communications concerned unless the employee has been notified in advance of that eventuality" *Standards* minimi che possono essere così riassunti e tradotti: (i) preventiva informazione al dipendente della possibilità che il datore di lavoro possa controllare la propria corrispondenza ed altre forme di comunicazione; (ii) verifica dell'estensione del controllo da parte del datore di lavoro ed il grado di intrusione nella *privacy* del dipendente, con riferimento al loro contenuto, al carattere totale o parziale dei dati monitorati, la durata del controllo, il numero di persone che hanno avuto accesso ai dati, l'esistenza o l'assenza di spazi esclusi dal monitoraggio; (iii) motivazioni legittime del datore di lavoro per la giustificazione del monitoraggio delle comunicazione e l'accesso ai loro contenuti effettivi; (iv) controllo se fosse stato possibile approntare un sistema di monitoraggio diverso basato su metodi meno invasi e senza accedere direttamente alle comunicazioni dei dipendenti; (v) conseguenze del controllo in capo al lavoratore e quale uso venga fatto da parte del datore di lavoro dei dati acquisiti; (vi) verifica se sono state predisposte misure a salvaguardia per rendere meno invasivo il controllo necessario.

[170] Nello svolgimento del controllo il datore di lavoro ha acquisito e trascrittole comunicazioni private del lavoratore, tra le quali erano dei messaggi inviati al fratello e alla fidanzata relativi alla salute e alla vita sessuale.

legittima aspettativa di riservatezza, rendendo conseguentemente ragionevole l'operato del datore di lavoro[171].

Nel giudizio di valori compiuto dalla Corte EDU, la conclusione della correttezza dell'operato del datore di lavoro nonostante l'intromissione nella vita privata del lavoratore è diretta conseguenza del fatto che l'illecito compiuto dal lavoratore non sarebbe stato accertabile in nessun altro modo, pertanto anche i criteri di proporzionalità e necessità sono stati ritenuti rispettati.

Ed infatti "*il controllo dei messaggi privati inviati dal dipendente, nella fattispecie concreta, costituiva l'unica possibilità di verificare il regolare svolgimento delle attività lavorative nonché la eventuale commissione di atti illeciti o dannosi per il sistema aziendale*"[172].

Giova rilevare che, in ogni caso, le valutazioni compiute dalla Corte EDU hanno sì una funzione nomofilattica e di indirizzo interpretativo generale, ma allo stesso tempo risentono della specificità dei casi concreti sui quali si ritrovano ad essere fatte[173].

Sul punto, il Garante per la protezione dei dati personali italiano ha estratto il principio di diritto generalmente applicabile dal provvedimento

---

[171] G. CONSONNI, *Il caso Barbulescu c. Romania e il potere di controllo a distanza dopo il Jobs Act: la normativa europea e italiana a confronto,* in *Dir. Rel. Ind*., 2016, 4.

[172] C. GAMBA, *Il controllo a distanza dei lavoratori e l'utilizzabilità delle prove*, in *Labour law issues*, vol. 2, n. 1/2016.

[173] In dottrina vi è chi si è persino interrogato sui possibili esiti del giudizio *Barbulescu* se lo stesso fosse avvenuto in Italia – M. DALLACASA, *Il controllo delle attività informatiche e telematiche del lavoratore*, nel Lavoro nella giurisprudenza, 7/2017. Nella vigenza del nuovo art. 4 dello Statuto sarebbe infatti stato fondamentale valutare se fosse stata data preventivamente un'adeguata informativa (III comma) sulle modalità d'uso dello strumento di lavoro, delle possibilità di monitoraggio sullo stesso nonché la proporzionalità della sanzione datoriale. In difetto di informazione o proporzionalità della condotta datoriale, il licenziamento sarebbe stato illegittimo ma con due conseguenze diverse. In mancanza di preventiva informazione, nel procedimento di impugnazione de licenziamento l'inutilizzabilità dei dati avrebbero dovuto portare ad un giudizio di insussistenza del fatto con conseguente reintegrazione in regime Fornero. Invece, laddove fosse stata accertato il difetto di proporzionalità della condotta datoriale e della conseguente sanzione espulsiva vi sarebbe stato spazio soltanto per la tutela risarcitoria.

CEDU. A parere del Garante, la Corte ha riaffermato, nel caso concreto, che i controlli datoriali sull'attività lavorativa sono ammissibili soltanto nella misura in cui siano strettamente proporzionati e non eccedenti lo scopo di verifica dell'adempimento contrattuale. Devono essere limitati nel tempo, mirati e fondati su presupposti (quali l'inefficienza dell'attività lavorativa del dipendente o il sospetto di un illecito) tali da legittimarne l'esecuzione.

I chiarimenti del Garante per la protezione dei dati personali sono serviti a ricondurre il provvedimento in esame della CEDU in linea con la Raccomandazione sulla protezione dei dati in ambito lavorativo, approvata il 1° aprile 2015 dal Consiglio d'Europa, secondo la quale veniva auspicata "*la minimizzazione dei controlli difensivi o comunque rivolti agli strumenti elettronici; l'assoluta residualità dei monitoraggi, con appositi sistemi informativi, sull'attività e il comportamento dei lavoratori in quanto tale*"[174].

Il Garante ha chiarito che anche dopo la riforma del 2015, i controlli sui beni strumentali sottratti alla procedura concertativa di installazione ed i controlli difensivi (soggetti o meno alla procedura in ragione dei vari orientamenti dottrinari), restano comunque soggetti alla disciplina generale in materia di *privacy* e, in particolare, ai principi di necessità, finalità, legittimità e correttezza, proporzionalità e non eccedenza del trattamento, ribaditi proprio dalla Corte EDU. Pertanto, la condotta del datore di lavoro, a prescindere dall'applicabilità o meno della procedura concertativa dovrà essere sempre valutata in ragione dei principi di ordine generale, oggi stabiliti dal GDPR.

[174] Raccomandazione CM/Rec (2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale (Adottata dal Comitato dei Ministri il 1° aprile 2015, nel corso della 1224ma seduta dei rappresentanti dei Ministri).

Un'altra pronuncia molto importante viene offerta da un caso spagnolo con la pronuncia *Lopez Ribalda c. Spagna* del 9 gennaio 2018. La sentenza della CEDU prende le mosse da un episodio di un controllo difensivo compiuto attraverso telecamere di sorveglianza (alcune ben visibili altre occultate) posto in essere da un datore di lavoro nei confronti di un proprio dipendente sospettato di furto. In particolare, il datore di lavoro, riscontrando degli ammanchi di magazzino rispetto agli incassi giornalieri e ritenendo che ciò fosse dovuto alla condotta di uno o più dipendenti, installava all'insaputa dei lavoratori delle telecamere per sorvegliare in maniera generalizzata tutto il personale al bancone di cassa.

Per rendere effettivo il controllo ed accertare l'illecito non veniva fornita alcuna informativa ai lavoratori nonostante, la normativa in materia di *privacy* spagnola, così come quella italiana, imponesse di dare comunicazione in modo esauriente ai lavoratori. Esperito il controllo venivano individuati i responsabili e licenziati; questi ultimi però impugnavano il licenziamento lamentando una lesione del proprio diritto di *privacy* (art. 8 CEDU) nonché la violazione del diritto di difesa (art. 6 CEDU) chiedendo l'inutilizzabilità dei dati acquisiti in maniera occulta.

Le Corti nazionali spagnole consideravano legittima la condotta del datore di lavoro ritenendo nel bilanciamento tra riservatezza e interesse datoriale alla tutela del patrimonio aziendale prevalente quest'ultimo, purché proporzionato all'illecito da accertare[175].

A ben vedere tale conclusione si pone in linea con quella parte di giurisprudenza che, con un orientamento meno restrittivo, ritiene possibili

[175] A. SITZIA, *Videosorveglianza occulta, privacy e diritto di proprietà: la Corte Edu torna sul criterio di bilanciamento*, in *Arg. Dir. Lav*., 2018, 2.

i controlli difensivi tecnologici quando siano l'unico modo per accertare l'illecito, specie se di rilevanza penale.

Tale decisione però veniva sovvertita dalla pronuncia della Corte EDU. Ed infatti, la Corte ha ritenuto la condotta del datore di lavoro sproporzionata rispetto alle finalità da raggiungere, dal momento che il controllo occulto era stata posto in essere indiscriminatamente nei confronti di tutti i lavoratori e, conseguentemente ha condannato lo Stato spagnolo che, tramite i propri giudici nazionali, ha errato nel bilanciamento tra riservatezza dei lavoratori ed interesse datoriale. La Corte EDU aggiunge che la verifica della proporzionalità del controllo difensivo deve essere ancora più stringente in quegli ordinamenti nazionali dove le leggi in materia di *privacy* sul lavoro sono idonee a fondare una più grande aspettativa di riservatezza nei lavoratori.

Pertanto, anche in questo caso come già analizzato per *Barbulescu c. Romania*, l'esame da compiere per la valutazione della legittimità del controllo da parte del datore di lavoro è mirato al rispetto dei principi generali del GDPR, così come declinati dalla Corte EDU, dal Garante per la Protezione dei dati personali italiano ed europeo nonché prima dal WP29 ed oggi dall'*European Data Protection Board* (EDPB).

CAPITOLO III

I CONTROLLI SUGLI STRUMENTI DI LAVORO E L'UTILIZZABILITÀ DEI DATI

3.1 Premessa

L'impresa fordista oggetto di regolamentazione dello Statuto dei lavoratori è notevolmente cambiata evolvendosi nell'impresa digitale dove gli strumenti tecnologici offerti dalla tecnica e dell'innovazione non sono più soltanto degli strumenti utilizzati per il controllo o alternativamente per l'adempimento della prestazione lavorativa, ma possono assolvere contemporaneamente entrambe le funzioni[176].

Inoltre, le nuove tecnologie consentono un'elaborazione di dati impensabile al momento della nascita dello Statuto consentendo un trattamento simultaneo di moltissimi dati e l'estrazione di altre informazioni da altri prestatori di lavoro. L'enorme mole di dati che vengono trattati dagli strumenti di lavoro, che però si è visto possono essere anche strumenti di controllo, introducono in azienda il fenomeno dei *big data*[177].

Il Garante europeo per la protezione dei dati personali intervenendo sul tema dei *big data* li ha definiti come "*la pratica di combinare enormi volumi di informazioni provenienti da diverse fonti e di analizzarle, usando sofisticati algoritmi per informare le decisioni*"[178].

[176] G. ZICCARDI, *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *Labour Law Issues*, 2016,2.
[177] I *big data* sono una elevatissima quantità di informazioni sia in termini di volume che di varietà che consentono tramite le nuove tecnologie di portare alla deduzione di informazioni particolari ed aggiuntive rispetto a quelle che ottenibili da piccole serie di dati.
[178] *Opinion* 7/2015 del Garante europeo per la protezione dei dati personali.

Utilizzare tali dati può agevolare il processo decisionale in azienda, redendo le scelte più consapevoli, ma dal punto di vista giuslavoristico può comportare dei problemi in ordine alla *privacy* dei lavoratori con riferimento all'attività che viene definita *HR analytics*[179].

Attraverso l'analisi dei dati acquisiti sia dalla attività lavorativa dei propri dipendenti, ma anche dalla loro vita privata come l'uso di *social network* oppure da test psico-attitudinali sottoposti in fase di selezione, il datore di lavoro potrebbe realizzare un'illegittima intromissione nella sfera privata dei propri dipendenti, soprattutto quando le informazioni vengono acquisite da fonti non strettamente correlate all'attività lavorativa.

Il GDPR, rispetto alla Direttiva del 95, di fatto agevola la possibilità di utilizzare i *big data* dal momento che consente un trattamento prolungato dei dati personali, slegato anche dal consenso, nel momento in cui tali dati subiscano un procedimento di pseudonomizzazione. A ben vedere però, il Garante per la protezione dei dati personali con un provvedimento del 24 novembre 2016[180] ha ammonito sull'uso di tali dati soprattutto quando essi possano creare una profilazione specifica del soggetto cui si riferiscano[181]. Da ultimo nella medesima direzione va il

[179] *L'HR analytics* è un sistema di analisi attraverso il quale esaminando molteplici dati della forza lavoro, combinandoli tra loro ed analizzandoli con degli algoritmi appositamente programmati il datore di lavoro riesce ad avere delle indicazioni per la gestione del personale, anche in ordine ai processi finalizzati ad identificare, selezionare e valutare candidati e lavoratori.
[180] Garante per la protezione dei dati personali - "*Piattaforma web per l'elaborazione di profili reputazionali"* 24 novembre 2016.
[181] Sul punto il GDPR all'art. 13, II comma, lett. f ed all'art. 14, II comma, lett. g, prevede che in caso di profilazione di un soggetto il titolare del trattamento debba rispettare un maggior onere di informazione comunicando la logica utilizzata per la profilazione, l'importanza e le conseguenze del trattamento per l'interessato, nonché l'esistenza di trattamenti automatizzati dei dati.

divieto di utilizzo del sistema "Savio" per la programmazione delle visite mediche nei confronti dei lavoratori da parte dell'INPS[182].

