UNIVERSITA' DEGLI STUDI DI PADOVA

DIPARTIMENTO DI SCIENZE ECONOMICHE ED AZIENDALI

"M. FANNO"

DIPARTIMENTO DI AFFERENZA RELATORE: DIPARTIMENTO DI DIRITTO PRIVATO E CRITICA DEL DIRITTO

CORSO DI LAUREA IN ECONOMIA

PROVA FINALE

"GDPR PRIVACY E CONTROLLI A DISTANZA: NUOVI ADEMPIMENTI PER I DATORI DI LAVORO"

RELATORE:

CH.MA PROF.SSA BARBARA DE MOZZI

LAUREANDA: GLORIA CAPPELLARI

MATRICOLA N. 1113007

ANNO ACCADEMICO 2017-2018

INDICE

INTRODUZIONE – LA NUOVA PRIVACY, OPPORTUNITA' E SFIDE

L'entrata in vigore del nuovo Regolamento europeo sulla privacy, propriamente "General Data Protection Regulation" (da cui deriva l'acronimo GDPR), si è abbattuta sull'ordinamento italiano, direbbero alcuni, come un fulmine a ciel sereno. Sebbene pubblicato sulla Gazzetta Ufficiale dell'Unione Europea il 4 maggio 2016, l'argomento ha riempito le principali testate giornalistiche solamente a partire da gennaio 2018.

Il tema della tutela della riservatezza dei lavoratori e, più in generale, della privacy ha trovato nel corso del tempo i suoi riferimenti normativi in diverse fonti europee, tra le quali la Direttiva n. 95/46/CE relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali (abrogata dallo stesso Regolamento), nonché la Direttiva n. 97/66/CE sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni o piuttosto nella Direttiva n. 2000/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (Barraco, 2016). A queste fonti si affiancano l'art. 12 della Dichiarazione Universale dei diritti umani[1], l'art. 8 della CEDU[2] e la Carta dei diritti fondamentali di Nizza, che prende ispirazione dallo stesso art. 8 CEDU per dare una definizione positiva del diritto alla protezione dei dati di carattere personale (Rotondi, 2018), inteso come diritto di ogni individuo a che i suoi dati siano trattati secondo una serie di principi per altro ripresi dallo stesso Regolamento. A livello statale, il D.lgs. 196/2003 (c.d. Codice Privacy) costituiva la fonte principale di attuazione delle direttive sopra indicate.

Lo scopo del Legislatore europeo era quello di conciliare le esigenze di realizzazione del mercato interno tutelando la privacy delle persone fisiche, lasciando un certo spazio di manovra agli Stati membri. Con il Regolamento UE 2016/679 sulla protezione dei dati personali si è vista un'inversione di tendenza dello stesso legislatore che ha voluto ridefinire la materia a livello centrale (si noti infatti l'utilizzo del regolamento, e non di una direttiva, con conseguenti differenze in tema di efficacia e diretta applicabilità); la scelta fatta trova la propria *ratio* nell'evitare di sostenere le disuguaglianze all'interno dell'UE, che potrebbero

[1] *"Nessun individuo potrà essere sottoposto ad interferenze arbitrarie nella sua vita privata, nella sua famiglia, nella sua casa, nella sua corrispondenza, né a lesione del suo onore e della sua reputazione". "Ogni individuo ha diritto ad essere tutelato dalla legge contro tali interferenze o lesioni".*

[2] *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 un'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.*

costituire un ostacolo all'esercizio delle attività economiche facendo venire meno le leggi della concorrenza.

L'entrata in vigore del Regolamento, dal 25 maggio 2018, ha portato alla disapplicazione delle disposizioni del Codice Privacy incompatibili con lo stesso, come avviene nei casi di antinomia tra leggi *self-executing* europee e leggi ordinarie italiane. Si rimanda al futuro per conoscere la sorte del D.lgs. 196/2003, in quanto il Parlamento, con la Legge 25 ottobre 2017, n. 163, ha incaricato il Governo di abrogare espressamente le disposizioni del D. lgs. 196/2003 incompatibili con il GDPR, di coordinare la normativa italiana in ambito di protezione dei dati personali con quanto previsto dal GDPR, di adottare, ove necessario, provvedimenti specifici, nel rispetto degli interventi del Garante in materia e di adeguare l'apparato sanzionatorio previsto dalla normativa italiana al GDPR (al momento attuale il decreto attuativo è ancora in fase di elaborazione).

In questo contesto, quali sono i riflessi sulla normativa italiana in materia di diritto del lavoro e in particolare sui controlli a distanza dei lavoratori? Il passaggio dalla tecnica all'informatica ha portato, negli ultimi anni, dei cambiamenti significativi in ambito lavorativo (si pensi all'uso di cercapersone, ai videoterminali equipaggiati di codici di accesso, alla geolocalizzazione tramite GPS, ai sistemi di registrazione delle presenze, ai braccialetti elettronici che registrano l'ansia e il battito cardiaco, ai dati biometrici utilizzati come chiave di accesso... Gli esempi sono sterminati). "Si è assai lontani dal contesto di fondo in cui si è inserito lo Statuto dei Lavoratori e la sua lungimirante disciplina sul controllo a distanza"[3] (Buttarelli, 2018), legge posta a tutela della parte debole della prestazione lavorativa, ovvero il lavoratore. E' intuitivo come i "nuovi mezzi" comportino un monitoraggio capillare della prestazione a discapito della dignità umana del lavoratore. Si tenga presente che i dati raccolti che si riferiscono al lavoratore sono potenzialmente classificabili come "dato personale" nel Regolamento e questi possono essere utilizzati, anche ai fini disciplinari, dal datore di lavoro, nel rispetto della legge 300/1970 e in particolare l'art. 4; ogni qualunque valutazione sull'art. 4 non potrà però prescindere dal rispetto delle norme

[3] BUTTARELLI, G.. 2018. *La rivoluzione copernicana del 25 maggio 2018 in materia di privacy La imminente applicazione del Regolamento europeo (GDPR) sulla protezione dei dati personali* [online]. Lavoro, Diritti, Europa - Rivista nuova del diritto del lavoro, estratto 1, pag. 5.
Disponibile su: <https://www.lavorodirittieuropa.it/images/articoli/pdf/ARTICOLO_BUTTARELLI.pdf> [data di accesso: 30/06/2018].

sulla privacy introdotte dal 25 maggio 2018 nell'ordinamento italiano, pena l'invalidità delle prove utilizzate a sostegno del potere disciplinare del datore di lavoro[4].

Proprio per la complessità della materia, il Legislatore europeo si è riservato di introdurre nel Regolamento l'art. 88 che riconosce la facoltà agli Stati membri di mantenere, modificare o introdurre *ex novo* specifiche regole (ad esempio, tramite accordi collettivi), giustificate dalla diversità culturale e della storia giuridica dei Paesi membri, in materia di diritto del lavoro.

[4] Si pensi, per esempio, al caso in cui il datore di lavoro intimi un licenziamento disciplinare ad un impiegato perché sorpreso a svolgere attività ludiche sul computer durante l'orario di lavoro, senza però aver precedentemente consegnato l'informativa – armonizzata al GDPR - allo stesso impiegato, come prevede l'art.4 comma 3 in riferimento agli "strumenti di lavoro"; in caso di contenzioso il giudice potrebbe invalidare il licenziamento intimando il reintegro del lavoratore.

CAPITOLO I – LA LEGISLAZIONE ITALIANA E L'ART.4 STATUTO LAVORATORI

1.1 Il "vecchio" art.4 L.300/1970

L'art.4 dello Statuto dei Lavoratori precedente la riforma del Jobs Act prevedeva il divieto assoluto dell'uso di impianti audiovisivi e altre apparecchiature per finalità di controllo a distanza[5] (Huge, 2017) del lavoratore. L'istallazione era permessa solo per "esigenze organizzative e produttive" e per "ragioni di sicurezza" previo accordo con le rappresentanze sindacali aziendali (RSA[6] o RSU[7]) oppure, in mancanza di queste, con la commissione interna. Nei casi in cui l'accordo non fosse stato possibile, l'art.4 prevedeva la possibilità per il datore di lavoro di fare istanza all'Ispettorato del Lavoro.

Emergeva il caso del c.d. "controllo preterintenzionale", ovvero il lavoratore che viene indirettamente ripreso dalle telecamere istallate secondo le disposizioni di quando detto sopra; il legislatore affermava l'impossibilità dell'utilizzo di questo tipo di riprese ai fini disciplinari. Per ovviare alla problematica, in un'ottica di bilanciamento degli interessi tra il lavoratore e la tutela della riservatezza e della dignità e il datore di lavoro e il suo potere di controllo e difesa dell'organizzazione produttiva, la giurisprudenza si era di fatto inventata i c.d. "controlli difensivi" ovvero:

- in un primo momento, erano genericamente intesi come verifiche volte ad accertare esclusivamente comportamenti illeciti, estranei al rapporto di lavoro, posti in essere dai dipendenti[8] ;
- "successivamente, l'interpretazione richiese non solo che la situazione rientrasse nel primo punto ma anche che il comportamento illecito non fosse in linea con la corretta esecuzione dell'obbligazione contrattuale del lavoratore[9] e che questo comportasse la violazione dei beni e degli interessi aziendali"[10] (Huge, 2017).

[5] HUGE, S., 2017. *L'art. 4 Statuto dei Lavoratori dopo la riforma di cui D.lgs. 151/2015: vecchie e nuove prospettive*. [online]. Disponibile su: <www.giuslavoristi.it/wp-content/uploads/2017/02/Sara-Huge-Art.-4-S.L.-07.03.2017.pdf> [data di accesso: 07/07/2018].