Dal punto di vista giuslavoristico, nel GDPR manca una norma specifica relativa all'*HR analytics,* pertanto si dovrà far riferimento alla normativa interna la quale con il divieto di cui all'art. 4 dello Statuto, I comma, esclude la possibilità di utilizzo di *software* di analisi di *big data* laddove da questi derivi un controllo diretto dei lavoratori. A ben vedere però, il medesimo art. 4 prevede l'utilizzabilità dei dati provenienti da strumenti di lavoro e controlli preterintenzionali "*a tutti i fini connessi al rapporto di lavoro*", potendo ritenersi che le informazioni così acquisite siano spendibili anche per le attività di *HR analytics*[183].

Pertanto, le informazioni legittimamente acquisite dal datore di lavoro potranno essere oggetto di analisi soltanto laddove il lavoratore abbia ricevuto un'adeguata informazione nel rispetto della disciplina generale in materia di *privacy*, fermo restando comunque il divieto di uso discriminatorio di tali dati.

In ogni caso, per evitare illegittime intromissioni nella sfera privata del lavoratore, "*è utile orientare la progettazione delle strumentazioni informatiche in modo da stralciare ogni dato rilevatore delle attitudini personali del lavoratore, sperimentando in tal modo una regolazione*

[182] Il Garante per la protezione dei dati personali in audizione al Senato il 19 settembre 2018 in tema di utilizzo delle metodologie di *data mining* per eseguire visite mediche di controllo nei confronti dei lavoratori del settore pubblico ha affermato l'incompatibilità del sistema "Savio" messo a punto dall'INPS negli ultimi 5 anni per la gestione delle visite di controllo nei confronti dei lavoratori in malattia. Secondo il Garante per la protezione dei dati personali tale sistema non è compatibile con la disciplina *privacy* in quanto "*realizza una vera e propria profilazione dei lavoratori interessati, non conforme al GDPR*", attribuendo ad ogni lavoratore "*un determinato grado di propensione all'assenza per malattia ingiustificata*".

[183] E. DAGNINO, *People Analytics: lavoro e tutele al tempo del management tramite big data*, ADAPT University Press, 2017.

veicolata dai codici informatici che attribuisca alla tecnologia una funzione indiretta ma essenziale di tutela delle posizioni giuridiche"[184].

Al momento però i *big data* in azienda vengono utilizzati per l'attività di analisi dei lavoratori come gruppo ed organizzazione aziendale in generale, limitando così la possibilità intrusiva nella sfera privata dei singoli lavoratori a differenza dei singoli strumenti di lavoro, i quali dopo la modifica dell'art. 4 dello Statuto sono stati esonerati dalla procedura concertativa per il controllo, rimanendo pertanto direttamente controllabili dal datore di lavoro, il quale dovrà fornire soltanto un'adeguata informazione ai lavoratori per utilizzare i dati acquisiti tramite tali strumenti.

Il controllo sul mezzo attraverso il quale viene resa la prestazione lavorativa viene così liberalizzato, ma come chiarito dal Ministero del lavoro con nota del 18 giugno 2015, ciò è vero finché lo strumento sul quale si svolge il controllo è uno strumento che serve per adempiere alla prestazione, mentre se esso viene alterato o modificato con l'aggiunta di un componente o un *software,* da strumento di lavoro diventa strumento di controllo, legittimo soltanto se svolto dopo la procedura concertativa di cui all'art. 4, I comma, dello Statuto.

A ben vedere nell'impresa 2.0 moltissimi degli strumenti di lavoro consentono contestualmente la possibilità di controllo del lavoratore; si pensi alla posta elettronica, al PC, agli *smartphones*, ai sistemi *GPS*, sino ai *social networks*. Pertanto, nonostante il II comma dell'art. 4 dello Statuto sia contrapposto al divieto di controlli a distanza generalizzati, è evidente come la possibilità per il datore di lavoro di controllare gli

[184] A. DONINI, *Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy*, in *Labour&Law Issues*, vol. 3, n. 1, 2017.

strumenti di lavoro (nonché agli strumenti di registrazioni degli accessi e delle presenze) nel rispetto della disciplina comune della *privacy* (con il riferimento all'interno dell'art. 4 dello Statuto al D.Lgs. n. 196/03) sia al tempo stesso un rafforzamento del potere datoriale di controllo ma anche una tutela per il lavoratore dal momento che i controlli su tali strumenti possono svolgersi soltanto previa adeguata informazione[185].

L'evoluzione normativa tracciata dal legislatore del 2015 sembra avallare la legittimità dei controlli sui mezzi di lavoro già sostenuta dalla teoria della proprietà degli strumenti di lavoro[186]. Secondo tale teoria sostenuta anche dalla giurisprudenza penale[187], i beni che il datore di lavoro mette a disposizione dei suoi dipendenti esclusivamente per l'adempimento della prestazione lavorativa sono beni dedicati all'attività professionale con una conseguente preclusione di uso privato.

In tal modo al lavoratore viene impedita la formazione di una aspettativa di privatezza nell'utilizzo dello strumento lavorativo. Ed infatti, utilizzando gli strumenti messi a disposizione dal datore di lavoro accetterebbe una compressione della propria riservatezza. Secondo l'orientamento in esame, ai fini della legittimità del controllo, l'unico presupposto necessario sarebbe la preventiva informazione dei lavoratori relativamente alla possibilità di controllo nell'utilizzo dello strumento lavorativo.

Tale suggestiva teoria in passato si scontrava con il dato normativo che non permetteva un siffatto tipo di controlli, ma oggi con il nuovo II comma dell'art. 4 statutario il legislatore sembra aver recepito a livello

[185] Sul punto si veda più diffusamente, V. NUZZO, *La protezione del lavoratore dai controlli impersonali*, Napoli, Editoriale Scientifica, 2018.
[186] M. DEL CONTE, *op. cit.*
[187] Sul punto si vedano: Tribunale di Torino del 20 giugno 2006 e Tribunale di Milano del 10 maggio 2012.

legislativo tale orientamento rendendo legittimi i controlli operati dal datore di lavoro sugli strumenti per l'adempimento della prestazione lavorativa, purché su di essi non vengano installati degli elementi aggiunti preordinati soltanto al controllo.

3.2 Il controllo degli *smartphones* e delle *sim* aziendali

A seguito della conquista del mercato da parte degli *smartphones,* il controllo del telefono aziendale da parte del datore di lavoro da strumento attraverso il quale fosse astrattamente possibile verificare soltanto le comunicazioni del proprio di dipendente (in ordine a durata, provenienza, indirizzo, sino nei casi più estremi a conoscerne il contenuto), oggi è diventato un mezzo attraverso il quale apprendere moltissimi dati personali del lavoratore.

Ed infatti, l'utilizzo sempre più diffuso delle applicazioni per gli usi più disparati e la destinazione del telefono anche a strumento di navigazione *web* genera in tali dispositivi un immagazzinamento di dati personali sempre più grande, rendendo difficile peraltro la distinzione tra uso privato ed uso lavorativo, in caso di *smartphones* assegnati al lavoratore per uso promiscuo.

I variegati usi degli *smartphones*, resi possibili dalla tecnica, rendono i telefoni e le *sim* aziendali degli strumenti di lavoro per l'adempimento della prestazione lavorativa, rientrando così nell'ambito applicativo dell'art. 4, II comma, dello Statuto.

A ben vedere però tale controllo non ha soltanto lo scopo di verificare l'esecuzione della prestazione lavorativa, ma, sempre nella logica di tutela del patrimonio aziendale da parte di azioni dei lavoratori che determinano il depauperamento dell'imprenditore, consente altresì la verifica delle spese legate allo *smartphone.*

La possibilità di controllo del telefono aziendale supera persino il divieto di intercettazioni sancito dalla norma penale di cui agli artt. 617-

617*bis* Cod. Pen.. Ed infatti, nella realtà aziendale, secondo la dottrina[188] il controllo delle comunicazioni, configura l'ipotesi della intercettazione (vietata dalla disciplina generale) soltanto quando le comunicazioni e le telefonate sono rivolte a terzi e non vi sia la minima presunzione dell'uso lavorativo del telefono in un momento specifico.

Al contrario il lavoratore che utilizza lo *smartphone* per ragioni lavorative, compie un'attività nella quale, almeno presuntivamente, è coinvolto anche il datore di lavoro, pertanto in tal caso non può configurarsi un'intercettazione in senso stretto[189].

L'esigenza di controllo da parte del datore di lavoro è stata ritenuta prevalente rispetto alla riservatezza del lavoratore anche nell'interpretazione del vecchio testo dell'art. 4 statutario purché l'ingerenza datoriale rispetti i principi di proporzionalità, equità e trasparenza.

La modifica dell'art. 4 dello Statuto ha ulteriormente chiarito la legittimità del controllo sui telefoni aziendali non più soltanto in quanto la loro verifica a tutela del patrimonio aziendale configuri un controllo difensivo, ma soprattutto poiché sono degli strumenti di lavoro attraverso i quali il datore di lavoro verifica il corretto andamento della propria organizzazione produttiva.

Rispetto al passato quindi il nuovo art. 4 statutario consente un maggior controllo del telefono aziendale da parte del datore di lavoro, ma come analizzato in premessa ciò può dirsi valido soltanto per il mero controllo dello strumento lavorativo, laddove invece venga aggiunto un

[188] A. VALLEBONA, *Il controllo delle comunicazioni telefoniche del lavoratore*, in *Il diritto del lavoro*, 2001, vol. 75, fasc. 4, pp. 357-362.
[189] A. VALLEBONA, *Note e dibattiti di attualità, il controllo delle comunicazioni telefoniche del lavoratore*, in *DL*, 2001.

software sul dispositivo, finalizzato esclusivamente al controllo o all'elaborazione dei dati ivi raccolti, si fuoriesce dall'ambito di applicazione del II comma dell'art. 4 statutario e si rientra invece nel I comma, rendendo necessario il procedimento concertativo per il monitoraggio.

Sul punto, si è recentemente pronunciato il Garante per la protezione dei dati personali con provvedimento n. 3 dell'11 gennaio 2018[190] nel quale vengono fornite indicazioni di grande rilevanza in merito al controllo del traffico dei telefoni aziendali in uso ai lavoratori.

Ed infatti, un controllo su uno strumento di lavoro che però può rilevare anche altre informazioni deve rispettare almeno i seguenti parametri individuati dal Garante per la protezione dei dati personali:

(i) le finalità perseguite con l'installazione di un *software* aggiuntivo sugli *smartphone* aziendali devono essere riconducibili ad esigenze organizzative o di tutela del patrimonio aziendale (ad esempio la riduzione dei costi) dal momento in cui venga configurato un controllo a distanza;

(ii) i principi di necessità e proporzionalità (nel controllo degli *smartphone* per riduzione di costi possono dirsi rispettati soltanto in caso di adozione di un profilo a consumo in fatturazione e non invece per una tariffazione "*flat*" che non giustificherebbe l'esigenza di verifica datoriale);

[190] Garante per la protezione dei dati personali - Verifica preliminare. Trattamento dei dati personali dei dipendenti cui è stato assegnato un telefono aziendale - 11 gennaio 2018.
Il provvedimento prende le mosse da una richiesta di verifica preliminare della *Johnson&Johnson Medical* S.p.A. con riguardo al trattamento di dati personali dei propri dipendenti cui sia stato assegnato un telefono aziendale. Il trattamento avrebbe la finalità di "controllo delle fatture del provider del servizio telefonico" nonché di "*analisi dell'andamento complessivo dei consumi in modo da valutare nel tempo l'adeguatezza del contratto con il provider […] con l'obiettivo di ridurre i costi aziendali e ottimizzare la qualità del servizio*" nonché "*rilevare eventuali situazioni anomale di consumi". Il trattamento sarebbe effettuato mediante l'adozione di un sistema che consentirebbe di raccogliere ed elaborare i dati personali dei dipendenti ad opera della società inglese Tangoe Europe Limited, specializzata nel settore*".

(iii) il tempo di conservazione che, nel caso di controllo dei dati telefonici, non può essere superiore ai sei mesi ai sensi dell'art. 123, II comma, D.Lgs. n. 196/03. Tale vincolo è peraltro rafforzato dall'art. 13, II comma, lett. a) del GDPR che, a differenza del codice *privacy* obbliga il titolare del trattamento ad informare l'interessato relativamente al periodo di conservazione.

È evidente quindi che per meglio regolare gli aspetti suesposti e fornire l'adeguata informazione di cui al III comma dell'art. 4 statutario, lo strumento necessario, così come rilevato dallo stesso Garante, sia la *"policy* aziendale" sulle modalità d'uso degli strumenti e sui controlli. In tale contesto quindi la *policy* aziendale rappresenta "*il momento fondamentale nella prospettiva della progettazione privacy e dovrà diventare sempre più il punto di riferimento per la corretta gestione di ogni aspetto del trattamento dei dati personali di dipendenti e collaboratori*"[191].

A ben vedere però, nonostante il controllo sul telefono aziendale sia possibile in quanto strumento di lavoro, nel caso di verifica dei costi generati dall'utilizzo del telefono aziendale si fuoriesce dall'ambito di applicazione del II comma dell'art. 4, rientrando nel I comma, dal momento che dei costi "anomali" nell'uso del telefono non possono che essere ricollegabili ad un uso per finalità non lavorativa del telefono (che sarebbero già conosciute dal datore di lavoro e quindi inidonee a creare un costo anomalo inaspettato)[192].