[6] Rappresentante sindacale dei lavoratori all'interno dell'azienda.

[7] Rappresentanza sindacale unitaria all'interno dell'azienda; è costituita dall'unione delle varie sigle sindacali presenti.

[8] Si veda a riguardo Cass. sez. lav., 3 aprile 2002, n.4746.

[9] Si veda a riguardo Cass. sez. lav., 23 febbraio 2012, n.2722.

[10] HUGE, S., 2017. *L'art. 4 Statuto dei Lavoratori dopo la riforma di cui D.lgs. 151/2015: vecchie e nuove prospettive*. [online]. Disponibile su: <www.giuslavoristi.it/wp-content/uploads/2017/02/Sara-Huge-Art.-4-S.L.-07.03.2017.pdf> [data di accesso: 07/07/2018].

In ogni caso si trattava di legittimazione di un controllo *ex post* sul dipendente, completamente estraneo alla disciplina dell'art.4.

1.2 Il "nuovo" art.4 L.300/1970

Con la legge delega n. 183/2014 il Legislatore ha incaricato il Governo di armonizzare la disciplina dei controlli a distanza all'evoluzione tecnologica tenendo presente le esigenze di entrambe le parti del rapporto di lavoro.

Il D.lgs. 151/2015 (il c.d. "Jobs Act"), all'art.23, ha introdotto così una disciplina nuova, divisa in 3 commi. Il primo comma afferma : gli impianti audiovisivi e gli altri strumenti dai quali derivi anche la possibilità di controllo a distanza, possono essere impiegati "solo per esigenze organizzative e produttive, per la sicurezza e per la tutela del patrimonio aziendale". La liceità dell'istallazione poggia sull'accordo collettivo siglato precedentemente con le rappresentanze sindacali, ovvero nel caso in cui l'azienda sia ubicata in diverse province o regioni l'accordo può essere siglato con le rappresentanze sindacali comparativamente più rappresentative a livello nazionale. In mancanza di accordo è prevista la possibilità di richiedere l'autorizzazione alla sede territoriale o centrale dell'Ispettorato Nazionale del Lavoro rispettivamente nel caso di unica sede o più sedi. Da sottolineare che, nel caso in cui dai controlli emerga un comportamento illecito che lede i beni estranei al rapporto di lavoro, le informazioni raccolte sono utilizzabili in giudizio anche in completa assenza dei requisiti normativi .

Il secondo comma afferma invece che l'accordo sindacale o l'autorizzazione non sono necessari nel caso in cui la possibilità di controllo derivi dagli strumenti di lavoro utilizzati dal lavoratore per svolgere la prestazione lavorativa ovvero dagli strumenti di registrazione delle presenze.

L'ultimo comma sostiene la possibilità di utilizzare le informazioni raccolte nel rispetto dei commi 1 e 2 del suddetto articolo "a tutti i fini connessi al rapporto di lavoro" (quindi anche ai fini disciplinari), a condizione che il lavoratore abbia ricevuto un'informativa dettagliata che indichi le modalità di utilizzo degli strumenti di lavoro e le possibilità di controllo che ne derivano e nel rispetto del D.lgs. 196/2003 (Codice Privacy).

Si nota chiaramente l'entità delle modifiche riportate nell'articolo in oggetto, modifiche che peraltro hanno causato la nascita di correnti interpretative diverse e di dibattiti dottrinali tra gli studiosi del diritto del lavoro. Seguendo l'ordine dei commi, la prima cosa che si nota è il venir meno del divieto assoluto del controllo a distanza intenzionale del "vecchio" art.4,

sostituito dalla locuzione “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”. Vi è un cambio di prospettiva in quanto la prima versione indicava il divieto assoluto e i commi successivi specificavano le eccezioni, mentre la seconda versione inverte la struttura precedente, anche se vi è la sensazione che l’avverbio “esclusivamente” evochi comunque il principio di assolutezza (Da Valle, 2016). Ulteriore novità del primo comma è l’aggiunta, tra le esigenze che giustificano l’istallazione degli impianti, della “tutela del patrimonio aziendale”; l’intenzione del Legislatore, secondo un’opinione condivisa, è quella di tipicizzare la categoria interpretativa dei “controlli difensivi”, soggiogandola all’accordo sindacale o, in mancanza, all’autorizzazione dell’Ispettorato Nazionale del Lavoro. Si noti l’aumento del carico burocratico sostenuto dal datore di lavoro (relativo agli accordi sindacali o alle autorizzazioni) a seguito dell’introduzione di questa nuova categoria di esigenze.

Numerose polemiche sono sorte a causa del secondo comma novellato, in particolare in riferimento all’interpretazione delle parole “strumenti di lavoro”. Si tenga ben presente che, in questo caso, l’accordo sindacale o l’autorizzazione non sono previsti. La problematica evidenziata dagli studiosi è l’identificazione di che cosa è (o non è) strumento di lavoro: quali sono le caratteristiche che lo strumento deve avere per essere ritenuto tale? Ci sono dei requisiti da soddisfare? La disposizione purtroppo non si esprime in merito, lasciando così la problematica a chi si trova ad applicarla. L’unica indicazione data è che lo strumento deve essere utilizzato dal lavoratore “per rendere la prestazione lavorativa”: viene in questo modo inteso come un attrezzo, affidato al lavoratore per svolgere strettamente le mansioni assegnate. Secondo alcuni, (Da Valle, 2016) la chiave di lettura utile alla distinzione tra strumento di lavoro (che ricade nel comma 2) o altro strumento dal quale derivi possibilità di controllo (che ricade invece nel comma 1) è chiedersi se suddetto strumento è più utile al lavoratore oppure al datore di lavoro. Il Ministero del Lavoro si è espresso in merito, a seguito delle numerose polemiche, tramite Comunicato Stampa del 18 giugno 2015; anche se la nota non ha valenza di interpretazione autentica, rappresenta un barlume di luce nel caos creato dal nuovo comma. In particolare, il comunicato conferma l’analogia tra il termine “strumento di lavoro” e “attrezzo” ed esclude la possibilità, soprattutto per gli strumenti tecnologici (quali, per esempio, tablet, pc, smartphone...) di far rientrare nel comma 2 quegli applicativi e/o software istallati dai quali derivi la possibilità di controllo sul lavoratore. A titolo esemplificativo: il pc è necessario all’impiegato di un ufficio per svolgere la prestazione

lavorativa , ovvero il pc è "strumento di lavoro", ricade nel comma 2 e non è necessario l'accordo sindacale o l'autorizzazione. Al contrario, un software di monitoraggio dell'accesso ai siti internet non è strettamente legato alla prestazione lavorativa del dipendente, piuttosto è uno strumento dal quale è possibile controllare a distanza il lavoratore, ricade quindi nel comma 1 ed vi è esigenza di accordo sindacale o di autorizzazione.

Per quanto riguarda gli strumenti di registrazione delle presenze, il legislatore ha voluto definitivamente porre fine ai contenziosi tra datore di lavoro e dipendente licenziato a causa di informazioni raccolte tramite i c.d. *badge*, per esempio riguardo ai ritardi. Il comma stabilisce che non è necessario l'accordo sindacale o l'autorizzazione. L'obbiettivo perseguito è quello di bilanciamento degli interessi tra i contraenti: il dipendente in ritardo è inadempiente e può essere quindi perseguito da azioni disciplinari.

Anche il comma di chiusura ha suscitato dibattiti interpretativi: come si è già detto, le informazioni raccolte sono subordinate all'informazione delle funzionalità degli strumenti di lavoro e alla disciplina del Codice Privacy che, se non rispettata, comporta l'inutilizzabilità dei dati ai fini dell'esercizio del potere disciplinare, nonché violazioni delle norme del Codice Privacy e eventuali responsabilità penali. "La condizione dell'adeguata informazione sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli rende indispensabile per il datore di lavoro la predisposizione di adeguate policy interne" (Da Valle, 2016): il suggerimento è quello di stilare un elenco di tutti gli strumenti e di identificarli, tramite un'analisi approfondita, tra gli strumenti di lavoro oppure tra gli impianti audiovisivi o altri strumenti; successivamente predisporre delle *policy* che indichino, per esempio, le corrette modalità di utilizzo dello strumento di lavoro, quali sono gli utilizzi vietati o limitati, le conseguenze dell'utilizzo improprio, le sanzioni disciplinari ecc...

Altra problematica evidenziata nel terzo comma è la difettosità dell'apparato sanzionatorio che dovrebbe seguire la violazione della norma. L'interprete ha a disposizione l'art 171[11] del Codice Privacy che rimanda all'art.38[12] dello Statuto dei Lavoratori, per le violazioni dei commi 1 e 2 dell'art.4 ma non ha nessuna sanzione indicata per la violazione del terzo comma, se non l'inutilizzabilità dei dati raccolti. Sembrerebbe quindi che, per le violazioni

[11] *"La violazione delle disposizioni di cui all'articolo 113 e all'articolo 4, primo e secondo comma, della legge 20 maggio 1970, n. 300, è punita con le sanzioni di cui all'articolo 38 della legge n. 300 del 1970."*

[12] *"Le violazioni degli articoli 2, 5, 6, e 15, primo comma, lettera a), sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da lire 100.000 a lire un milione o con l'arresto da 15 giorni ad un anno.*
Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente.
Quando, per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo.
Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del codice penale."

dei commi uno e due, vengano irrorate le sanzioni penali previste, ma che non vi sia la conseguenza dell'inutilizzabilità dei dati. Al contrario, la violazione del comma 3 non è collegata ad alcuna sanzione penale ma i dati divengono non utilizzabili se non sorretti dall'informativa e dall'adeguatezza alla disciplina Privacy.

Fino all'avvento del *General Data Protection Regulation* UE 2016/679 la disciplina lavoristica dei controlli a distanza e la tutela dei dati personali non ha visto un'eccessiva reciproca contaminazione. I due rami si muovevano su piani paralleli e i punti di contatto erano ben definiti. La modifica dell'art.4, apposta dal Jobs Act, ha compromesso il rapporto tra il suddetto articolo e il Codice Privacy ed anche la tecnica legislativa, che, secondo alcuni, ha dimostrato una notevole degradazione (Vicarelli, 2016).

Ad esempio dello stringente legame instaurato invece tra le fonti europee e la disciplina del controllo a distanza degli Stati membri, si porta la recente sentenza della CEDU del 9 gennaio 2018 (Ribalta e altri c. Spagna). Alcuni lavoratori addetti ad un supermercato spagnolo erano stati ripresi, tramite telecamere nascoste orientate sui registratori di cassa del supermercato, a sottrarre merce esposta in vendita. "Con la predetta decisione la CEDU ha ritenuto che l'installazione occulta e l'utilizzo di telecamere avesse violato il diritto alla privacy dei lavoratori previsto dall'art. 8 della CEDU in quanto eccedente i principi di trasparenza (necessaria informazione preventiva [...]), gradualità (necessità di fondati sospetti di illeciti anche in relazione agli autori che nella fattispecie non erano stati preventivamente identificati nemmeno in via indiziaria) e proporzionalità (in quanto le riprese erano durate settimane, avevano riguardato tutti i cassieri indistintamente e senza limiti di orario divenendo quindi di carattere esplorativo)" (Pedroni, 2018).

L'assetto si è ulteriormente modificato a partire dal 25 maggio 2018: l'utilizzabilità dei dati è subordinata all'adeguamento del datore di lavoro a una serie di disposizioni indicate nel GDPR (nel gergo comune questo adeguamento viene definito "*gdpr compliance*") che ha di fatto soppiantato le disposizioni del Codice Privacy incompatibili con lo stesso e ha introdotto nuovi adempimenti per i datori di lavoro e in generale per qualunque soggetto che si trovi a trattare dei dati.

CAPITOLO II – IL REGOLAMENTO, DISPOSIZIONI ED OBBLIGHI

Quali sono gli obbiettivi che il Legislatore europeo ha voluto perseguire nell'elaborazione del Regolamento UE 2016/679? Tra le motivazioni si possono trovare la creazione di un quadro di maggiore certezza del diritto e di maggiore uniformità della disciplina privacy nei vari Paesi europei, l'individuazione di una base giuridica a fondamento del trattamento, il miglioramento della tutela dei dati degli interessati, ma soprattutto la responsabilizzazione del titolare del trattamento.

2.1 Alcune definizioni

L'art.4 del Regolamento raccoglie una serie di definizioni che aiutano il lettore a cogliere più facilmente le altre disposizioni. Innanzitutto, viene data una definizione di "dato personale", ovvero qualsiasi informazione riguardante una persona fisica identificata o identificabile[13]. Si capisce che il Legislatore, con "qualsiasi informazione", richiama dati oggettivi ma anche soggettivi, come opinioni e valutazioni[14] (De Nicola, Pizzetti, Rotunno, 2018). Con riferimento al concetto di identificabilità si considera identificabile una persona che può direttamente o indirettamente essere individuata a seguito di un particolare riferimento (nome, numero identificazione, dati relativi all'ubicazione, IP del computer, cookies[15]…). I Considerando 26 e 27 del Regolamento escludono dall'oggetto del trattamento i dati di persone decedute o dati anonimi.

Cambia invece la definizione di quelli che sotto il vigore della direttiva 95/46/CE erano noti come "dati sensibili". Essi sono ora indicati come "categorie particolari di dati personali" *ex* art. 9 GDPR; in particolare rientrano in questa categoria i dati relativi all'origine razziale o etnica, le opinioni politiche e le convinzioni religiose o filosofiche, l'appartenenza sindacale, i dati relativi alla salute, i dati genetici, i dati biometrici, i dati relativi alla vita sessuale o all'orientamento sessuale di una persona. Il Regolamento dispone il divieto di trattamento di questa categoria di dati ma prevede alcune deroghe al paragrafo 2 del suddetto articolo, tra le quali il caso di prestazione del consenso esplicito per una o più finalità specifiche dell'interessato, il caso del trattamento necessario per assolvere obblighi o esercitare diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro o della

[13] La persona fisica alla quale i dati appartengono viene definita "interessato".
[14] Anche la direttiva 95/46/CE, abrogata dal GDPR, e il parere del Working Party 29 n. 4/2017, sostengono questa tesi.
DE NICOLA A., PIZZETTI F., ROTUNNO, I., a cura di., 2018. L'ESPERTO RISPONDE - *Privacy. Le nuove regole tra opportunità e sfide*. Il SOLE24 ORE, #135 (21 maggio), pag. 3.
[15] A proposito si veda il Considerando n. 30 del Regolamento UE 2016/679.

sicurezza sociale e protezione sociale e il caso di trattamento per finalità di valutazione medica oggettiva del dipendente.

All'art.10 viene indicato il trattamento di "dati giudiziari" ovvero relativi a condanne penali e reati: il trattamento deve avvenire sotto il controllo dell'autorità pubblica o previa autorizzazione dal diritto dell'UE o degli Stati membri.[16]

Il Regolamento introduce molte definizioni assenti nel Codice Privacy. In particolare, si richiama la definizione di "archivio", parzialmente coincidente con "banca dati" (lett. p dell'art. 4 del D.lgs. n. 196/2003): nel Regolamento si parla di "insieme strutturato", mentre nel Codice italiano si parla di "complesso organizzato". La questione è di notevole importanza, in quanto il Regolamento all'art. 2, indica che oltre a tutti i trattamenti automatizzati, la disciplina si applica anche ai trattamenti non automatizzati, ma solo se quest'ultimi riguardano dati contenuti in un archivio o destinati a figurarvi. Il Regolamento esplicita, poi, le definizioni di profilazione, limitazione del trattamento e pseudonimizzazione: la prima viene definita come trattamento automatizzato di dati che produce valutazioni su determinati aspetti personali dell'interessato; con la seconda si intende il contrassegno dei dati personali conservati con l'obbiettivo di limitarne il trattamento futuro mentre la terza definizione indica il meccanismo di conservazione dei dati che non possono essere attribuiti a un interessato specifico senza utilizzo di altre informazioni che sono conservate separatamente[17].

Che cosa si intende per trattamento dei dati e quali sono i soggetti che intervengono nelle operazioni? All'art.4 paragrafo 2 si trova una definizione puntuale di trattamento: "*Qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali o insiemi di dati personali, come la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modifica, l'estrazione, la consultazione, l'uso, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione".*

La persona fisica o giuridica che determina le finalità e i mezzi del trattamento viene definita all'art.4 paragrafo 7 come "titolare del trattamento"; si noti la presenza di un'altra categoria di

[16] In Italia, per esempio, il datore di lavoro deve necessariamente richiedere il c.d. "certificato del casellario giudiziario" relativo a condanne penali che coinvolgono minori nel caso in cui l'attività del lavoratore preveda un contatto diretto e regolare con gli stessi.

[17] Si pensi, per esempio, a un consulente del lavoro che ha raccolto i dati relativi alle detrazioni dei dipendenti da applicare in busta paga in una cartella contrassegnata non dal "nome e cognome" del dipendente ma da un codice identificativo; in separata sede, viene tenuto un elenco con il "nome e cognome" del dipendente abbinato al codice di riferimento.

soggetti, definiti "responsabili del trattamento" (indicata dall'art.28) ovvero gli incaricati al trattamento dei dati per conto del titolare del trattamento. Il punto strategico che permette di individuare con chiarezza la distinzione tra la prima categoria e la seconda risiede nell'individuazione del soggetto che determina le finalità e i mezzi del trattamento[18]. Da notare assolutamente le raccomandazioni del GDPR in ambito di nomina del responsabile del trattamento: è necessaria, prima di tutto, l'elaborazione dell'atto di nomina sottoscritto da entrambi i soggetti ma, soprattutto, la caratteristica di "*gdpr compliant*" del responsabile del trattamento, ovvero l'adeguamento alla regolamentazione che verrà indicata nei prossimi paragrafi. L'autorizzazione deve indicare, tra le altre cose, le misure di sicurezza adottate dal responsabile[19]. Le misure "minime" di sicurezza che ogni soggetto "trattante" deve obbligatoriamente adottare sono indicate all'art 32 del Regolamento, ai paragrafi da a) a d):

- pseudonimizzazione e cifratura dei dati personali;
- capacità di assicurare la riservatezza, integrità, disponibilità, resilienza dei sistemi e dei servizi di trattamento;
- capacità di ripristinare tempestivamente la disponibilità di accesso dei dati personali in caso di incidenti fisico o tecnico;
- predisposizione di una procedura per testare e valutare l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

I titolari dello stesso trattamento possono essere molteplici (se definiscono congiuntamente finalità e mezzi): la situazione è regolamentata dall'art.26 del Regolamento che tratta la categoria dei "contitolari del trattamento". Le disposizioni che valgono sono le stesse del titolare del trattamento ma è prevista la stipulazione di un accordo interno tra le parti che indichi le rispettive posizioni, funzioni e responsabilità nell'adempimento degli obblighi derivanti dalla disciplina.

Nel Regolamento manca una definizione puntuale di "incaricato" (presente invece nel Codice italiano), ma ad esso ci si riferisce, all'interno della definizione di "terzo", come "persona autorizzata al trattamento dei dati sotto l'autorità diretta del titolare o del responsabile". Non vi è obbligo di nomina[20] ma vi è obbligo di formazione e di mantenimento della riservatezza.