[191] A. SITZIA, *Controllo sulle sim aziendali: necessaria la policy interna*, in *Diritto&Pratica del Lavoro*, 8/2018.
[192] F. CARACCIOLO DI MELISSANO, *Uso illegittimo del telefono aziendale e licenziamento. I profili della riservatezza del lavoratore*, in *Dir. merc. lav.,* 2012, II.

Tale questione rappresenta l'ostacolo principale al controllo del telefono aziendale dal momento che molto spesso i datori di lavoro che procedono alla verifica dei costi apprendono informazioni riservate ed appartenenti alla sfera privata dei lavoratori.

Sul punto, la Corte EDU negli ultimi arresti giurisprudenziali[193] ha chiarito che anche laddove vengano coinvolti dati personali di natura strettamente privata, l'aspettativa di privatezza del lavoratore non può essere prevalente rispetto all'esigenza di controllo del datore di lavoro, laddove questi abbia compiuto una verifica adeguata che abbia rispettato i seguenti parametri:

(i) adeguata informazione sulla possibilità di monitoraggio e misure di controllo;

(ii) grado di intrusione nella sfera privata del lavoratore limitato e solo in quanto strettamente necessario;

(iii) ragione legittima del datore di lavoro per azionare il monitoraggio;

(iv) utilizzo delle informazioni raccolte proporzionato e pertinente all'attività lavorativa.

Al fine di evitare una commistione tra dati personali privati e dati personali attinenti all'attività lavorativa, oltre alla redazione di una *policy* aziendale, per quei lavoratori a cui viene assegnato un telefono aziendale ad uso promiscuo è buona pratica far anteporre ai numeri da chiamare, un codice numerico in grado di far attivare sul dispositivo cellulare il sistema della "doppia fatturazione" o "*dual billing*" in modo da ripartire tra datore

[193] A. SITZIA, *I limiti del controllo della posta elettronica del lavoratore: una chiara presa di posizione della Grande Camera della Corte eur. dir. uomo*, nota alla sentenza della CORTE EUR. DIR. UOMO, Grande Camera, 5.9.2017, ric. 61496/08, in *Nuova Giur. civ. commentata,* n. 12/2017.

di lavoro e dipendente i costi di fatturazione e diminuire ancora di più l'aspettativa di riservatezza che il lavoratore può nutrire nell'utilizzo del telefono per fini lavorativi nel momento in cui non antepone il codice concordato per le chiamate di carattere personale[194].

Mentre il controllo del telefono aziendale ai fini del monitoraggio dei costi e, quindi, della tutela del patrimonio aziendale, configura un controllo preterintenzionale, ciò potrebbe non valere per i controlli svolti sul telefono aziendale di quei lavoratori che svolgono la propria prestazione lavorativa essenzialmente al telefono. I lavoratori dei *call center* sono il caso più emblematico.

Nella prassi la registrazione delle telefonate effettuate dai lavoratori addetti al *call center* è utilizzata al fine del monitoraggio degli *standard* qualitativi delle telefonate svolte dagli operatori. Dal momento che tali monitoraggi rientrano sicuramente tra i controlli di cui all'art. 4, II comma, dello Statuto, l'unico profilo di criticità può essere sollevato in merito all'adeguata informazione da rivolgere da un lato ai lavoratori (di solito attraverso specifiche *policy*) e dall'altro ai terzi che effettuano o ricevono una telefonata (informandoli prima dell'inizio della conversazione che la loro telefonata potrà essere registrata per finalità di monitoraggio della qualità del servizio offerto).

Nella vigenza del vecchio testo, il Ministero del lavoro con provvedimento del 2010[195] aveva chiarito che il controllo campione sulla qualità della telefonata dell'operatore di *call center* fosse possibile soltanto laddove non ci fosse stato un controllo personale, bensì i dati acquisiti fossero criptati e spersonalizzati.

[194] R. IMPERIALI, R. IMPERIALI, *Controlli sul lavoratore e tecnologie,* Milano, Giuffré, 2012.
[195] Ministero del Lavoro - Interpello n. 2 del 1° marzo 2010.

Alla luce delle novità normative, in particolare in merito all'art. 4 statutario, il controllo del telefono di un operatore addetto al *call center* sembrerebbe astrattamente legittimo in quanto per tali lavoratori il telefono è sicuramente uno strumento per rendere la prestazione lavorativa. A ben vedere però, per monitorare le telefonate sarebbe comunque necessario installare sui dispostivi o sulla rete aziendale dei *software* aggiuntivi, che come già analizzato, altererebbero la genuinità del bene aziendale, configurando quindi un controllo a distanza preterintenzionale e come tale soggetto alla procedura concertativa di cui al I comma dell'art. 4 statutario.

Sul punto è recentemente intervenuto il Garante per la protezione dei dati personali con il provvedimento n. 139 del'8 marzo 2018[196]. Riconducendo tali monitoraggi nei controlli preterintenzionali, il Garante ha ritenuto illegittimo il trattamento dei dati personali nel caso in esame mancando la procedura di cui al comma I dell'art. 4 statutario e poiché non vi era stata adeguata informazione sulle modalità d'uso da parte del *software* nei confronti degli operatori.

Ed infatti, a parere del Garante nel caso in esame di controlli telefonici su operatori di *call center* non poteva parlarsi di "strumenti di lavoro" di cui al II comma dell'art. 4 dello Statuto in quanto in considerazione "*delle accertate caratteristiche del sistema e il novero delle operazioni di trattamento da questo rese possibili non risultano in via esclusiva funzionali alla mera gestione del contatto con il cliente e, dunque, al mero svolgimento della prestazione lavorativa.... pertanto,*

[196] il Garante per la protezione dei dati personali ha sanzionato il trattamento dei dati personali operato da una Società nei confronti dei propri dipendenti addetti al *call center* per non aver fornito agli stessi una completa informativa sul funzionamento di uno specifico software di gestione delle chiamate e senza aver svolto la procedura concertativa prevista dal comma 1 dell'art. 4 dello Statuto dei Lavoratori.

contrariamente a quanto sostenuto dalla società, il sistema così configurato non può essere considerato "strument[o] utilizzat[o] dal lavoratore per rendere la prestazione lavorativa" (ai sensi e per gli effetti dell'art. 4, comma 2, l. n. 300/1970), quanto piuttosto rientra tra quegli strumenti organizzativi, dai quali può indirettamente derivare il controllo a distanza dell'attività dei lavoratori, con conseguente necessità di attivare le procedure ivi previste (art. 4, comma 1, l. n. 300/70)"[197].

Il Garante ha concluso considerando il trattamento del caso di specie non "*idoneo, in applicazione dei principi di liceità e correttezza dei trattamenti, ad informare in modo chiaro e dettagliato circa la raccolta e le caratteristiche dell'effettivo trattamento dei dati personali dei dipendenti*", in considerazione delle lacune informative presenti nella *policy* sottoposta ai lavoratori.

Alla luce di tali considerazioni, sebbene da un lato il nuovo testo dell'art. 4 dello Statuto possa far ritenere il controllo dei dispositivi telefonici un controllo rientrante nella fattispecie di esenzione della nuova norma ("strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa") dall'altro l'impossibilità di monitorare tali strumenti senza l'ausilio di *software* rende un siffatto controllo necessariamente un controllo a distanza rientrante nel I comma dell'art. 4 statutario. Pertanto, può ritenersi ancora oggi valida l'interpretazione fornita dal Ministero con la nota del 2010 in ordine al controllo della qualità delle telefonate nei *call center* secondo la quale per non rendersi necessaria la procedura concertativa sindacale-amministrativa è necessario che i dati acquisiti nel monitoraggio non siano tecnicamente riferibili ad alcun operatore e pseudonomizzati.

[197] Garante per la protezione dei dati personali – provvedimento n. 139 dell'8 marzo 2018.

Inoltre, anche l'attività di controllo sul telefono aziendale senza l'ausilio di *software* aggiuntivi potrebbe comunque richiedere l'avviamento della procedura di cui all'art. 4 dello Statuto in ragione delle funzionalità aggiuntive innate negli odierni *smartphones* come il sistema di geolocalizzazione. Ed infatti, quando il dispositivo telefonico fornito al lavoratore, per la tecnologia su di esso installata "nativamente" oppure per dei *software* aggiunti dal datore di lavoro, possa indirettamente prestarsi a rilevare informazioni non legate essenzialmente all'adempimento della prestazione lavorativa, esso non è più ascrivibile alla categoria dei meri "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa", bensì un apparato di controllo a distanza utilizzabile previo l'esperimento della procedura concertativa sindacale-amministrativa[198].

[198] P. RAUSEI, *Tutto Jobs Act. La nuova dottrina del lavoro,* Milano, Ipsoa, 2016.

3.3 La geolocalizzazione dei lavoratori

Il sistema di geolocalizzazione satellitare (*GPS – Global Positiong System*[199]) è un sistema ormai diffuso sia nella società civile che nel mondo del lavoro. Per la finalità lavorativa il sistema di geolocalizzazione si è rivelato essere uno strumento formidabile ai fini della garanzia della sicurezza dei beni aziendali in quanto il datore di lavoro è sempre in grado di sapere in tempo reale dove essi si trovano all'interno e all'esterno dell'azienda.

La diffusione di tale sistema ha portato la giurisprudenza ad interrogarsi sulla legittima delle pratiche che tramite esso si pongono in essere, controllando la posizione di persone in generale o lavoratori.

Ad esempio, in un primo momento ci si è interrogati se il monitoraggio in tempo reale della posizione di un individuo potesse configurare gli estremi di un'intercettazione o meno. La conclusione della giurisprudenza di legittimità è stata negativa[200]. Ed infatti, secondo i giudici di legittimità conoscere in tempo reale il posizionamento di una persona piuttosto che configurare un'intercettazione il cui oggetto di indagine è il contenuto di una comunicazione, realizza una sorta di "pedinamento tecnologico" che sarebbe realizzabile di persona senza integrare la fattispecie dell'intercettazione[201].

La capacità di controllo di tale sistema non poteva restare al di fuori dell'azienda, dal momento che rappresentava uno strumento perfetto per

---

[199] Il GPS è un sistema di posizionamento realizzato tramite il segnale radio proveniente da satelliti orbitanti intorno alla Terra che viene inviato ad un dispositivo di rilevazione (ricevitore) dal quale è possibile ottenere informazioni per identificare le coordinate geografiche in cui si trova il ricevitore. Più sono i satelliti che inviano il segnale al ricevitore, maggiore è la precisione dell'identificazione delle coordinate geografiche.

[200] Cass. 28 maggio 2008, n. 21366; Cass. 10 marzo 2010, n. 9667.

[201] D. GENTILE, *Tracking satellitare mediante GPS: attività atipica di indagine o intercettazione di dati? Nota a Cass. pen. 10 marzo 2010, n. 9667,* in Diritto penale e processo n. 12/2010.

il controllo della movimentazione dei beni aziendali e delle merci (in particolare, si pensi al settore della logistica) sino al controllo dei lavoratori stessi.

L'impiego principale del GPS in ambito lavorativo sinora è stato prevalentemente per il monitoraggio delle vetture che trasportano valori oppure per gli spedizionieri per esigenze di controllo giustificate dal valore dei bene trasportato, peraltro al di fuori dell'azienda dove necessariamente si affievolisce il potere di controllo del datore di lavoro.

Non vi è mai stato alcun dubbio circa la legittimità del loro impiego in azienda, purché la loro installazione sui veicoli aziendali fosse preceduta dalla procedura autorizzatoria sindacale-amministrativa di cui all'art. 4 dello Statuto ed i lavoratori addetti ai mezzi monitorati fossero adeguatamente informati circa la presenza di tali strumenti a bordo (con appositi cartelli di immediata comprensione[202]), del loro funzionamento, dei dati acquisibili e dei soggetti che svolgeranno il trattamento di tali dati.

Con le novità legislative in materia di *privacy*, i provvedimenti del Garante per la protezione dei dati personali, nonché le pronunce della giurisprudenza di legittimità[203], i margini per l'utilizzo dei sistemi di geolocalizzazione in ambito lavorativo sono aumentati.

In particolare, in considerazione dell'esenzione dalla procedura concertativa sindacale-amministrativa di cui all'art. 4 dello Statuto per gli strumenti di lavoro, va chiarito se tale sistema possa o meno ritenersi

[202] Nel provvedimento del 4 ottobre 2011 è lo stesso Garante per la protezione dei dati personali a fornire un esempio di segnale idoneo all'identificazione del sistema di geolocalizzazione a bordo sul quale dovrà essere riportata la dicitura "*veicolo sottoposto a localizzazione*".
[203] Cass. 12 ottobre 2015, n. 20440 – la quale ha affermato la legittimità di un licenziamento intimato ad un lavoratore all'esito di un'indagine di controlli difensivi svolta tramite i sistemi di geolocalizzazione.

ascrivibile a tale categoria di strumenti per rendere la prestazione lavorativa[204]. Sul punto non vi è ancora chiarezza interpretativa.