[18] Tipico esempio è il consulente incaricato dal datore di lavoro – titolare del trattamento – di trattare i dati dei dipendenti per l'elaborazione dei cedolini paga piuttosto che per altri adempimenti.

[19] Sul sito del CNIL francese è disponibile un fac-simile con "clausole esempio" da inserire nell'atto di nomina del responsabile del trattamento; al momento il Garante della Privacy italiano non ha ancora elaborato nessun documento. Disponibile al sito: https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses.

[20] Nella bozza di decreto attuativo (promosso dalla Legge di delegazione europea 2016/2017 del 25 ottobre 2017, n. 163), all'art 2-ter dieces, è prevista la possibilità da parte del titolare e del responsabile del trattamento di individuare e autorizzare puntualmente gli incaricati. Bozza disponibile al sito: https://www.cyberlaws.it/2018/bozza-aggiornata-10-mag-del-nuovo-codice-privacy-2018-schema-del-decreto-legislativo/.

Al momento il Garante non si è ancora espresso riguardo alle modalità di formazione del personale.

2.2 Le disposizioni generali e i principi fondamentali

Il Regolamento si apre con alcune norme generali, suddivise in due capi: le disposizioni generali propriamente dette e i principi. Le disposizioni generali (articoli da 1 a 4) sono dedicate a individuare l'oggetto, le finalità, le definizioni (già sviluppate nel paragrafo precedente) e l'ambito di applicazione territoriale.

Con riferimento a quest'ultimo, l'art. 3 dispone i confini dell'efficacia della disciplina: i criteri che si devono rispettare riguardano la residenza del soggetto che tratta i dati ed alcuni casi particolari. Il primo criterio impartisce l'applicazione ai trattamenti effettuati da soggetti stabiliti nell'Unione Europea (indipendentemente dal fatto che il trattamento sia effettuato o meno nell'Unione); il secondo criterio invece prevede l'imposizione ai soggetti che, sebbene non siano situati nell'Unione Europea, trattano dati personali secondo i casi tassativamente previsti dall'articolo, i quali sono l'offerta di beni o la prestazione di servizi agli interessati stabiliti nell'UE e il monitoraggio degli interessati all'interno dell'UE.

Nel Capo II del Regolamento vengono indicati i principi da rispettare, primo passo verso lo status di "*gdpr compliant*". Tra i più importarti si trovano il principio di liceità, di correttezza e di trasparenza; non di meno è il principio dell'accountability, assoluta novità del Regolamento, e quello di minimizzazione dei dati.

Il trattamento è lecito solo se avviene nel rispetto della legge. La trattabilità dei dati dipende dal verificarsi di una delle situazioni indicate nell'articolo 6 del Regolamento. E' possibile dividere il trattamento in due macro-categorie: il caso in cui l'interessato ha prestato il consenso (richiesto peraltro in tutti i trattamenti dei dati *ex* art. 9, con finalità specifiche) e il caso in cui l'interessato non ha prestato il consenso ma il trattamento è necessario:

- all'esecuzione di un contratto di cui l'interessato è parte,
- ad adempiere un obbligo legale,
- per il perseguimento del legittimo interesse del titolare del trattamento o di terzi, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali dell'interessato e la loro protezione,
- ..altro[21].

[21] Per le altre casistiche si veda art.6 Regolamento UE 2016/679, paragrafi da a) a f).

Nel primo caso, grava sul titolare del trattamento l'onere della prova: è suo compito elaborare una dichiarazione scritta chiara e facilmente comprensibile per l'interessato, che deve essere sottoscritta in piena libertà. E sicuramente escludibile da questa categoria il rapporto di lavoro, in quanto lo status di soggetto debole del dipendente non risulterebbe allineato con l'ultimo requisito.

Nel secondo caso, i tre punti sopra elencati rilevano maggiormente, ciascuno secondo una sfumatura diversa del rapporto di lavoro: sicuramente l'esecuzione del contratto di lavoro rende necessario il trattamento dei dati dell'interessato-dipendente, ma anche il versamento delle ritenute fiscali a carico del datore di lavoro in virtù del ruolo di sostituto d'imposta potrebbe far ricadere in questa categoria il trattamento dei dati, in quanto obbligo legale. Maggiore attenzione è data soprattutto alla definizione di "interesse legittimo", peraltro sottolineata dal Considerando 47 del Regolamento e analizzata a fondo, con la previsione di casi ricorrenti, dal Working Party (Gruppo di lavoro) ex art. 29[22] nell'elaborato n.249/2017. L'interesse legittimo principale del datore di lavoro concerne il perseguimento degli obbiettivi imprenditoriali e la tutela del patrimonio aziendale ma questo non deve prevalere sui diritti e sulle libertà del dipendente (si noti come questo sia conforme anche alla disciplina dello Statuto dei Lavoratori). E' compito del datore di lavoro valutare preventivamente se il trattamento dei dati è proporzionato e giustificato al perseguimento dell'interesse legittimo (c.d. *balancing test*). L'obbligo di "responsabilizzazione" e di valutazione che grava sul datore di lavoro, e in generale su ogni titolare del trattamento, è generale e non è quindi esclusivamente collegato al contesto dell'interesse legittimo: si tratta del cosiddetto principio dell'*accountability*. Novità dirompente del Regolamento, comporta la piena responsabilità in capo al titolare del trattamento riguardo le modalità, le misure di sicurezza e i limiti adottati. Prima del 25 maggio 2018, vigeva l'art.17 del Codice Privacy che sosteneva che il trattamento, esclusi i dati sensibili, doveva seguire le misure e gli accorgimenti dal Garante (tra cui la verifica preliminare o la richiesta diretta del parere dell'ente); con la nuova disciplina non vi è più l'obbligo di verifica preliminare ma il titolare del trattamento deve valutare in piena autonomia la conformità e l'adeguatezza del trattamento e deve sempre essere in grado di dimostrare di non essere inadempiente.

[22] Organo consultivo indipendente istituito dalla direttiva UE 95/46 con lo scopo di fornire delucidazioni e interpretazioni alle autorità nazionali di vigilanza e protezione dei dati. E' stato sostituito dal Consiglio europeo per la protezione dei dati (EDPB) dal Regolamento UE 2016/679. Il Consiglio, rappresentato dal presidente, è composto dalla figura di vertice dell'autorità di controllo di ciascuno Stato membro e dal Garante europeo della protezione dei dati, o dai rispettivi rappresentanti. Le funzioni del Consiglio europeo per la protezioni dei dati comprendono oltre che la sorveglianza sull'osservanza del Regolamento e la consulenza, anche la pubblicazione di linee guida e codici di condotta, fuzione precedentemente attribuita al Gruppo di Lavoro art.29. Disponibile sul sito: https://protezionedatipersonali.it/gruppo-di-lavoro-art-29.

A questo principio se ne collega un altro ovvero quello della "minimizzazione del trattamento dei dati": il dato trattato deve essere indispensabile per la finalità del titolare e ogni altro dato superfluo e/o non necessario deve essere oscurato o comunque eliminato dal trattamento.

I dati devono essere esatti ed aggiornati se necessario. Devono, inoltre, essere conservati per un periodo di tempo non superiore alla realizzazione della finalità per i quali sono trattati ed è necessaria la predisposizione di un sistema di protezione che li mantenga integri e protetti.

2.3 I diritti dell'interessato

I diritti dell'interessato sono trattati nel Capo III del Regolamento; l'articolo di apertura rimarca il dovere del titolare del trattamento di adottare le misure appropriate per fornire all'interessato tutte le informazioni necessarie secondo i principi cardine su cui poggia la disciplina.

Innanzitutto l'interessato ha il diritto di conoscere le finalità del trattamento e i diritti da lui esercitabili, i dati di contatto del titolare e del responsabile del trattamento, il periodo di conservazione (o i criteri utilizzati per determinarlo), le categorie di dati trattati, l'esistenza di processi automatizzati di profilazione, eventuali destinatari terzi dei dati ed eventuali interessi legittimi del titolare del trattamento. Il titolare del trattamento ha l'obbligo di fornire queste informazioni gratuitamente e senza giustificato ritardo tramite l'informativa (il tempo massimo è di un mese dal ricevimento della richiesta, aumentato a due mesi in casi particolari; in caso di raccolta dati presso l'interessato, come nella fase di costituzione del rapporto di lavoro, questo deve essere informato contestualmente all'operazione). L'ultimo paragrafo dell'art.13 dispone che, nel caso in cui l'interessato sia già al corrente delle informazioni obbligatorie, allora non è necessario consegnare l'informativa. Da notare che le informative consegnate prima dell'entrata in vigore del GDPR non rispettano almeno due punti della nuova normativa, ovvero l'indicazione del periodo di trattamento dei dati e la possibilità dell'interessato di proporre reclamo all'autorità di controllo; se ne deduce che i titolari del trattamento dovranno provvedere necessariamente alla rielaborazione delle informative e alla consegna delle stesse.