Ed infatti, la prima pronuncia interpretativa significativa sul tema è il Parere n. 5689 del 10 maggio 2016 della Direzione interregionale del lavoro di Milano. La Direzione nel menzionato Parere ha ritenuto che laddove un'azienda fornisca ad un dipendente un veicolo per eseguire la propria prestazione lavorativa e tale veicolo sia dotato di un rilevatore GPS per "*esigenze assicurative e/o per esigenze produttive e/o di sicurezza*" tali due strumenti debbano ritenersi "*inscindibilmente e unitariamente"* serventi l'attività del lavoratore. Pertanto, secondo tale Parere, non sarebbe necessario svolgere la procedura concertativa sindacale-amministrativa prima di fornire tali veicoli ai lavoratori, fermo restando soltanto l'obbligo di adeguata informazione agli stessi nel rispetto della normativa generale in materia di *privacy*.

Di diverso avviso è la circolare n. 2/2016 dell'Ispettorato Nazionale del lavoro in cui si ritiene che i rilevatori GPS debbano considerarsi degli elementi aggiuntivi al veicolo aziendale, che invece è strumento di lavoro. I rilevatori GPS sarebbero la manifestazione di un'esigenza diversa rispetto all'esecuzione della prestazione lavorativa da parte del dipendente, pertanto potrebbero essere installati soltanto previo l'esperimento della procedura concertativa sindacale-amministrativa. L'Ispettorato nella stessa circolare individua soltanto delle ipotesi marginali in cui i rilevatori GPS possano essere considerati strumenti di lavoro ed esentati dalla procedura di cui all'art. 4, I comma, dello Statuto: (i) il GPS sia necessario ed indispensabile allo svolgimento della

[204] M. LAMBROU, *Geolocalizzazione di veicoli aziendali,* in *Diritto & Pratica del Lavoro* 5/2018.

prestazione lavorativa oppure (ii) l'installazione dei rilevatori GPS sia prevista da un obbligo di legge[205].

Il Garante per la protezione dei dati personali con il provvedimento n. 138 del 16 marzo 2017 si è invece pronunciato sui principi generali in materia di *privacy* da rispettare da parte del datore di lavoro durante un trattamento dei dati acquisiti tramite sistema di geolocalizzazione[206]. In particolare, il datore di lavoro che può acquisire i dati rilevati dal GPS nel rapporto di lavoro deve rispettare i seguenti limiti: (i) tempi di conservazione dei dati acquisiti proporzionati alla finalità per la quale i dati vengono raccolti; (ii) accesso ai dati raccolti soltanto al personale incaricato tramite delle credenziali di autenticazione diverse per ogni incaricato; (iii) adozione di strumenti di cancellazione automatica al decorso dei termini stabiliti; (iv) garanzia di anonimato per i lavoratori per le rilevazioni con finalità statistiche.

A ciò, precisa il Garante, va aggiunta l'adeguata informazione da fornire ai lavoratori ai fini dell'utilizzazione dei dati acquisiti tramite la rilevazione con il sistema di geolocalizzazione.

Il Garante per la protezione dei dati personali è nuovamente intervenuto sul tema in ragione di una richiesta di verifica preliminare (*ex* art. 17 D.Lgs. n. 196/03) sul trattamento dei dati acquisiti tramite dispositivi che consentono la geolocalizzazione con il provvedimento n. 232 del 18 aprile 2018[207].

---

[205] La Circolare dell'Ispettorato ha richiamato la legge in materia di uso dei sistemi GPS per il trasporto di portavalori superiore a euro 1.500.000,00, ecc.

[206] Nel caso di specie i dati raccolti tramite i rilevatori montati sul veicolo aziendali erano idonei a rivelare i percorsi effettuati dal mezzo, le tempistiche di scarico e carico, la velocità media del veicolo, nonché i tempi di percorrenza.

[207] Nella fattispecie esaminata dal Garante, il sistema di geolocalizzazione veniva attivato dal lavoratore (guardia giurata) con un codice identificativo e password all'inizio del turno lavorativo e terminava le rilevazioni alla fine dello stesso. Tale sistema consentiva di monitorare la posizione e la velocità del veicolo in dotazione necessario per lo svolgimento della prestazione

Nel caso di specie dal momento che l'azienda richiedente la verifica della liceità dei trattamenti si occupava di servizi di sicurezza tramite guardie giurate, il monitoraggio è stato ritenuto proporzionato e necessario anche per ragioni di sicurezza, anche perché il datore di lavoro si era impegnato ad avviare la procedura concertativa sindacale-amministrativa ed aveva stabilito dei tempi di conservazione consoni alla finalità di acquisizione dei dati.

Tale provvedimento ha consentito al Garante di delineare anche delle raccomandazioni di carattere generale per tutti i trattamenti di dati tramite sistemi di geolocalizzazione. Ed infatti, per rendere il monitoraggio meno invasivo e soprattutto trasparente andrebbero sempre predisposti: (i) almeno un'icona rivelatrice dello stato di funzionamento del dispositivo; (ii) oscuramento della visibilità della posizione geografica dopo un determinato periodo di inattività del lavoratore; (iii) periodi differenzianti per la conservazione dei dati in ragione della finalità e del tipo di attività; (iv) verifiche periodiche del sistema di "eccesso di sosta" (sistema che lancia un allarme alla centrale operativa quando non viene rilevato il movimento del veicolo monitorato per un certo lasso di tempo).

Alla luce di tale quadro normativo e dei provvedimenti interpretativi[208] sembra che il controllo dei lavoratori tramite sistemi di geolocalizzazione ricada ancora nell'ambito di applicazione dell'art. 4, I comma, dello Statuto, per il quale è necessaria la procedura concertativa sindacale-amministrativa. Tale interpretazione si basa sul fatto che i

lavorativa ed i dati acquisiti venivano conosciuti soltanto da un numero ristretto di soggetti incaricati del trattamento e muniti di apposite credenziali di autenticazione. Inoltre, al lavoratore veniva preventiva fornita un'adeguata informativa circa gli estremi del trattamento dei dati risultante dal sistema di geolocalizzazione, nonché del funzionamento dello stesso.

[208] Tale ricostruzione interpretativa viene da ultimo confermata ancora dal Garante per la protezione dei dati personali nel provvedimento del 29 marzo 2018 (n. 8576577) - Verifica preliminare. Installazione di un sistema di localizzazione satellitare sui veicoli in uso alla polizia locale - 29 marzo 2018

sistemi di rilevazione, salvo casi particolari, non siano degli strumenti di lavoro, ma degli elementi aggiuntivi che applicandosi su di essi sono mirati soltanto al controllo del lavoratore.

Infine, è di sicuro interesse sul punto ricordare la nota vicenda "Amazon" in tema di braccialetti dotati di sistema di rilevazione di posizionamento in dotazione ai "*picker"* (magazzinieri) per guidarli nel rinvenimento in magazzino dei pacchi da prelevare. La vicenda ha acceso il dibattito dell'opinione pubblica che affermava che tali sistemi avrebbero violato la dignità del lavoratore configurando un controllo estremo sul lavoratore, dall'altro lato l'azienda sosteneva che tale braccialetto sarebbe stato necessario per lo svolgimento della prestazione lavorativa per i magazzinieri anche se indirettamente poteva prestarsi al loro controllo.

Nel contesto delineato dalla nuova norma, laddove si segua la linea interpretativa dell'Ispettorato del Lavoro, il "braccialetto Amazon" non è considerabile "strumento per l'adempimento della prestazione lavorativa" in quanto esso non può essere considerato indispensabile per lo svolgimento della prestazione lavorativa da parte del lavoratore, ma soltanto strumentale ad essa. Pertanto, laddove la multinazionale americana avesse voluto inserire nei suoi processi lavorativi tale strumento anche nella vigenza della nuova norma sarebbe stata comunque necessaria la procedura concertativa sindacale-amministrativa, a meno che l'azienda riesca a dimostrare l'indispensabilità dell'utilizzo di tale strumento per rendere la prestazione lavorativa.

3.4 Il monitoraggio delle *email* e del *pc* aziendale

Nella società informatizzata la posta elettronica è divenuto il mezzo di comunicazione endoaziendale ed esoaziendale principale. Ed infatti, non solo nel tempo ha sostituito la posta ordinaria ma si è imposta anche come canale di comunicazione tra le differenti aree della stessa azienda. Pertanto, oggi la maggior parte dei lavoratori che svolgono la propria prestazione lavorativa anche tramite il pc viene dotata di un indirizzo di posta elettronica aziendale.

In tale contesto il corretto bilanciamento tra esigenza di controllo della posta elettronica da parte del datore di lavoro ed aspettativa di riservatezza da parte del lavoratore assume un ruolo determinante nella definizione della *privacy* in azienda.

Nel controllo della posta elettronica dei lavoratori oltre al rispetto della normativa *privacy* il datore di lavoro incontra due ostacoli giuridici: l'art. 15 Cost. (libertà e segretezza della corrispondenza) e l'art. 616 c.p. (rilevanza penale della condotta che vìola la segretezza della corrispondenza)[209].

Tali articoli che trovano sicuramente applicazione nelle comunicazioni tra *email* private non vedono nel loro ambito di applicazione anche la posta elettronica aziendale, ove l'esigenza datoriale della conoscenza di informazioni aziendali e la tutela della infrastruttura informatica aziendale richiedono un bilanciamento con la privatezza della posta elettronica[210].

[209] D. PIZZONIA, *Controllo della posta elettronica, tutela della privacy e potere di controllo*, in *Rivista giuridica del lavoro e della previdenza sociale*, fasc. 4, 2008 – in particolare con riferimento alla casella di posta elettronica protetta da *password*.
[210] F. SANTINI, *La corrispondenza elettronica aziendale tra diritto alla riservatezza e potere di controllo del datore di lavoro*, in *Arg. dir. lav.*, 2007, II.

Prima di arrivare all'art. 4 L. n. 300/70, così come oggi riformato, si riteneva già che fermo restando alcuni limiti di segretezza della posta elettronica aziendale questa potesse essere monitorata rispettando alcune precauzioni e principi generali. Tali precauzioni procedurali vengono fornite dal WP29 secondo cui deve essere redatta un'adeguata *policy* aziendale per definire le modalità di uso della posta elettronica in azienda chiarendo: (i) se il lavoratore ha diritto ad un indirizzo di posta elettronica per motivi esclusivamente personali, liceità dell'uso di altri indirizzi di posta elettronica a lavoro; (ii) accesso alla casella di posta elettronica aziendale in caso di assenza imprevista del dipendente; (iii) modalità di *backup* dei messaggi di posta elettronica e relativo periodo di conservazione; (iv) tempistica di cancellazione definitiva dei messaggi di posta elettronica; (v) sistemi di sicurezza utilizzati.

Il WP29 conclude affermando che per evitare la commistione tra dati personali privati del lavoratore e dati di rilevanza professionale ed aziendale il datore di lavoro dovrebbe limitare a priori la possibilità di usi privati della casella di posta elettronica privata aziendale fornendo i lavoratori anche un indirizzo di posta privata. In tal modo il lavoratore non avrebbe alcuna aspettativa di privatezza nell'uso della casella di posta elettronica aziendale che sarebbe pertanto monitorabile dal datore di lavoro, mentre al contrario, sarebbe precluso il controllo sulla casella fornita per uso privato[211].

Anche la giurisprudenza[212] prima della modifica del testo dell'art. 4 statutario aveva ritenuto che il datore di lavoro potesse controllare la posta elettronica aziendale messa a disposizione del lavoratore o per

[211] F. TOFFOLETTO, *op. cit*.
[212] Cass. 23 febbraio 2012, n. 2722; Tribunale di Milano, sez. penale, 10 maggio 2002.

ragioni di funzionalità aziendale oppure per la verifica della commissione di illeciti.

Il Garante per la protezione dei dati personali per cercare di chiarire i dubbi interpretativi degli operatori ha emanato il provvedimento del 1° marzo 2007 in ordine alle possibilità di monitoraggio della posta elettronica aziendale. Secondo tale provvedimento è essenziale la predisposizione di una *policy* aziendale che informi i lavoratori in ordine alle modalità di controllo della posta elettronica aziendale, al fine di consentire ai datori di lavoro di dimostrare il rispetto dell'onere di informazione che su di loro incombe[213].

Secondo parte della dottrina[214] l'adozione della *policy* aziendale sulla posta elettronica aziendale non sarebbe comunque sufficiente a ritenere rispettato l'onere di informazione a cui è tenuto il datore di lavoro, per tutti i casi di trattamento di dati personali non connaturato allo svolgimento in senso stretto del rapporto di lavoro (aventi la loro base giuridica nel contratto di lavoro) per i quali si rende necessaria una specifica informativa ed acquisizione del relativo consenso.

Sempre ai fini dell'inibizione preventiva di un uso illegittimo della posta elettronica aziendale, può essere utile per il datore di lavoro limitare dal punto di vista tecnico le modalità d'uso della stessa[215]. Ed infatti, il datore di lavoro può consentire l'invio di email soltanto ad indirizzi con

[213] Le indicazioni operative del Garante per la protezione dei dati personali sono mirate ad evitare la commistione tra dati personali privati e professionali ad esempio (i) creando indirizzi di posta elettronica condivisi tra più lavorati; (ii) fornitura di due indirizzi di posta elettronica, uno privato e l'altro professionale; (iii) comunicazione delle coordinate di un altro dipendente in caso di assenza del lavoro oppure nomina di un fiduciario che in caso di assenza imprevista del lavoratore possa controllare i messaggi del dipendente, possa controllare il contenuto dei messaggi di posta elettronica (iv) invio ai destinatari dell'email di una comunicazione sulla natura non privata dei messaggi.
[214] G. FAGGIOLI - A. ROZZA, *op. cit.*
[215] G. ANDREAZZA, *Posta elettronica su computer del lavoratore e limiti di conoscibilità del datore di lavoro*, in *Diritto penale e processo*, fasc. 2 n. 11/2008.

certi domini (@azienda – per usi interni), oppure limitare la dimensione degli allegati inviabili o ricevibili e comunque non scaricabili sui dispositivi aziendali.

Il controllo della casella di posta elettronica prima della modifica normativa dell'art. 4 era un controllo indiretto ed eccezionale che poteva essere giustificato soltanto per ragioni di funzionalità organizzativa o per sospetti illeciti (controlli difensivi), negli altri casi non vi era uniformità di interpretazione sulla sua legittimità o meno essendo preferibile, come analizzato, evitare a monte la necessità di controllo impedendo a priori degli usi privati o impropri della casella di posta elettronica aziendale. La *ratio* delle indicazioni del Garante è quella di attuare una "*procedimentalizzazione dell'impiego delle apparecchiature elettroniche, con una finalità marcatamente prevenzionistica rispetto ai rischi connessi ai possibili comportamenti opportunistici del datore di lavoro che utilizzi impropriamente le informazioni in suo possesso*"[216].

La modifica normativa dell'art. 4 statuario ha definitivamente chiarito la possibilità di controllo dei mezzi con i quali il lavoratore adempie la propria prestazione lavorativa, ivi incluso il controllo della posta elettronica aziendale. Il mutamento del quadro normativo ha portato il Garante per la protezione dei dati personali all'emanazione del provvedimento del 17 febbraio 2017 in materia di posta elettronica e cellulare aziendale dal momento che il provvedimento del 2007 non era più in grado di comporre gli interessi confliggenti nel rapporto di lavoro.

Il Garante con il provvedimento del 2017 rileva come effettivamente il datore di lavoro nell'ambito della novella normativa possa controllare l'esatto adempimento della prestazione professionale ed

[216] M. DEL CONTE, *op. cit*., pag. 505.

il corretto utilizzo degli strumenti di lavoro da parte dei dipendenti, ma ciò non comporta una liberalizzazione indiscriminata del potere di controllo del datore di lavoro che, in ogni caso, non può porre in essere un monitoraggio massivo ed ininterrotto della posta elettronica del lavoratore.

Ed infatti, la compressione della riservatezza dei lavoratori in favore dell'interesse al controllo degli strumenti lavorativi da parte del datore di lavoro ai sensi dell'art. 4, II comma, dello Statuto può avvenire lecitamente da parte del datore di lavoro ma soltanto quando essa sia proporzionata e motivata.

La possibilità di controllo della posta elettronica aziendale richiede comunque una adeguata informazione da parte del datore di lavoro nei confronti dei propri dipendenti sulle modalità del monitoraggio e di trattamento dei dati acquisiti.

La *ratio* dei provvedimenti e delle decisioni adottate dal Garante per la protezione dei dati personali nella vigenza del nuovo testo dell'art. 4 statutario e del GDPR è quella di permettere i controlli sulla casella di posta elettronica aziendale ma vietando monitoraggi indiscriminati, generalizzati[217], continui e sistematici[218].

[217] S. PETRILLI, *Internet e posta elettronica sul luogo di lavoro: il Garante ribadisce il divieto del controllo indiscriminato*, in *Azienditalia – il Personale*, 2016, 11.

[218] Provvedimento Garante per la protezione dei dati personali 1° febbraio 2018 n. 53 in Guida al Lavoro, n. 16 del 13 aprile 2018. In tale pronuncia il Garante ha ritenuto illegittimità la condotta di una società che conservava sul *server* aziendale tutte le email spedite e ricevute sugli account assegnati ai propri dipendenti per tutta la durata del rapporto di lavoro ed anche successivamente per eventuali contenziosi e comunque non era stata fornita una *policy* aziendale ai dipendenti sull'uso della posta elettronica. Secondo il Garante tale monitoraggio non risulta conforme alla disciplina *privacy* per due ragioni. In primo luogo, il monitoraggio sistematico di ogni email e il periodo di conservazione così dilatato non risultavano essere conformi ai principi di liceità, necessità e proporzionalità del trattamento. In secondo luogo, l'assenza della *policy* aziendale o comunque di qualsiasi informazione fornita ai lavoratori in ordine all'uso della casella di posta elettronica violano il principio di correttezza nel trattamento ed evidenziano il mancato rispetto dell'onere informativo da parte del datore di lavoro.

A ben vedere però vi è chi non ritiene legittimo il controllo della posta elettronica aziendale anche nella vigenza dell'attuale testo dell'art. 4 statutario. Ed infatti, sebbene in esso si affermi la possibilità di controllare gli strumenti per rendere la prestazione lavorativa, va rilevato che la casella di posta elettronica sia lo strumento lavorativo verificabile nella sua funzionalità, ma non il contenuto dei messaggi di posta i quali dovrebbero essere tutelati dalla normativa *privacy*. Si ritiene quindi che "*il semplice fatto che la casella email appartenga all'azienda, o che sia stata assegnata al lavoratore per ricevere ed inviare informazioni nell'interesse della stessa, non vale ad escludere la possibile rilevanza penale del comportamento di chi illegittimamente ne prenda conoscenza*"[219] diversamente opinando si confonderebbe il mezzo di trasporto del messaggio (di proprietà aziendale) con le informazioni.

In ogni caso non vi sono dubbi sulla illegittimità di controlli sulla casella di posta elettronica del lavoratore effettuati utilizzando *software* per la selezione dei messaggi per il controllo[220], dal momento che tali programmi non possono evidentemente rientrare nella categoria degli strumenti di lavoro e beneficiare dell'esenzione di cui al II comma dell'art. 4 statutario, dovendo procedersi per il loro utilizzo ed installazione alla procedura concertativa sindacale-amministrativa[221], salvo tali monitoraggi configurino dei controlli difensivi[222] necessari al fine della tutela del

[219] A. SITZIA, D. PEZZONIA, *il controllo del datore di lavoro su internet e posta elettronica: quale riservatezza sul luogo di lavoro?*, in *Nuova Giur. Civ.,* 2016, 6.
[220] P. DUI, *Monitoraggio della posta elettronica e accesso a internet,* in *Lav. Giur.,* 2010, 8.
[221] Cass. 23 febbraio 2010, n. 4375, la quale ha affermato che in caso di utilizzo dei *software* aggiuntivi per il controllo della posta elettronica essi devono essere installati soltanto dopo la procedura concertativa sindacale-amministrativa prevista dall'art. 4 L. n. 300/70.
[222]Sono numerose le pronunce della giurisprudenza di legittimità relative ai controlli difensivi occasionati da un controllo sulla casella di posta elettronica di un proprio dipendente. Si veda tra le altre, Cass. 23 febbraio 2012, n. 2722.

patrimonio aziendale, oppure l'immagine esterna dell'azienda che si presume possa essere lesa dalla condotta del proprio dipendente.

A ben vedere nonostante le novità normative il controllo della posta elettronica aziendale è tutt'altro che legittimo in ogni circostanza. Anzi, è necessario valutare caso per caso se esso sia o meno necessario e proporzionato ai fini del rispetto dei principi generali del GDPR, ma soprattutto se esso sia stato preceduto da un'adeguata informazione ai propri dipendenti così come richiesto dall'art. 4, III comma, dello Statuto, pena l'inutilizzabilità dei dati comunque acquisiti[223].

È evidente quindi che anche in tale quadro normativo la *policy* aziendale sulle modalità di utilizzo della casella di posta elettronica da parte del lavoratore resti l'elemento chiave nel contemperamento tra potere di controllo del datore di lavoro e riservatezza del lavoratore, sui soggetti abilitati all'accesso, sulla durata della conservazione dei messaggi e più in generale sulle modalità d'uso della posta elettronica.

In ogni caso sulla novella normativa dell'art. 4 statutario non vi è ancora uniformità di interpretazione circa l'applicabilità del II comma al controllo della posta elettronica aziendale, dal momento che alcuni la ritengono strumento di lavoro in generale, mentre altri, pur ritendendolo il mezzo attraverso il quale rendere la prestazione lavorativa, affermano che sia escluso da tale possibilità di monitoraggio il messaggio inviato tramite posta elettronica, svuotandone così il potere di verifica del datore di lavoro.

[223] Da ultimo il Tribunale di Roma con la sentenza del13 giugno 2018, n. 57668 in relazione ad un licenziamento avvenuto successivamente alla riforma dell'art. 4 dello Statuto dei lavoratori ha ritenuto illegittimo tale licenziamento poiché basato su addebiti formulati accendendo alla posta elettronica aziendale del lavoratore senza preventivamente fornire al dipendente un'adeguata informativa in ordine (i) al fatto che la sua attività avrebbe potuto essere controllata attraverso tali strumenti di lavoro e (ii) sulle modalità di svolgimento del controllo.

Per quanto riguarda invece il controllo sul computer aziendale non vi possono essere dubbi circa la sua ascrivibilità tra gli strumenti di lavoro e quindi in ordine al suo monitoraggio da parte del datore di lavoro.

Come già emerso per gli altri strumenti, per adempiere la prestazione lavorativa non possono ritenersi rientranti nella nozione di PC i *software* finalizzati al mero controllo mentre invece si nutrono dei dubbi sul monitoraggio della navigazione *internet*[224], nonostante il Garante per la protezione dei dati personali abbia incluso anche la navigazione *web* tra gli strumenti per rendere la prestazione lavorativa[225].

Secondo il Garante rientrano quindi nella funzione di strumenti lavorativi, esentati quindi dall'applicazione della procedura concertativa sindacale-amministrativa, solo servizi, *software* o applicativi strettamente funzionali alla prestazione lavorativa, nonché i servizi concernenti il profilo della sicurezza[226]. Inoltre, dal momento che l'esenzione dalla procedura concertativa prevista soltanto per gli strumenti per rendere la prestazione lavorativa è norma eccezionale derogatoria dei limiti (sostanziali e procedurali) posti al datore di lavoro, essa deve essere interpretata necessariamente in senso restrittivo senza alcuna possibilità di applicazione ad ipotesi analoghe.

Nel nuovo quadro normativo il datore di lavoro può verificare in ogni momento la correttezza dell'uso del PC aziendale fornito ai dipendenti in quanto esso nella impresa 2.0 rappresenta lo strumento di lavoro per eccellenza. In ogni caso deve essere fornita ai lavoratori

[224] A. SITZIA, *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in *Arg. Dir. Lav*. 2017, 3, 804 ss.
[225] Garante per la protezione dei dati personali provvedimento n. 303 del 13 luglio 2016.
[226] A. TROJSI, *Al cuore del nuovo art. 4, co. 2. St. Lav.: la delimitazione della fattispecie degli "strumenti utilizzati per rendere la prestazione lavorativa*, in *Rivista Italiana di diritto del lavoro,* fasc. 2, 2017.

un'adeguata informazione per impedirgli la formazione dell'aspettativa di privatezza nell'uso dello strumento lavorativo.

Per quanto riguarda invece gli accessi ad *internet*, così come per la posta elettronica, è bene procedere ad un'opera di prevenzione al fine di evitare la necessità di controllo. Ciò è possibile tramite l'impedimento del collegamento dei dispositivi aziendali a particolari siti quali *social network*, siti pornografici, oppure tramite l'attivazione di strumenti che impediscano la possibilità di *download* di *files* sul PC aziendale, ad eccezione di alcuni siti preventivamente individuati dal datore di lavoro necessari per finalità professionali.

Nella *policy* aziendale da predisporre, anche per l'uso del PC aziendale e gli accessi ad internet dovrà essere chiarito in che limiti è consentito l'uso privato della navigazione ai lavoratori, dal momento che impedirlo in via assoluta significa non tenere in considerazione il fatto che comunque il *web* può essere di grande aiuto nella vita quotidiana dei propri dipendenti.

Pertanto, come precisato dal WP29[227], il datore di lavoro deve indicare ai propri dipendenti: (i) le condizioni in cui è consentito l'uso privato di *internet*; (ii) i divieti di accesso ad alcuni siti indicando le modalità attraverso le quali constatare gli abusi; (iii) le modalità di partecipazione dei propri rappresentanti sindacali nell'indagine per le presunte infrazioni.

Nonostante il mutato quadro normativo, al fine della corretta applicazione dei principi generali in materia di *privacy*[228] sono ancora determinanti a livello interpretativo le indicazioni contenute nelle Linee

[227] *Opinion 8/2001 on the processing of personal data in the Employment context*.
[228] P. J. NATALI, *Navigazione internet dei lavoratori e tutela della privacy*, in *Diritto & Pratica del Lavoro*, n.32-33/2015.

guida del Garante per la protezione dei dati personali del 1° marzo 2007[229]. Ed infatti, tali Linee guida, al di là delle misure tecniche pratiche consigliate per la prevenzione dei controlli, stabiliscono che i trattamenti dei dati personali acquisiti tramite monitoraggi di accessi internet debbano rispettare i principi di necessità, di correttezza, di pertinenza e non eccedenza, nella misura meno invasiva possibile, tenendo anche conto del principio di segretezza della corrispondenza.