Gli articoli da 16 a 21 trattano degli altri diritti esercitabili dell'interessato:

- il diritto di accesso, ovvero il diritto di ottenere in ogni momento dal titolare del trattamento la conferma che sia o meno in corso un trattamento dei dati e, in caso di risposta affermativa, di ricevere una serie di informazioni elencate dall'articolo 15 (finalità, destinatari, profilazione...). Questa disposizione impartisce indirettamente

l'obbligo per il titolare del trattamento di predisporre un sistema che permetta di raccogliere velocemente tutte le informazioni richieste e di elaborare una copia da consegnare all'interessato (il Considerando 63 del Regolamento suggerisce l'utilizzo di piattaforme da cui l'interessato possa accedere da remoto);

- il diritto di rettifica, ovvero la tempestiva correzione o modifica dei dati una volta che l'interessato ne abbia fatto comunicazione;
- il diritto all'oblio (altra novità del Regolamento), ovvero il diritto di ottenere la rapida cancellazione dei dati personali nei casi di revoca del consenso, trattamento illecito dei dati, completamento della finalità, e altre casistiche. Il diritto all'oblio non può essere esercitato nel caso in cui il trattamento risulti, tra gli altri casi, essere obbligatorio per l'adempimento di un obbligo legale; si capisce che il dipendente, almeno per i dati necessari al datore di lavoro per l'elaborazione dei normali adempimenti, non possa richiederne la cancellazione;
- il diritto della limitazione al trattamento, nel caso di inesattezza dei dati trattati o di trattamento illecito;
- il diritto alla portabilità dei dati, ovvero il diritto a ricevere dal titolare del trattamento un formato contenente tutti i dati personali dell'interessato che questi deve trasferire ad un altro titolare del trattamento (ad esempio il passaggio di consegne dal precedente consulente del lavoro al nuovo); questo diritto è esercitabile nei casi in cui il trattamento si basi sul consenso o su un contratto. Anche in questo caso si capisce la necessità del datore di lavoro o in generale di un qualunque titolare, di elaborare un sistema che renda possibile la creazione del "formato strutturato";
- il diritto di opposizione, esercitabile in qualsiasi momento. Il titolare del trattamento deve immediatamente interrompere il trattamento dei dati a meno che non dimostri l'esistenza di motivi legittimi che prevalgono sui diritti dell'interessato.

E' facile capire come il titolare del trattamento sia sottoposto ad una normativa per alcuni lati molto "rischiosa" ed è chiara la necessità di adoperarsi di tutti gli strumenti necessari per l'adeguamento alla disciplina. In tema di controlli a distanza, i dati raccolti attraverso i videoterminali devono necessariamente rispettare i principi del GDPR mentre la liceità del controllo derivante dagli strumenti del lavoro poggia, oltre che sull'adeguatezza alla disciplina e il rispetto della privacy, anche sulla conformità dell'informativa consegnata ai dipendenti. L'informativa dovrà precisare le modalità di effettuazione dei controlli e di raccolta dati, pena l'inutilizzabilità del dato raccolto, anche ai fini disciplinari.

2.4 Gli altri adempimenti: il registro dei trattamenti, la DPIA, la nomina del DPO

Il Regolamento prescrive una serie di adempimenti che devono essere effettuati nel caso in cui il trattamento dei dati ricada all'interno delle casistiche previste.

Prima di tutti è la "Valutazione d'impatto sulla protezione dei dati" (*Data Protection Impact Assessment* – DPIA) indicata all'art.35. L'elaborazione preventiva del documento è obbligatoria in tre casi specifici ovvero il trattamento automatizzato dei dati, compresa la profilazione, che produce effetti giuridici sugli interessati, il trattamento su larga scala di categorie particolari di dati e la sorveglianza sistematica su larga scala di una zona accessibile al pubblico. Analizzando più da vicino le casistiche, si potrebbe pensare che la valutazione d'impatto sia obbligatoria solo per un bersaglio ristretto di titolari del trattamento. Il primo caso è molto raro, il secondo e il terzo caso poggiano sul concetto di "larga scala". Secondo il Considerando 91 il concetto di larga scala concerne un trattamento notevole di quantità di dati che deve essere misurato con l'individuazione della quantità degli interessati diretti rapportata al numero di interessati accumunati dalla stessa caratteristica o dalla stessa portata geografica, colpiti dalla stessa finalità di trattamento dei dati[23]. In realtà, l'articolo apre indicando espressamente che il trattamento dei dati deve essere anticipato dalla valutazione d'impatto "*ogni qualvolta rappresenti un rischio elevato per i diritti e le libertà delle persone fisiche*": si ricava chiaramente il collegamento al principio dell'*accountability* e l'obbligatorietà per la maggior parte dei soggetti che trattano dati di sviluppare la valutazione. L'obbligo della DPIA si ha, secondo le Linee Guida del documento Working Party 29 n.248[24], in alcuni casi specificamente indicati; tra i citati ci sono il caso di trattamento di dati sensibili e il monitoraggio continuo dei dipendenti attraverso sistemi di videosorveglianza.

La DPIA deve contenere almeno una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compresi gli eventuali interessi legittimi; deve altresì contenere la valutazione della necessità e proporzionalità dei trattamenti in base alle finalità, i rischi ai quali i dati trattati sono soggetti, le misure di sicurezza poste in essere dal titolare del trattamento e eventuali rischi residui non eliminabili. La particolarità della valutazione d'impatto risiede al paragrafo 11 dell'art.35 che prescrive l'obbligo di rielaborazione del documento almeno quando avvengono variazioni: si tratta di un processo di revisione continuo, non di un unico adempimento contestuale all'inizio del trattamento e soprattutto, nel

[23] Si pensi, per esempio, al dottore commercialista che elabora le dichiarazioni dei redditi di 1000 clienti; anche se il numero a prima vista sembra elevato, questo dovrebbe essere rapportato a livello nazionale (portata geografica dell'evento). Quanti sono i contribuenti che presentano le dichiarazioni e si affidano ad altri studi? Sicuramente il concetto di "larga scala" viene meno.

[24] Documento disponibile sul sito: ttps://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/7015994

caso in cui il titolare non procedesse al riesame della valutazione, potrebbe essere accusato di non aver valutato i rischi e adottato misure di sicurezza in armonia con il principio dell'*accountability*. E' disponibile sul sito del Garante Privacy un software per l'elaborazione di una valutazione d'impatto "standardizzata"; il software è stato elaborato dal CNIL francese ed è stato successivamente tradotto e messo a disposizione per gli utenti italiani.

Nel caso in cui la valutazione d'impatto mostri un rischio elevato per i diritti e le libertà degli interessati, non limitabile dalle misure di sicurezza, il titolare del trattamento è obbligato a richiedere consultazione preventiva al Garante Privacy; la richiesta è soggiogata alla capacità del titolare di capire, attraverso le riflessioni e valutazioni precedentemente effettuate, la necessità della consultazione preventiva.

La valutazione d'impatto realizza chiaramente uno dei principi cardine del GDPR, il "*privacy by design*" ovvero la protezione dei dati fin dal momento della progettazione, quando il titolare deve avvalersi di misure tecniche e organizzative adeguate (quali la pseudonimizzazione, la minimizzazione ecc...). Come chiariscono le Linee Guida del 4 ottobre 2017, anche se non vi è obbligo generale di pubblicazione della DPIA, questa è comunque consigliata come dimostrazione della trasparenza e della responsabilizzazione adottata dal titolare del trattamento.

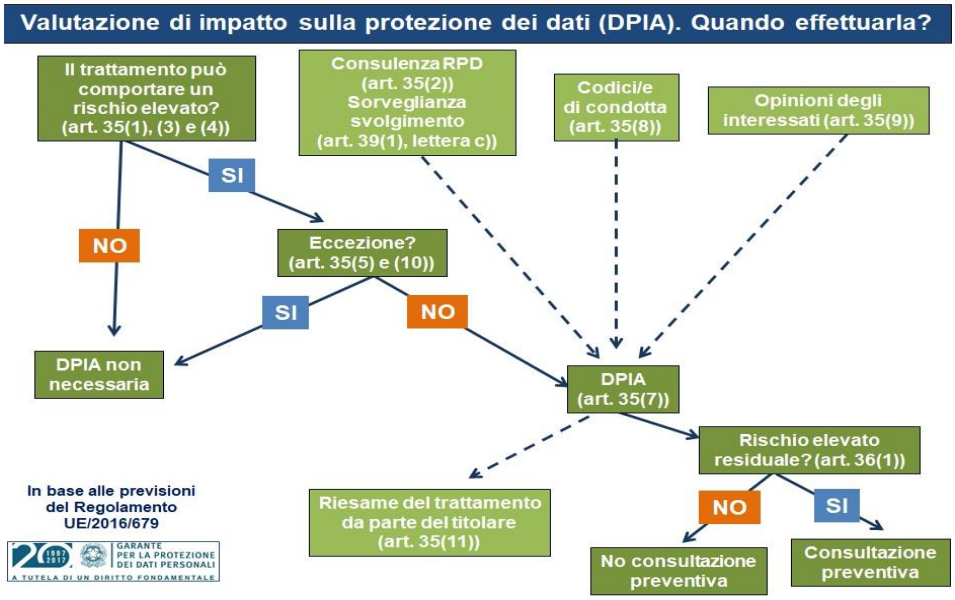

Immagine disponibile sul sito https://www.garanteprivacy.it/regolamentoue/DPIA

Il registro dei trattamenti costituisce un ulteriore adempimento prescritto dal Regolamento all'art.30. Consiste in un registro contenente tutte le attività di trattamento; le informazioni necessarie riguardano i nomi e i dati di contatto del titolare, del contitolare, del responsabile

del trattamento e del responsabile della protezione dei dati, piuttosto che le finalità del trattamento, la descrizione delle categorie di interessati e delle categorie di dati personali, i destinatari, le misure di sicurezza adottate. Il registro deve essere tenuto in forma scritta oppure in formato elettronico e deve essere esibito al Garante nel caso in cui questo ne faccia richiesta. Il paragrafo 5 dell'articolo dispone l'obbligo del registro dei trattamenti per le aziende con più di 250 dipendenti, per il trattamento non occasionale di dati *ex* art.9 e 10 e in generale per ogni trattamento che "possa presentare un rischio per i diritti e le libertà dell'interessato". Si ricade in questo modo nello schema ricorrente, valido anche per la valutazione d'impatto: in un primo momento si ha la sensazione che l'adempimento sia obbligatorio solo per grandi realtà strutturate ma da un'analisi più approfondita ne deriva l'obbligo per tutti coloro che trattano dati personali. A sostegno di questa tesi il Garante ha esposto alcune raccomandazioni sul proprio sito[25] indicando espressamente che il Registro dei trattamenti non costituisce un obbligo formale bensì parte integrante del sistema di corretta gestione dei dati personali e invitando i titolari del trattamento e i responsabili, a prescindere dalle dimensioni dell'organizzazione o dell'impresa, ad effettuare tutti i passi necessari all'elaborazione di tale registro.