I controlli effettuati sul PC aziendale (senza *software* aggiuntivi), nella vigenza del nuovo testo dell'art. 4 statutario, sono esenti dall'applicazione della procedura concertativa sindacale-amministrativa, ma devono comunque rispettare i principi citati. Il controllo sul PC aziendale ed il monitoraggio degli accessi internet è legittimo anche nei casi in cui venga posto in essere con dei *software* specifici per il controllo dei dati purché vi siano esigenze specifiche (organizzative e produttive, di sicurezza del lavoro o di tutela del patrimonio aziendale) e la loro installazione sia preceduta dalla procedura concertativa di cui all'art. 4, comma I, dello Statuto ed ai lavoratori venga fornita un'adeguata informazione sulle modalità di utilizzo del sistema informatico.

Ed infatti, oggi i controlli preterintenzionali sul monitoraggio degli accessi ad internet sono legittimi anche per esigenze di tutela del patrimonio aziendale, nel quale è ascrivibile anche la struttura informatica che potrebbe essere compromessa da un'indebita ed illegittima navigazione *web* su siti non sicuri da parte del dipendente.

[229] Anche in tale provvedimento del Garante, così come nell'*Opinion* del WP29 per ridurre il rischio di usi impropri dei pc e della navigazione *web* è fondamentale adottare opportune misure per prevenire la necessità di controlli sul lavoratore: (i) categorie di siti visitabili; (ii) filtri che prevengano determinate operazioni; (iii) trattamento dei dati in forma anonima e pseudonomizzazione dei dati; (iv) conservazione dei dati per il periodo strettamente necessario.

In tale contesto l'utilizzo del PC e di *internet* da parte dei dipendenti può essere oggetto di analisi, profilazione e integrale ricostruzione mediante *files log* della navigazione *online*, sempre però nel rispetto dei principi della normativa generale *privacy* (GDPR). Pertanto, non possono considerarsi legittime le ipotesi di monitoraggio indiscriminato delle pagine *web* visitate oppure di ogni operazione compiuta sul PC aziendale poiché ciò configurerebbe una violazione del principio di proporzionalità e, quindi, un controllo a distanza illegittimo.

È evidente quindi che per il rispetto dell'art. 4, III comma, statutario, nonché per evitare la formazione di un'aspettativa di riservatezza nell'uso del PC aziendale e della navigazione *web*, la predisposizione della *policy* aziendale per specificare le modalità d'uso di ogni strumento lavorativo messo a disposizione al lavoratore resta lo strumento più idoneo a cui deve ricorrere il datore di lavoro per non incorrere in trattamenti dei dati illegittimi.

3.5 Il controllo dei *social networks*

L'uso dei *social network*[230] nel mondo del lavoro è ormai una prassi diffusissima per finalità legate sia all'attività lavorativa (es. *Linkedin*[231]) che extra lavorativa (es. *Facebook*[232]).

Ed infatti, se in passato l'uso dei *social network* da parte dei lavoratori poneva soltanto delle criticità circa la sottrazione del tempo di lavoro in favore di un uso personale dei dispositivi aziendali e la possibilità di acquisizione di dati personali estranei dal rapporto di lavoro, oggi non è più così, poiché in alcune particolari professioni il *social network* può essere considerato uno degli strumenti per l'adempimento della prestazione lavorativa[233], oppure perché alcuni *social network* hanno per scopo stesso quello di essere uno strumento utile per l'attività lavorativa.

Linkedin, per citarne uno, consente di reperire candidati per specifiche posizioni lavorative oppure di pubblicare offerte di lavoro ed interfacciarsi in rete con le possibili risorse da inserire in azienda. Tale uso del *social* è evidente che possa essere di grande valore pratico per il settore delle risorse umane in fase di selezione dei candidati per l'instaurazione del rapporto di lavoro[234]. Al punto che alcuni *social network* specialisti

---

[230] I *social network* sono dei siti *web* o programmi sui quali è possibile comunicare e fornire informazioni con altri utenti utilizzando la rete *internet.*

[231] *Linkedin* è il principale *social network* dedicato al business e all'attività lavorativa in tutti i suoi aspetti ovvero per comunicare con la propria rete di clienti o colleghi, per cercare o condividere informazioni lavorative oppure offrire o reperire nuove opportunità lavorative.

[232] *Facebook* è invece il principale *social network* generalista ideato per consentire agli utenti di essere collegati alla propria rete di amici tramite il *web* comunicando con essi e condividendo informazioni. Tale uso iniziale di *Facebook* è poi cambiato nel tempo dal momento che oggi esso viene utilizzato come un canale generalista di comunicazione di ogni tipo di contenuti e non più ristretta alla sola cerchia di propri contatti (tramite delle sponsorizzazioni finalizzate al *marketing online*).

[233] Si pensi ai settori del *social media communication, social media marketing, social media management*.

[234] A. DONINI, *Mercato del lavoro sul web: regole e opportunità*, in *Diritto delle Relazioni Industriali*, fasc. 5, 2015, che analizza diffusamente il rapporto tra domanda-offerta di lavoro nel *web*.

hanno persino ottenuto l'autorizzazione allo svolgimento di attività di intermediazione, inserendosi nel sistema dei servizi per l'impiego[235].

Facebook invece, per citare un *social* generalista, consente gli usi più disparati, tanto da poter essere utile anche per alcune funzioni aziendali come ad esempio a raggiungere la propria clientela oppure comunicare tramite specifici gruppi creati *ad hoc* con il proprio personale.

Al di là degli usi possibili dei *social network* è evidente che essi possano comportare notevoli rischi per la *privacy* sia dei lavoratori candidati sia dei terzi con i quali vengono condivisi alcuni dati personali. I *social network* presentano un rischio della riservatezza molto elevato, dal momento che i dati una volta pubblicati *online* fuoriescono dalla disponibilità del titolare con una possibilità molto elevata di diffusione anche a terzi (proporzionata alla gestione delle impostazioni della riservatezza di ciascun profilo[236]).

È evidente che per prevenire tali rischi occorre sviluppare anche all'interno delle aziende delle regole chiare e precise di organizzazione e gestione che consentano un uso consapevole e limitato dei *social network*, impendendo, ad esempio, la pubblicazione di dati acquisiti nello svolgimento della propria prestazione lavorativa sulla "piazza virtuale"[237].

Pertanto, anche relativamente a tale strumento informatico, che a volte può persino configurarsi come strumento lavorativo, è essenziale predisporre un'adeguata *policy* aziendale per rendere edotti i lavoratori

[235] Si pensi ad esempio a Monster Italia, iscritta all'albo delle agenzie del lavoro, sez. IV, che mette a disposizione degli utenti una bacheca ed un apposito *networking* per fungere da possibili punti di incontro.

[236] Sul punto è dirimente la diffusione delle informazioni pubblicate sul *social network.* Ed infatti, sarà maggiormente lesivo un profilo dell'utente/lavoratore aperto a chiunque (ivi incluso il datore di lavoro per le finalità di controllo) piuttosto che il profilo visibile soltanto da utenti qualificati e circoscritti.

[237] L.C. NATALI, *Uso dei social network da parte dei lavoratori*, in *Diritto & Pratica del Lavoro*, n. 29/2018.

circa gli usi consentiti di tali mezzi, dal momento che laddove il loro uso venga consentito, anche parzialmente, l'azienda dovrà prestare delle maggiori cautele dal punto di vista informatico. Sul punto infatti, va segnalata la difficoltà di individuare il titolare del trattamento dei dati nei trattamenti svolti a mezzo *social network*, nonostante non vi siano dubbi sull'applicabilità del GDPR anche a tali fattispecie e comunque sia in corso di definizione il Regolamento europeo dell'*e-privacy*[238].

Anche relativamente all'uso dei *social network*, in ragione della loro elevata potenzialità lesiva, è opportuno intervenire preventivamente piuttosto che eseguire dei controlli postumi. Ed infatti, nelle già citate Linee guida del Garante del 1° marzo 2007 in materia di utilizzo di *internet* e posta elettronica vi sono delle cautele operative dirette o adattabili all'uso *dei social network* tra cui: (i) la predisposizione di *standard* minimi di sicurezza elevati; (ii) l'adattamento delle misure di sicurezza alle specificità del *social network* utilizzato in azienda, o comunque il cui uso è consentito al dipendente; (iii) la sottoposizione ai dipendenti di adeguata informativa sull'uso dei *social network* e responsabilizzazione degli stessi in caso di utilizzo di tali strumenti; (iv) la mancata utilizzazione del nome del lavoratore o quello dell'azienda (salvo profilo istituzionale) e quindi preferire degli pseudonimi; (v) l'utilizzazione delle impostazioni orientate alla *privacy* limitando al massimo la disponibilità altrui dei propri dati personali.

In ragione della polivalenza del *social network* esso può essere utilizzato come strumento principale per rendere la prestazione lavorativa per alcune professioni. In tali casi, i lavoratori vengono forniti di

[238] Il Regolamento europeo dell'*e-privacy* sostituirà la vecchia direttiva *e-privacy* (2002/58/CE) adattando la *privacy* alle nuove sfide che l'evoluzione tecnica del mondo digitale ha posto. A titolo esemplificativo verrà disciplinata la *privacy* relativamente ai metadati, ai *cookies* ed in generale ai dati delle comunicazioni elettroniche.

credenziali per accedere ad un certo profilo aziendale che potrà sempre essere monitorato dal datore di lavoro con la possibilità di acquisire i dati ed utilizzarli come prove dal combinato disposto dei commi 2-3 dell'art. 4 L. n. 300/70. Pertanto, il lavoratore che viene reso edotto della natura di strumento di lavoro (nonché delle modalità d'uso) del *social* che gli viene messo a disposizione non può vantare alcuna aspettativa di privatezza nell'uso dello stesso, anche se tramite codesto canale comunichi delle informazioni di carattere strettamente personale, dal momento che il datore di lavoro è nel pieno potere di sorvegliare a distanza tali strumenti, sempre nel rispetto dei principi generali sanciti dalla normativa generale.

Il *social network* può altresì essere un mezzo di controllo del lavoratore molto efficace, poiché consente al datore di lavoro di conoscere alcune informazioni della vita privata del lavoratore che egli decide di condividere nella "pubblica piazza virtuale". L'accesso alle pagine personale dei *social* dei propri dipendenti, purché motivato da esigenze specifiche (es. sospetto di illecito) non sembra configurare un'intromissione illegittima dal momento che sono gli stessi lavoratori che, pubblicando alcuni dati personali *online*, decidono di rinunciare a parte della loro sfera privata condividendo con il *web* delle informazioni anche di carattere personale che a volte possono avere rilevanza anche ai fini del rapporto di lavoro. A ben vedere però va segnalato che parte della dottrina[239] ritiene che anche per tali controlli sia necessaria la procedura concertativa di cui all'art. 4 statutario, aderendo a quell'orientamento che nella nuova formulazione della norma statutaria ritiene tale procedura applicabile a tutti i controlli difensivi.

[239] A. INGRAO, *Il controllo a distanza realizzato mediante Social network,* in *Labour and Law Issues*, vol. 2 n. 1, 2016.

Il datore di lavoro grazie ai *social network* ha quindi la possibilità di verificare alcune informazioni personali anche di rilevanza disciplinare per il rapporto di lavoro per concessione dello stesso lavoratore che, condividendo tali informazioni con la generalità degli utenti *web,* ha accettato che esse possano essere acquisite anche dalla loro controparte contrattuale.

Sui controlli dei lavoratori realizzati tramite *social network* vi è un'ampia casistica[240] e la giurisprudenza di legittimità è persino arrivata a considerare legittima la condotta di un responsabile del personale che ha creato un profilo falso di una donna per mettersi in contatto con un dipendente ed accertarne le conversazioni telefoniche via internet durante l'orario di lavoro localizzandone altresì la posizione nei locali aziendali[241]. Tale comportamento datoriale, che di fatto realizza un controllo difensivo occulto, è stato ritenuto legittimo dal momento che esso era rivolto ad accertare comportamenti illeciti del dipendente (diversi dal mero inadempimento dell'attività lavorativa), ovvero una serie di "distrazioni" che insieme ad altre precedentemente contestate metteva a rischio il patrimonio aziendale[242].

Dall'altro lato anche commenti negativi e denigratori nei confronti del datore di lavoro possono configurare una responsabilità disciplinare

[240] Tribunale di Milano, ordinanza del 1° agosto 2014, in RIDL, 2014, in cui è stato considerato legittimo il licenziamento per giusta causa comminato nei confronti di un lavoratore che durante l'orario di lavoro aveva scattato e pubblicato delle foto tali da provare l'allontanamento dal posto di lavoro e la conseguente interruzione della prestazione. Ed ancora, il Garante per la protezione dei dati personali con nota del 26 agosto 2010 che si è pronunciato sul caso di un dipendente aveva pubblicato nel proprio profilo personale *Facebook,* quindi visibili ad "amici di amici", delle foto dalle quali erano visibili dei disegni coperti dal segreto industriale.
[241] A. VALLEBONA, *Nota a Cass. 27 maggio 2015, n. 10955*, in *Massimario di Giurisprudenza del Lavoro,* 2016, 286.
[242] V. AMATO, *Legittimità del controllo difensivo occulto attraverso i social networks, nota a Cass. 27 maggio 2015, n. 10955*, nel Lavoro nella giurisprudenza n. 10/2015.

del lavoratore[243], dal momento che le dichiarazioni del dipendente espresse in rete equivalgono a quelle effettuate all'interno dell'azienda ed anzi, a ben vedere, hanno una portata lesiva maggiore in quanto sono direttamente accessibili da più utenti[244]. Di tale orientamento[245] è stato il T.A.R. Lombardia[246] che ha confermato la sospensione dal lavoro e dalla paga nei confronti di un dipendente di un'amministrazione penitenziaria, per aver espresso disvalore nei confronti dell'operato della pubblica amministrazione cui era dipendente tramite il *like* ad un commento negativo di un altro utente del *social network*. L'assoggettamento del lavoratore al potere disciplinare anche nell'uso dei *social network* non è una limitazione della libertà di pensiero o di espressione del proprio dipendente, ma soltanto "l'altra faccia della medaglia" dell'obbligo di diligenza e fedeltà che il lavoratore particolarmente attivo sui *social network* deve saper conciliare con l'attività lavorativa, astenendosi dai comportamenti suscettibili di danneggiare, anche solo potenzialmente, il datore di lavoro[247].

---

[243] I. LEVERONE, *Legittimo il licenziamento del lavoratore che pubblica su Facebook commenti denigratori del datore di lavoro,* nota a Cass. civ. 27 aprile 2018, n. 10280, in *Diritto&Giustizia*, fasc. 77, 2018. Nel caso di specie è stato ritenuto legittimo il licenziamento di una lavoratrice che sulla propria bacheca *Facebook* ha espresso disprezzo per l'azienda in cui era impiegata preannunciando l'intenzione di ricorrere fittiziamente all'assenza per malattia, ritenendo che tale condotta integra la fattispecie di reato di diffamazione ed integra la giusta causa di licenziamento idonea a ledere irrimediabilmente il vincolo fiduciario.

[244] F. IAQUINTA – A. INGRAO, *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, in *Dir. Rel. Int.,* 4/2014. In tale contributo viene dato atto dell'esistenza di un gruppo sul social network Facebook nel quale gli utenti raccontano la loro storia lavorativa cessata per le opinioni e i commenti espressi o le esperienze immortalata in foto postate sulla rete.

[245] Fanno parte di tale orientamento: (i) Tribunale di Ivrea, ordinanza del 28 gennaio 2015 che ha confermato il licenziamento per giusta causa a seguito di un *post* diffamatorio pubblicato su *Facebook* da parte del lavoratore ai danni dell'azienda e di altri dipendenti; (ii) Tribunale di Milano, 1 agosto 2014 che ha confermato il licenziamento di un dipendente per aver pubblicato su *Facebook* delle fotografie scattate durante l'orario di lavoro, accompagnate da commenti offensivi riferiti all'azienda.

[246] T.A.R. Lombardia, Sez. III, 3 marzo 2016, n. 246.

[247] M. COTTONE, *Social Network: limiti alla libertà d'espressione e riflessi sul rapporto di lavoro (il "Like"), nota a T.A.R. Lombardia, Sez. III, 3 marzo 2016, n. 246*, in il Lavoro nella giurisprudenza, n. 4/2017.

In considerazione dell'importanza dei *social network* nella società informatizza e soprattutto per le nuove generazioni (presenti o futuri lavoratori), si pensi ai *Millennials*[248], è naturale che il datore di lavoro abbia sviluppato il desiderio di controllare la condotta dei propri dipendenti sulla piattaforma digitale anche al fine di valutare il rispetto del loro obbligo di diligenza e fedeltà.

Diverso è invece il controllo realizzato tramite l'aggregazione delle informazioni rilasciate dalla navigazione sui *social network* rilasciate dai propri dipendenti sui dispositivi informatici aziendali che determini una profilazione degli utenti, il cui trattamento è però precluso sia dall'art. 8 L. n. 300/70 (divieto di indagare su opinioni e abitudini dei propri lavoratori) ma anche dell'art. 4 dello Statuto dal momento che per profilare la navigazione sui *social network* da parte dei propri dipendenti sarebbe necessario installare sui dispositivi informatici aziendali dei *software* aggiuntivi che come tali realizzino dei controlli a distanza (leciti soltanto se preceduti dalla procedura concertativa sindacale-amministrativa).

Salvo la particolare ipotesi pocanzi citata nella quale i controlli sono da ritenersi vietati, il controllo dei *social network* è un controllo legittimo poiché è il lavoratore che sceglie di disporre del proprio diritto alla riservatezza limitandolo *online* nei confronti di una serie indefinita di soggetti ivi incluso il datore di lavoro. Pertanto, in tale quadro, viene indebolita la porta precettiva dell'art. 8 statutario anche in considerazione della mutata percezione della *privacy* nel contesto sociale. Tale articolo sebbene immutato nel testo risulta essere "*schiacciato: l'art. 4 St. lav. la cui vocazione dominante è stata avallata e rafforzata dalla novella del*

[248] Con tale termine si indicano convenzionalmente i nati tra gli anni '80 e l'anno 2000. Tale generazione ha come tratto distintivo rispetto alle altre una maggiore propensione alla comunicazione, ai *media,* alle nuove tecnologie digitali e che vive la rete non più come un mezzo a cui connettersi ma uno dei canali principali dove vivere.

2015, la disciplina generale che, continuando a viaggiare in parallelo rispetto alla disciplina speciale in tema di controlli sulle opinioni, si rivela un passepartout capace di superare chiusure poco realistiche nel mondo moderno"[249].

In conclusione, il datore di lavoro nel contesto normativo definito dal GDPR e dal novellato art. 4 statutario potrà sempre controllare il profilo social dei dipendenti che utilizzino la piattaforma *social* per effettuare la propria prestazione lavorativa (profilo aziendale le cui credenziali saranno messe a disposizione dallo stesso datore di lavoro), in via eccezionale potrà controllare anche i profili *social* personali dei propri dipendenti ma soltanto quando ciò sia legittimato da una motivata esigenza di controllo (ad esempio sospetto di un illecito) nel rispetto della principio di proporzionalità e necessità del trattamento imposto dalla normativa generale *privacy* (nonostante la disponibilità di informazioni nella rete) ed infine gli sarà vietato il monitoraggio dei *social network* realizzato tramite *software* specifici finalizzati al solo controllo a distanza (utilizzabili soltanto previo esperimento della procedura concertativa di cui all'art. 4, I comma, L. n. 300/70).

In ogni caso però le informazioni acquisite tramite il controllo realizzato sulla piattaforma *social network* per finalità lavorative saranno utilizzabili da parte del datore di lavoro soltanto se sia stata conferita ai lavoratori un'adeguata informazione nel rispetto dei principi generali di trasparenza e correttezza.

[249] L. TEBANO, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?,* in *Rivista Italiana di Diritto del Lavoro*, fasc. 3, 2016, pag. 345.

BIBLIOGRAFIA

AA. VV., *La nuova disciplina della privacy*, commentario diretto da S. SICA E P. STANZIONE, Bologna, Zanichelli, 2004.

ALVINO I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra regole dello Statuto dei lavoratori e quelle del Codice della privacy*, in *Labour law issues*, 2/2016.

ALVINO I.*, L'articolo 4 dello Statuto dei lavoratori alla prova di internet e della posta elettronica,* in *Diritto delle relazioni industriali*, 4, 2014.

AMATO V., *Legittimità del controllo difensivo occulto attraverso i social networks, nota a Cass. 27 maggio 2015, n. 10955*, nel Lavoro nella giurisprudenza n. 10/2015.

AMOROSO G., DI CERBO V. e MARESCA A., *Diritto del lavoro vol. 1, sub art. 8*, Milano, Giuffré, 2013.

ANDREAZZA G., *Posta elettronica su computer del lavoratore e limiti di conoscibilità del datore di lavoro*, in *Diritto penale e processo*, fasc. 2 n. 11/2008.

ARBORE A., *La nuova disciplina dei controlli ex art. 4 St. Lav.,* in GHERA E. –GAROFALO D. (a cura di), *Semplificazioni – sanzioni - ispezioni nel Jobs Act 2,* Bari, Cacucci, 2016, 161 ss.

AULETTA T. A., *Riservatezza e tutela della personalità*, Giuffrè, Milano, 1978.

BARRACO E., SITZIA A., *La tutela della privacy nei rapporti di lavoro*, in *Monografie di diritto del lavoro*, dirette da MISCIONE M., Milano, Ipsoa, 2008.

BARRACO E., *La tutela della privacy: la riservatezza del lavoratore*, in *Diritto e Pratica del Lavoro*, 19/2018.

BARRACO E., *Strumenti di lavoro e controllo a distanza*, in *Diritto & Pratica del Lavoro*, 31/2018 pag. 1943.

BELLAVISTA A., *Controlli a distanza e necessità del rispetto della procedura di cui al comma 2 dell'art. 4 St. lav.*, in *Riv. giur. lav.*, 2008, II, pp. 358 ss.

BELLAVISTA A., *Dignità e riservatezza*, in P. Lambertucci (a cura di), *Dizionari del diritto privato. Diritto del lavoro*, Milano, Giuffré, 2010.

BELLAVISTA A., *I poteri dell'imprenditore e la privacy del lavoratore*, in *Il diritto del lavoro*, fasc. 3, 2002.

BELLAVISTA A., *Il controllo sui lavoratori*, Torino, Giappichelli, 1995.

BELLAVISTA A., *Sorveglianza, privacy e rapporto di lavoro*, in *Dir. internet*, 5, 2006.

BIFULCO R., CELOTTO A., OLIVETTI M., *Commentario alla Costituzione*, vol. I, Torino, UTET 2006.

BUTTARELLI G., *Banche dati e tutela della riservatezza, La privacy nella società dell'informazione*. *Commento analitico alle Leggi 31 dicembre 1996 n. 675 e 676*, Milano, Giuffré, 1997.

CAIRO L., *Orientamenti della giurisprudenza in tema di controlli difensivi*, in *Guida Dir*. n. 37/2007.

CARACCIOLO DI MELISSANO F., *Uso illegittimo del telefono aziendale e licenziamento. I profili della riservatezza del lavoratore*, in *Dir. merc. lav.,* 2012, II.

CARDARELLI F., SICA S., ZENO-ZENCOVICH V*., Il codice dei dati personali - temi e problemi*, Milano, Giuffrè, 2004.

CATAUDELLA A., *Scritti giuridici*, Padova, Cedam, 1991.

CHIECO P., *Privacy e lavoro. La disciplina del trattamento dei dati personali del lavoratore*, Bari, Cacucci, 2000, pag. 12.

CONSONNI G., *Il caso Barbulescu c. Romania e il potere di controllo a distanza dopo il Jobs Act: la normativa europea e italiana a confronto,* in *Dir. Rel. Ind*., 2016, 4.

COSATTINI L.A, *Le modifiche all'art. 4 st. lav. sui controlli a distanza, tanto rumore per nulla?,* in *Lav. giur.* 2015, n. 11.

COTTONE M., *Social Network: limiti alla libertà d'espressione e riflessi sul rapporto di lavoro (il "Like"), nota a T.A.R. Lombardia, Sez. III, 3 marzo 2016, n. 246*, in il Lavoro nella giurisprudenza, n. 4/2017

CRISCULO C., *Controlli difensivi e Codice della "privacy", Nota a Cass. sez. I civ. 19 settembre 2016, n. 18302; Cass. sez. lav. 5 ottobre 2016, n. 19922,* in *Rivista italiana di diritto del lavoro,* 2017, fasc. 1, pt. 2, pp. 39-46.

DALLACASA M., *Il controllo delle attività informatiche e telematiche del lavoratore*, nel Lavoro nella giurisprudenza, 7/2017.

DAGNINO E., *People Analytics: lavoro e tutele al tempo del management tramite big data*, ADAPT University Press, 2017.

DE LUCA V., CANNONE E., IACOBELLIS A., VELLA L., PORTARO L., *Privacy in azienda. La nuova disciplina dal 25 maggio 2018*, Studio Legale De Luca & Partners (a cura di), in *Guida al Lavoro* n. 17 del 20 aprile 2018.

DE LUCA TAMAJO R., *I controlli sui lavoratori*, in *i poteri del datore di lavoro nell'impresa*, ZILIO GRANDI G. (a cura di), Atti del convegno di Studi Venezia 12 aprile 2002, Padova, 2002.

DE LUCA TAMAJO R., *Nuove tecnologie e tutela della riservatezza dei lavoratori*, F. Angeli, 1988.

DEL CONTE M., *Internet, posta elettronica e oltre: il Garante della privacy rimodula i poteri del datore di lavoro*, in *Dir. Informatica*, vol. 23, n. 3, 2007.

DEL PUNTA R., *La nuova disciplina del controllo a distanza sul lavoro (art. 23 D.Lgs. 151/2015),* in *RIDL*, 1/2016.

DI FRANCESCO M., *Licenziamento per giusta causa e controlli difensivi occulti*, in *Diritto & Pratica del lavoro*, 34-35/2017.

DONINI A., *Mercato del lavoro sul web: regole e opportunità*, in *Diritto delle Relazioni Industriali*, fasc. 5, 2015.

DONINI A., *Profilazione reputazionale e tutela del lavoratore: la parola al Garante della Privacy*, in *Labour&Law Issues*, vol. 3, n. 1, 2017.