Nuova figura è quella del DPO – D*ata Protection Officer* – o "responsabile per la protezione dei dati". La designazione di un responsabile, esterno o interno all'azienda, è compito del titolare del trattamento ed è prevista, anche in questo caso, al verificarsi di situazioni espressamente indicate nel Regolamento. La designazione è obbligatoria per il trattamento dati da parte soggetti pubblici con un'unica eccezione (l'Autorità giurisdizionale nell'esercizio delle sue funzioni) e per tutti quei soggetti privati che svolgono attività principali di monitoraggio regolare e sistematico degli interessati o trattamento di dati sensibili e/o giudiziari (tra cui i dati relativi alla salute e l'appartenenza sindacale) su larga scala; le casistiche sono alternative. Si ricade sui concetti già precedentemente visti in tema di valutazione d'impatto. Il parere del Working Party n.243/2016 coadiuva con modalità più precise nell'interpretazione di tali concetti un po' "volatili", tipici del fenomeno della "*soft law*"[26], in particolare sostiene che il concetto di *larga scala* deve essere misurato come il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento, il volume dei dati e/o le diverse tipologie di dati

[25]GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (2018), *Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali, Edizione aggiornata a febbraio 2018, pag.26-27*. Disponibile sul sito: https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf

[26] Con il termine "soft law" si intende il metodo, adottato del Legislatore Europeo, di coordinamento aperto che vede le Autorità nazionali, nel nostro caso il Garante Privacy e gli organi affiliati, impegnati nell'elaborazione di linee guida interpretative.
BARRACO, E. (2016). POTERE DI CONTROLLO E PRIVACY (2016). Milano: Wolters Kluver Italia S.r.l., pag. 124.

oggetto di trattamento, la durata, ovvero la persistenza dell'attività di trattamento o la portata geografica dell'attività di trattamento e presenta a riguardo diversi esempi. Il concetto di *monitoraggio regolare e sistematico*, sicuramente rilevante ai fini dei controlli a distanza, viene inteso invece come il monitoraggio del comportamento degli interessati che avviene a intervalli definiti o comunque ripetuti nel tempo secondo uno schema temporale, attuato tramite un sistema predeterminato o svolto nell'ambito di una strategia. Il reindirizzamento di messaggi di posta elettronica, le attività di profilazione e *scoring* per finalità di valutazione del rischio (per esempio, per prevenzione delle frodi e quindi per "tutela del patrimonio aziendale"), il tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili o i sistemi di videosorveglianza costituiscono esempi espressi e trattati nel documento sopraesposto[27].

Il ruolo del Responsabile per la protezione dei dati ingloba tutte le questioni che riguardano il trattamento dei dati, dalla consulenza alla formazione dei dipendenti, dal controllo sull'osservanza del GDPR al parere sulla valutazione d'impatto piuttosto che la cooperazione con l'autorità di controllo. Devono essergli forniti tutti i mezzi necessari all'espletamento delle sue funzioni e non deve ricevere alcuna indicazione dal titolare/responsabile del trattamento riguardo l'esecuzione dei suoi compiti. E' direttamente responsabile assieme al titolare e responsabile del trattamento e non può operare nel caso di conflitto di interessi.

La figura del DPO è soggetta ai requisiti di professionalità e conoscenza specialistica in ambito privacy; anche in questo caso in Regolamento non fornisce un elenco puntuale di requisiti specifici ma si limita a indicare le competenze in modo generale. La legittimità dell'operato risiede nell'istanza di comunicazione del nominativo presentata al Garante per la protezione dei dati personali tramite una procedura online direttamente indicata nel sito ufficiale[28]. La designazione del DPO può essere anche volontaria, a discrezione del titolare del trattamento, a seguito delle valutazioni da lui poste in essere. Nel caso in cui il DPO sia designato volontariamente è ovviamente valida la stessa regolamentazione del caso di designazione obbligatoria. Il diritto dell'UE o degli Stati membri può comunque prevedere altri casi obbligatori, aggiuntivi rispetto a quelli del Regolamento.

[27] GRUPPO DI LAVORO PER LA PROTEZIONE DEI DATI, 2016. *Linee guida sui responsabili della protezione dei dati*. *Adottate il 13 dicembre 2016 Versione emendata e adottata in data 5 aprile 2017* [online]. Disponibile sul sito: https://www.garanteprivacy.it/documents/10160/0/WP+243+-+Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf [data di accesso: 12/07/2018].

[28] Procedura di nomina del DPO al sito: https://www.garanteprivacy.it/regolamentoue/rpd

2.5 Violazioni, responsabilità e sanzioni

Già nell'informativa è indicata la possibilità per l'interessato di proporre reclamo, oltre ad ogni altro ricorso amministrativo o giurisdizionale, all'autorità di controllo dello Stato membro nel momento in cui ritenga che un determinato trattamento sia lesivo nei suoi confronti. Le autorità giurisdizionali competenti sono situate o nello Stato membro in cui il titolare del trattamento ha uno stabilimento oppure, in alternativa, nello Stato membro in cui l'interessato risiede abitualmente; vale il criterio della residenza dell'interessato anche per la designazione dell'autorità di controllo, al quale si aggiunge il luogo in cui l'interessato lavora o il luogo in cui si presume si sia verificata la violazione. Per agevolare la proposta di reclamo, l'autorità di controllo dovrebbe predisporre dei moduli adatti, attraverso i quali è possibile inviare, anche elettronicamente, la segnalazione. L'interessato può proporre reclamo singolarmente o tramite organizzazione o associazione senza scopo di lucro, altresì senza mandato; anche in questo caso la regola nasce con lo scopo di fornire una tutela forte a interessi che si inseriscono in un contesto generale e trovano rilevanza nella somma e nella sintesi di tante posizioni individuali[29] (Candini, Finocchiaro, 2018). Precedentemente, la direttiva 95/46/CE a causa della fissità dei processi prescritti, non riusciva a realizzare il miglioramento della protezione dei dati personali; al contrario, il Regolamento predispone le basi per la creazione di meccanismi e procedure efficaci che hanno come obbiettivo generale la protezione dei dati personali, ma nello specifico dei trattamenti che potenzialmente presentano un rischio elevato per i diritti e le libertà delle persone fisiche, per esempio a causa del crescente utilizzo delle nuove tecnologie.

La normativa prevede anche il caso di ricorso giurisdizionale nei confronti dell'autorità del Garante, nel caso in cui la decisione promossa non sia condivisa e l'interessato sia predisposto al ricorso; il ricorso è possibile anche se, a tre mesi dalla segnalazione, l'autorità di controllo non abbia trattato il reclamo ricevuto.

Anche il titolare del trattamento può rivolgersi all'autorità garante del Paese in cui è stabilito, ad opera del principio "One stop shop" : se il titolare del trattamento o il responsabile del trattamento è stabilito in più di uno Stato membro o se il trattamento incide o può verosimilmente incidere in modo sostanziale su interessati in più di uno Stato membro, l'autorità di controllo dello stabilimento principale del titolare del trattamento o del

[29] CANDINI A., & FINOCCHIARO G., 2018,. Conto alla rovescia per la nuova privacy. *Il Sole 24ORE*, Norme & tributi (25 aprile)" p. 11.

responsabile del trattamento o dello stabilimento unico funge da autorità capofila. L'autorità capofila deve cooperare con le altre autorità interessate ed è competente per l'adozione di decisioni vincolanti. Ogni autorità di controllo che non agisce in qualità di autorità di controllo capofila, previo coordinamento con quest'ultima, rimane competente a trattare casi locali qualora l'oggetto dello specifico trattamento riguardi unicamente il trattamento effettuato in un singolo Stato membro e coinvolga soltanto interessati in tale singolo Stato membro (ad esempio quando l'oggetto riguardi il trattamento di dati personali di dipendenti nell'ambito di specifici rapporti di lavoro in uno Stato membro). Per quale motivo il titolare del trattamento dovrebbe rivolgersi all'autorità di controllo? Circostanza poco gradita ma obbligatoria è il verificarsi del cosiddetto "*data breach*", ovvero la violazione dei dati personali dell'interessato. Per **"**violazione di dati" si intende "*la violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati"*[30]; attenzione che anche l'incendio di un archivio o il furto di un laptop viene considerato "*data breach*", rientrando nella definizione. La comunicazione al Garante deve essere fatta entro 72 ore dal momento in cui si viene a conoscenza della violazione; nel caso di sforamento del termine si devono dimostrare le motivazioni per le quali la segnalazione ha subito un ritardo. Il titolare del trattamento ha l'obbligo di documentare qualunque violazione dei dati personali, i rimedi messi in atto e le eventuali conseguenze sui diritti e le libertà della persona fisica. Il contenuto della comunicazione è costituito dalla descrizione della natura della violazione dei dati personali, dalle probabili conseguenze e dalle misure messe in atto per limitare, eliminare, attenuare gli effetti negativi del *data breach*. Anche in questo caso, secondo il principio dell'*accountability*, è il titolare del trattamento che deve valutare la gravità della violazione e deve autonomamente decidere se intraprendere la strada di segnalazione al Garante o se ritiene che i diritti e le libertà dei cittadini non siano stati compromessi e quindi la segnalazione non ha motivo di essere fatta. La comunicazione è obbligatoria anche nei confronti dell'interessato e deve essere redatta con un linguaggio semplice, chiaro e comprensibile al lettore. Qualora, però, sia rispettato almeno uno dei presupposti dell'art. 34, allora l'obbligatorietà della comunicazione viene meno: il titolare deve aver messo precedentemente in atto misure di sicurezza adeguate che permettano di rendere i dati incomprensibili (c.d. cifratura) oppure le suddette misure sono state adottate al

[30] Come indica la definizione dell'art.4 paragrafo 12 del Regolamento (UE) 2016/679.

momento di sopraggiungimento della problematica, o invece la comunicazione richiede sforzi spropositati per il titolare del trattamento[31].