DOSSI G., *Controlli a distanza e legalità della prova: tra esigenze difensive del datore di lavoro e tutela della dignità del lavoratore,* in *Dir. Rel. Ind.*, 2010

DUI P., *Monitoraggio della posta elettronica e accesso a internet,* in *Lav. Giur.,* 2010, 8.

FAGGIOLI G. –ROZZA A., *Privacy per posta elettronica e internet in azienda*, Roma, Cesi Professionale, 2008.

FREDIANI M., *La delazione protetta quale diritto-dovere alla segnalazione d'allarme*, in *Il lavoro nella giurisprudenza*, n. 3/2018.

GAMBA C., *Il controllo a distanza dei lavoratori e l'utilizzabilità delle prove*, in *Labour law issues*, vol. 2, n. 1/2016.

GAETA L.*, La dignità del lavoratore e i turbamenti dell'innovazione* in *Lav. Dir*., 203, 1990.

GENTILE D., *Tracking satellitare mediante GPS: attività atipica di indagine o intercettazione di dati? Nota a Cass. pen. 10 marzo 2010, n. 9667,* in Diritto penale e processo n. 12/2010.

GHIRIBELLI A., *Il diritto alla privacy nella Costituzione italiana*, in Teutas (sito istituzionale – *www.teutas,it*), 30 novembre 2007.

GRANDI M., *Persona e contratto di lavoro. Riflessioni storico critiche sul lavoro come oggetto del contratto di lavoro*, in *Arg. dir. lav*., 1999, 309.

GREMIGNI P., *La normativa italiana sulla privacy si adegua a quella europea*, in *Guida al Lavoro*, n. 36/2018.

IAQUINTA F. –INGRAO A., *La privacy e i dati sensibili del lavoratore legati all'utilizzo di social networks. Quando prevenire è meglio che curare*, in *Dir. Rel. Int*., 4/2014.

ICHINO P., *Il contratto di lavoro*, in *Trattato di diritto civile e commerciale*, Tomo III, Milano, Giuffrè, 2003.

IMPERIALI R., IMPERIALI R., *Controlli sul lavoratore e tecnologie,* Milano, Giuffré, 2012.

INGRAO A., *Il controllo a distanza realizzato mediante Social network,* in *Labour and Law Issues*, vol. 2 n. 1, 2016.

INGRAO A.*, Il controllo disciplinare e la "privacy" del lavoratore dopo il "Jobs act"***, nota a Cass. sez. I civ. 19 settembre 2016, n. 18302; Cass. sez. lav. 5 ottobre 2016, n. 19922,* in *Rivista italiana di diritto del lavoro,* 2017, fasc. 1, pt. 2, pp. 46-54.

LAMBERTUCCI P., *I poteri del datore di lavoro nello Statuto dei lavoratori dopo l'attuazione del c.d. jobs act del 2015: primi spunti di riflessione,* in Arg. dir. lav., 2016, 530 ss.

LAMBERTUCCI P., *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act),* WP (Working Papers) C.S.D.L.E. "Massimo D'Antona" IT - 255/2015.

LAMBROU M., *Geolocalizzazione di veicoli aziendali,* in *Diritto & Pratica del Lavoro* 5/2018.

LANOTTE M., *La ridefinizione dei limiti al potere di controllo a distanza,* in LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza Lo Statuto dei lavoratori dopo il Jobs Act*, Milano, Giuffré, 2016.

LEVERONE I., *Legittimo il licenziamento del lavoratore che pubblica su Facebook commenti denigratori del datore di lavoro,* nota a Cass. civ. 27 aprile 2018, n. 10280, in *Diritto&Giustizia*, fasc. 77, 2018.

LEVI A., *Il controllo informatico sull'attività del lavoratore*, Torino, Giappichelli, 2013.

LISO F., *Computer e controllo dei lavoratori*, in *Dir. lav. rel. Ind*., 1986.

MAIO V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. Dir. Lav*., 6/2015, pp. 1186 ss.

MARAZZA M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in Arg. dir. lav., 2016, pp. 485 ss.

MARESCA A., *Controlli tecnologici tutele del lavoratore nel nuovo art. 4 dello Statuto dei lavoratori, in Rivista Italiana di diritto del lavoro*, 2016, pag. 513 e ss.

MARESCA A., *Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore*, in *Forum Tuttolavoro Ipsoa,* 2016.

MCAFEE A., *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges*, Harvard Business Review Press, 2009.

MISCIONE M., *I controlli intenzionali, preterintenzionali e difensivi sui lavoratori in contenzioso continuo,* in *Lav. giur.*, n. 8-9/2013.

MONTUSCHI L., *Potere disciplinare e rapporto di lavoro*, Milano, Giuffré, 1973.

NAPOLI M., *Lo Statuto dei lavoratori ha quarant'anni, ben portati*, in *Lav. dir.*, 2010.

NATALI L.C., *Uso dei social network da parte dei lavoratori*, in *Diritto & Pratica del Lavoro*, n. 29/2018.

NATALI P. J., *Navigazione internet dei lavoratori e tutela della privacy*, in *Diritto & Pratica del Lavoro*, n.32-33/2015.

NISSENBAUM H., *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Stanford University Press, 2009.

NUNIN R., *Utilizzo di dati biometrici da parte del datore di lavoro: la prescrizione del garante per la privacy*, in *Lav. nella giur.*, 2007, Vol. n. 15 fasc. 2.

NUZZO V., *La protezione del lavoratore dai controlli impersonali*, Napoli, Editoriale Scientifica, 2018

OGRISEG C., *GDPR and Personal Data Protection in the Employment context,* in *Labour Law Issues*, vol. 3, n. 2, 2017.

PERRONE F., *La tutela della privacy sul luogo di lavoro: il rinnovato dialogo tra Corte Europea dei diritti dell'Uomo e giurisdizione nazionale dopo la sentenza Barbulescu 2*, in *Labor – Il lavoro nel diritto* n. 3/2018.

PETRILLI S., *Internet e posta elettronica sul luogo di lavoro: il Garante ribadisce il divieto del controllo indiscriminato*, in *Azienditalia – il Personale*, 2016, 11.

PIZZONIA D., *Controllo della posta elettronica, tutela della privacy e potere di controllo*, in *Rivista giuridica del lavoro e della previdenza sociale*, fasc. 4, 2008.

POLICELLA E.O., *Le linee-guida del Garante sull'uso di internet e posta elettronica: conseguenze sanzionatorie*, in Lav. Giur. n. 4/2008.

PROIA G., *Trattamento dei dati personali, rapporto di lavoro e l'"impatto" della nuova disciplina dei controlli a distanza, in Rivista Italiana di diritto del lavoro*, 2016, pp. 547 e ss.

RAUSEI P., *Tutto Jobs Act. La nuova dottrina del lavoro,* Milano, Ipsoa, 2016.

RECCHIA G.A., *Controlli datoriali difensivi: note su una categoria in via di estinzione*, in Lavoro nella giurisprudenza, 4/2017.

RODOTA' S., *Intervista su privacy e libertà*, Bari, Laterza, 2005.

RUSSO A., TUFO M., *I controlli preterintenzionali: la nozione*, in LEVI A. (a cura di), *Il nuovo art. 4 sui controlli a distanza. Lo statuto dei lavoratori dopo il Jobs Act*, Milano, Giuffrè, 2016.

SALAZAR P. e FAILLA L., *Controlli difensivi: quali limiti nel nuovo contesto dell'art. 4, L. n. 300/1970,* in *Il lavoro nella giurisprudenza*, 2/2017.

SALIMBENI M.T., *Il controllo a distanza sull'attività dei lavoratori: la sopravvivenza dell'art. 4 sugli impianti audiovisivi*, in *Dir. lav. merc*., 2010, pp. 795 ss.

SALIMBENI M.T., *La riforma dell'art. 4 dello statuto dei lavoratori: l'ambigua risolutezza del legislatore,* in *Riv. It. Dir. lav*., 2015 n. 4.

F. SANTINI, *La corrispondenza elettronica aziendale tra diritto alla riservatezza e potere di controllo del datore di lavoro*, in *Arg. dir. lav.*, 2007, II.

SCORCELLI R., *Ancora in tema di controlli a distanza ai sensi dell'art. 4 SL sui limiti di liceità dei cd controlli difensivi*, in *DL Rivista di diritto del lavoro privato e pubblico*, 2007 fasc. 4, pp. 1205 ss.

SERRANI L., *Moderne soluzioni di registrazione audio-visiva: ambito di applicazione e limiti dell'art. 4 dello statuto dei lavoratori*, in *Dir. rel. ind*., 2010, 529.

SIMITIS S., *Reconsidering the premises of Labour Law: Prolegomena to an EU Regulation on the Protection of Employees' Personal Data*, in *European Law Journal*, 1999.

SITZIA A., *Controllo sulle sim aziendali: necessaria la policy interna*, in *Diritto&Pratica del Lavoro*, 8/2018.

SITZIA A., PEZZONIA D., *Il controllo del datore di lavoro su internet e posta elettronica: quale riservatezza sul luogo di lavoro?*, in *Nuova Giur. Civ.,* 2016, 6.

SITZIA A., *I limiti del controllo della posta elettronica del lavoratore: una chiara presa di posizione della Grande Camera della Corte eur. dir. uomo*, nota alla sentenza della CORTE EUR. DIR. UOMO, Grande Camera, 5.9.2017, ric. 61496/08, in *Nuova Giur. civ. commentata,* n. 12/2017.

SITZIA A., *Il controllo (del datore di lavoro) sull'attività dei lavoratori: il nuovo art. 4 st. lav. e il consenso del lavoratore*, in *Labour&Law Issues,* vol. 2 n. 1, 2016.

SITZIA A., *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Padova CEDAM, 2013, pag. 10.

SITZIA A., *Personal computer e controlli "tecnologici" del datore di lavoro nella giurisprudenza*, in *Arg. Dir. Lav*. 2017, 3, 804 ss.

SITZIA A., *Videosorveglianza occulta, privacy e diritto di proprietà: la Corte Edu torna sul criterio di bilanciamento*, in *Arg. Dir. Lav*., 2018, 2.

SPINELLI G., *La legittimità dei controlli datoriali c.d. "difensivi": certezze apparenti in una categoria dubbia*, in *Riv. It. Dir. lav*., 2013, n. 1.

STANCHI A., *Apparecchiature di controllo, strumenti di comunicazione elettronica e controlli difensivi del datore di lavoro*, in *Lav. giur*., 2008, vol.
Fasc. 4, pp. 351 ss.

STANCHI A., *Privacy, Le Linee Guida del Garante per Internet e posta elettronica*, in Guida Lav., n. 12/2007.

TACCONI C., *La disciplina della privacy e la tutela del lavoratore*, in CUFFARO V. D'ORAZIO R. RICCIUTO V. (a cura di), *Il codice di trattamento dei dati personali*, Torino, Giappichelli, 2007.

TAMPIERI A., *I controlli a distanza mediante impianti audiovisivi*, in R. PESSI (a cura di), Codice commentato del lavoro, Torino, 2011.

TEBANO L., *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?,* in *Rivista Italiana di Diritto del Lavoro*, fasc. 3, 2016, pag. 345.

TEBANO L., *Le visite di controllo "in uscita" nel diritto vivente*, in *Diritto Lavori e Mercati*, 2010, 3.

TOFFOLETTO F., *Le nuove tecnologie informatiche e tutela del lavoratore,* Milano, Giuffré, 2006.

TROJSI A., *Al cuore del nuovo art. 4, co. 2. St. Lav.: la delimitazione della fattispecie degli "strumenti utilizzati per rendere la prestazione lavorativa*, in *Rivista Italiana di diritto del lavoro,* fasc. 2, 2017.

TROJSI A., *Il diritto del lavoratore alla protezione dei dati personali*, Giappichelli, Torino, 2013.

TULLINI P., *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, RIDL 2009, I, 323 ss.

TULLINI P., *Tecnologie informatiche in azienda: dalle Linee-guida del Garante alle applicazioni concrete*, in TULLINI P. (a cura di), *Tecnologie della comunicazione e riservatezza nel rapporto di lavoro*, Padova, CEDAM, 2010.

VALLAURI M.L., *E' davvero incontenibile la forza espansiva dell'art. 4 dello Statuto dei lavoratori?*, in *Orient. giur. lav*., 2008.

VALLEBONA A., *Il controllo delle comunicazioni telefoniche del lavoratore*, in *Il diritto del lavoro*, 2001, vol. 75, fasc. 4, pp. 357-362

VALLEBONA A., *Istituzioni di diritto del lavoro. Il rapporto di lavoro*, Padova, Cedam, 2012.

VALLEBONA A., *Nota a Cass. 27 maggio 2015, n. 10955*, in *Massimario di Giurisprudenza del Lavoro,* 2016, 286.

VALLEBONA A., *Note e dibattiti di attualità, il controllo delle comunicazioni telefoniche del lavoratore*, in *DL*, 2001.

VENEZIANI B., *Sub art. 4, in Lo Statuto dei lavoratori*, Commentario diretto da G. Giugni, Milano, 1979.

WARREN S. e BRANDEIS L., *The Right to privacy*, Harvard Law Review, 1890.

ZICCARDI G., *Il controllo delle attività informatiche e telematiche del lavoratore: alcune considerazioni informatico-giuridiche*, in *Labour Law Issues*, 2016,2.

ZOLI C., *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, in *Riv. it. dir. lav.*, 2009, 4, pp.485 ss.