Il Regolamento prescrive il risarcimento per chiunque subisca un danno materiale o immateriale cagionato dalla violazione della normativa. La responsabilità è del titolare del trattamento o del responsabile del trattamento (quest'ultimo solo se non ha adempiuto agli obblighi da lui sottoscritti) e l'onere della prova grava sui due e non sull'interessato: il titolare o responsabile del trattamento deve dimostrare che l'evento dannoso si è verificato non a causa dell'inadeguatezza del trattamento piuttosto che delle misure di sicurezza bensì per cause a lui in alcun modo non imputabili. Nel caso in cui i due soggetti operino congiuntamente la responsabilità è solidale, salvo il diritto di rivalsa in proporzione alla responsabilità attribuita al responsabile del trattamento nel contratto di nomina.

Le sanzioni amministrative pecuniarie irrorate devono presentare, in conformità con la disciplina, le caratteristiche di effettività, proporzionalità e di deterrente. Vi sono diversi elementi che concorrono alla formazione dell'importo, tra i quali la natura e la gravità della violazione, l'oggetto e la finalità del trattamento, il numero di interessati coinvolti, il carattere colposo o doloso della violazione, le misure adottate in termini di sicurezza, il grado di cooperazione con l'autorità di controllo piuttosto che eventuali precedenti violazioni, l'adesione ai codici di condotta o altri fattori aggravanti. "Il Regolamento si limita a indicare il massimo importo delle sanzioni amministrative"[32] (Bottini, Pucci, 2018), quindi la determinazione puntuale è a discrezione dell'Autorità. Le sanzioni amministrative sono previste dall'articolo 83 del Regolamento e possono arrivare a seconda delle norme violate:

- fino a 10 milioni di euro, o per le imprese, fino al 2 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, nel caso di violazioni di obblighi del titolare e/o responsabile del trattamento quali, per esempio, la mancata protezione dei dati secondo il principio "privacy by design", la realizzazione dei compiti del responsabile del trattamento non conforme con la normativa, la mancata formazione dell'incaricato, la mancata adozione delle misure di sicurezza a protezione dei dati o la mancata notifica di violazione dei dati all'Autorità di controllo;
- fino a 20 milioni di euro, o per le imprese, fino al 4% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore, per esempio, per violazioni dei principi base del trattamento e le condizioni relative al consenso, per il non rispetto dei diritti

[31] Tale comunicazione può essere sostituita da comunicazione pubblica o misura simile.

[32] BOTTINI, A., & PUCCI, P., 2018. Conto alla rovescia per la nuova privacy. *Il Sole 24ORE*, Norme & Tributi (25 aprile), p. 14.

dell'interessato o la disciplina relativa all'informativa, o meglio ancora per i trasferimenti dei dati personali in Paesi terzi[33].

Il potere di applicare sanzioni è esercitato in aggiunta ad altri poteri correttivi indicati all'art.58 paragrafo 2 del Regolamento, come gli avvertimenti o gli ammonimenti[34]; quindi, anche se l'importo massimo dell'apparato sanzionatorio ha la capacità di far chiudere la maggior parte delle PMI del nostro territorio, si deve tener conto che le sanzioni indicate hanno (anche) lo scopo di scoraggiare il trattamento illecito dei dati e hanno carattere inibitorio. Questo però non vuol dire che l'Autorità non possa applicarle, in quanto previste dalla normativa. Sicuramente, la completezza dello status di "*GDPR compliant*" non concerne la sistemazione superficiale di qualche documento qui e là, ma è l'inizio di un percorso di adeguamento tutt'altro che semplice e veloce.

[33] I trasferimenti di dati verso Paesi extra-UE sono disciplinati nel Capo V del Regolamento; il trasferimento dei dati è ammesso se la Commissione "certifica" l'adeguatezza del Paese di destinazione, secondo criteri puntuali, tra cui il funzionamento delle autorità di controllo, gli impegni internazionali portati a termine, la serietà delle istituzioni e quant'altro. In mancanza di certificazione, il titolare del trattamento può comunque trasferire dati in Paesi extra-UE a patto che fornisca delle garanzie adeguate e che gli interessati possano esercitare i diritti; nell'informativa il soggetto extra-UE di destinazione deve essere obbligatoriamente indicato. Anche se la disposizione può sembrare in un primo momento poco concreta, si tenga presente che anche l'archiviazione in Cloud su piattaforme di soggetti extra-UE potrebbe costituire "trasferimento dei dati verso Paesi terzi" e quindi il titolare del trattamento dovrebbe adempiere a una serie di obblighi aggiuntivi rispetto ai trattamenti effettuati in territorio UE.

[34] Il Considerando 148 sostiene che, in caso di violazione minore, potrebbe essere rivolto un ammonimento anziché una sanzione pecuniaria.

CAPITOLO III – GLI ADEMPIMENTI IN PRATICA ED ALCUNI CASI PARTICOLARI

3.1 Dalla teoria alla pratica

In tema di controlli a distanza si deve tenere ben presente che l'oggetto del controllo è l'attività del lavoratore, non il lavoratore in sé inteso come persona (Agostini, 2017); proprio per questo motivo le riprese effettuate dai videoterminali devono essere "incidentali", coerenti con l'art.5 del Regolamento ovvero il principio di minimizzazione dei dati. Nell'accordo con le OO.SS (o in mancanza, l'autorizzazione dell'Ispettorato Nazionale del Lavoro) il datore di lavoro deve specificare puntualmente le finalità sottese all'istallazione degli impianti (ricollegabili ovviamente alle motivazioni di tutela del patrimonio aziendale o a esigenze tecnico-organizzative), la descrizione degli strumenti e le modalità di funzionamento oltre che il periodo di conservazione dei dati e i soggetti abilitati all'accesso ai dati; ricorrono in questo elenco altri principi del GDPR, quali il tempo di conservazione dei dati ma anche la definizione delle modalità e mezzi che vigono in capo al titolare del trattamento. Nel caso in cui il datore di lavoro non proceda come definito dall'art.4 comma 1 o non provveda a informare preventivamente i lavoratori sulle modalità di funzionamento del sistema di videosorveglianza si vede l'applicazione del comma 3 ovvero la conseguenza dell'inutilizzabilità dei dati ai fini del rapporto di lavoro.

Ma, nella pratica, date le disposizioni del Regolamento UE 2016/679, che cosa cambia concretamente per le aziende e per i datori di lavoro? Quali sono gli adempimenti da porre in essere per non vedersi annullare delle potenziali prove che testimoniano la negligenza del dipendente? Innanzitutto, si deve prendere in considerazione la possibilità che il datore di lavoro deleghi la gestione dei dati raccolti in tema di videosorveglianza (per esempio le immagini raccolte, i video ecc..) ad una figura esterna, ovvero ad un responsabile del trattamento. Anche se sembra una casistica alquanto remota, si pensi solamente all'archiviazione in cloud delle riprese: la casa di software dovrebbe essere nominata responsabile del trattamento in questo caso. Il responsabile del trattamento deve avere i requisiti del "*gdpr compliant*" per investire questo ruolo e il tutto deve concretizzarsi attraverso l'atto di nomina. Situazione a cui si deve prestare molta attenzione è il caso in cui il responsabile del trattamento sia un soggetto extra-UE (nell'esempio in esame, la società di cloud potrebbe avere sede legale in territorio extra-UE) e quindi il trasferimento di dati rientra

nella casistica: il titolare del trattamento deve verificare che il Paese di destinazione dei dati sia ritenuto congruo dalla Commissione in base al Capo V del Regolamento oppure, in mancanza di certificazione, questo deve prestare ulteriore garanzie a protezione dei dati degli interessati.

Ulteriore problematica, sia per il titolare del trattamento che per il responsabile del trattamento, è lo status di "*gdpr compliant*". Argomento su cui già ci si è espressi è che lo status di "*gdpr compliant*" si acquista al completamento dell'adeguamento alla disciplina Ue; problematica portata alla luce da diversi specialisti in materia[35] è che, in alcuni casi, l'applicazione delle "misure minime di sicurezza", in particolare la "pseudonimizzazione", non è possibile. Si pensi all'archiviazione di filmati, non è possibile rompere i fotogrammi in diverse parti in modo che, se parte del dato viene perduto, la parte restante risulta incomprensibile a chi lo consulta; stessa cosa vale per dei documenti che vengono prodotti e archiviati in formato .pdf (si pensi alle buste paga dei dipendenti). Le *software house* al momento sono state informate della problematica ma le tecnologie disponibili non permettono, per alcuni formati, di attuare questo meccanismo di protezione. La questione che ci si pone è che, alla luce di quanto si è detto, nessuno sarebbe adatto a trattare dati in quanto uno dei requisiti minimi di sicurezza è violato: ci si aspetta che il Garante esponga la sua opinione in merito.

Altro fatto concreto è la modifica dell'informativa: il comma 2 dell'art.4 Statuto Lavoratori prevede la consegna di un'informativa che comunichi agli interessati il funzionamento degli strumenti di lavoro e le possibilità di controllo che ne derivano. Le informative consegnate prima del 25 maggio 2018 non sono sicuramente in armonia con l'art.13 del *General Data Protection Regulation* perché in difetto su due fronti: l'informazione all'interessato della possibilità di rivolgersi direttamente all'Autorità di controllo per le segnalazioni, in caso di violazione, e la durata del trattamento dei dati. Particolare attenzione si deve prestare al momento di redazione dell'informativa, nell'indicare tutti gli incaricati o i responsabili del trattamento destinati a lavorare con i dati raccolti oppure se vi è la possibilità che i dati vengano trasferiti in Paesi extra-UE.

C'è chi sostiene, che oltre alla consegna dell'informativa in caso di rapporto di lavoro, sia auspicabile la raccolta del consenso al trattamento dei dati. Secondo le teorie dell'interesse legittimo questo non sarebbe opponibile in caso di contenzioso perché il lavoratore sarebbe sottoposto a una pressione troppo evidente perché il consenso sia prestato in piena libertà.

[35] SCHIAVONE, R., Master di specializzazione erogato da Euroconference – Centro Studi Lavoro e Previdenza. *"Gestione della privacy nei rapporti di lavoro*"; Venezia, in data 23/05/2018 e 30/05/2018.

Alcuni sostengono[36] che il trattamento dei dati, in caso di contenzioso, è "eventuale" e non "obbligatorio" come nel rapporto di lavoro: cambierebbero quindi le finalità del trattamento che è legittimo solo per l'espletamento del contratto di lavoro e non in sede giudiziaria. Il suggerimento è quello di raccogliere comunque il consenso ed eventualmente non utilizzarlo.

Se vi sono soggetti, diversi dal titolare del trattamento, quali i responsabili del trattamento e gli "incaricati al trattamento"[37], vi è la necessità che questi abbiano intrapreso un percorso di formazione in tema di privacy e trattamento dei dati. Nel Regolamento non vi è nessuna specifica riguardo alla durata della formazione, piuttosto che agli argomenti, al rilascio di qualche tipo di attestato e quant'altro; anche in questo caso le disposizioni sono generiche. Il suggerimento che si può dare è di documentare la formazione, in caso di controllo dell'Autorità, indicando in particolare l'ingresso dell'entrata-uscita al corso di formazione, il programma del corso, la documentazione consegnata, il test di autovalutazione e una marca temporale per l'indicazione della data certa.

Il Registro dei trattamenti rappresenta un'altra novità del Regolamento e quindi un nuovo adempimento. Deve essere redatto da tutti i datori di lavoro ed esibito alle Autorità in caso di controllo. Il Registro dei trattamenti è un elaborato riassuntivo che permette velocemente di capire, a chi lo consulta, quali sono i trattamenti in attività e la loro durata, suddivisi per categoria di interessati. Proprio per questa sua caratteristica, il registro dei trattamenti non cessa mai di essere aggiornato: è un processo continuo e ricorrente in base alla durata indicata dei relativi trattamenti. Attualmente, diverse *software house* hanno elaborato dei programmi che permettono di predisporre il Registro dei trattamenti e di inserire degli "*allert*" che permettono di verificare, in prossimità della scadenza, la necessità del rinnovo del trattamento oppure il suo venir meno.

Anche la Valutazione d'impatto, seppur non obbligatoria se non in casi specifici, costituisce un buon metodo per l'espressione del principio dell'*accountability*. Nel caso dell'istallazione di impianti di videosorveglianza è sicuramente richiesta, come indicano peraltro le Linee Guida del Working Party *ex* art. 29. Valutare i rischi e le problematiche derivanti dalla ripresa incidentale sui dipendenti è utile al datore di lavoro per comprendere se esiste la necessità di richiesta di consultazione preventiva al Garante oppure se le misure di sicurezza sono adeguate, se il trattamento dei dati non eccede le finalità e in generale per definire un quadro completo dei trattamenti predisposti. La valutazione d'impatto è uno degli adempimenti che

[36] SCHIAVONE, R., Master di specializzazione erogato da Euroconference – Centro Studi Lavoro e Previdenza. *"Gestione della privacy nei rapporti di lavoro*"; Venezia, in data 23/05/2018 e 30/05/2018.
[37] Secondo la definizione puntuale del Codice Privacy; la definizione di incaricato manca nel Regolamento UE 2016/679.

sicuramente richiede più tempo: per ogni *asset* aziendale si devono indicare le categorie di dati trattati, i soggetti che possono intervenire sui dati oppure consultarli, le minacce riscontrate e le misure di sicurezza adottate. A titolo di esempio, per un impianto di videosorveglianza, ogni videocamera dovrebbe essere valutata in base alle minacce che comporterebbero un *data breach* (manomissione, incendio, perdita dei dati dovuta ad allentamento della tensione elettrica, introduzione di Malware che interferiscono con il funzionamento...) e alle relative misure di sicurezza adottate (sistema di rilevamento fumo e gas, estintori, gruppo di continuità istallato, utilizzo di antivirus nel sistema..). Più è specifica la valutazione d'impatto, più è utile al titolare del trattamento nella valutazione dei rischi e più è dimostrazione del principio di *accountability* dinanzi all'Autorità di controllo. Anche in questo caso il processo di elaborazione è ricorrente perché il documento va implementato per ogni nuovo *asset* acquisito in azienda.

I carichi indicati devono essere impostati di *default* dal datore di lavoro, con lo scopo di proteggere il suo potere esercitabile sul lavoratore. Ci sono dei casi, indicati dal WP249, che ricorrono in tema di controlli a distanza dei lavoratori. La crescente penetrazione degli strumenti informatici individuati come strumenti di lavoro e l'avvento di figure come gli *smartworking*[38] hanno richiesto l'illuminazione del Garante più e più volte; l'ambiente produttivo espone a carichi lavorativi eccessivi e si proietta sulla salute dei lavoratori, alimentando i rischi sociali generati dalla invasione dello spazio riservato alla vita personale ad opera dell'espletamento delle attività di lavoro[39] (Poletti, 2017) ma anche i rischi aziendali aumentano a causa dell'esposizione dei database alle minacce esterne.

3.2 Caso particolare: il monitoraggio degli strumenti di lavoro elettronici

Può capitare che il lavoratore utilizzi gli strumenti di lavoro informatici[40] per questioni personali, non legati alla prestazione lavorativa. Da considerare l'esistenza di tecnologie informatiche utilizzabili dal datore di lavoro per il controllo a distanza del lavoratore, "pericolose" in tema di diritti e libertà del lavoratore quasi quanto un sistema di videosorveglianza (si pensi ai sistemi di *Data Loss Prevention*[41]*, eDiscovery technologies*[42],

[38] In lingua italiana "lavoratore agile". Sono lavoratori che offrono la prestazione lavorativa fuori dal contesto aziendale. Precedentemente intesi come sinonimo di "telelavoristi" attualmente assumono una concezione più generale: gli *smart working* possono lavorare in ogni luogo grazie soprattutto ai sistemi di connessione Internet e Wi-fi, accedendo quotidianamente ai database aziendali.

[39] POLETTI, D., 2017. *IL C.D. DIRITTO ALLA DISCONNESSIONE NEL CONTESTO DEI «DIRITTI DIGITALI »*, Responsabilita' Civile e Previdenza, fascicolo 1, pag. 3.

[40] Ne sono esempio PC, tablet, smartphone ecc...

[41] Tecnica di individuazione e prevenzione di trasmissione dati non autorizzata relativamente a dati e informazioni aziendali riservate, tramite e-mail o in generale mezzi di comunicazione elettronici.

BYOD[43]). E' risaputo che l'utilizzo di queste tecnologie ai fini del mero controllo a distanza è assolutamente vietato; è quindi più auspicabile adottare soluzioni diverse volte ad anticipare il ricorso "ad accessi successivi ai dati dei lavoratori"[44] (Agostini, 2017) come la predisposizione di un elenco di siti in cui la navigazione è vietata, la previsione di calendari di posta personali, la predisposizione di un'apposita *policy* per l'uso della strumentazione informatica.

Aggiuntive rispetto a quelle indicate sono le raccomandazioni del WP249 in caso di procedure *Data Loss Prevention*. Il datore di lavoro dovrebbe informare i lavoratori dell'utilizzo della procedura e indicare le regole che il programma segue per identificare la violazione all'obbligo alla riservatezza dei dati aziendali della mail uscente; inoltre, il datore di lavoro dovrebbe informare il lavoratore, in caso di effettiva violazione, dando la possibilità di non inviare la comunicazione.

Con particolare riferimento all'utilizzo della strumentazione informatica del lavoratore (BYOD), i controlli effettuati dal datore di lavoro sui dispositivi utilizzati, in nome della sicurezza del patrimonio aziendale (es chiedendo l'utilizzo di antivirus, scansionando il contenuto dei dispositivi ecc...) sono ritenuti un rischio troppo elevato per i diritti del lavoratore. Il datore di lavoro non può adottare misure di sicurezza non proporzionate rispetto alle finalità perseguite; ha, invece, il compito di aumentare le misure di sicurezza nel rispetto della riservatezza degli interessati. Il WP249 suggerisce, per esempio, il blocco alle aree private del lavoratore, come l'accesso all'archivio fotografico.[45]

Per quanto riguarda invece le funzionalità "*eDiscovery"*, si capisce che la finalità dei suddetti programmi è di mero controllo e quindi vietata in nome dell'art. 4 comma 1 dello Statuto dei Lavoratori.

---

[42] Sono programmi e procedure atte a individuare informazioni memorizzate in formato digitale; illecitamente il datore di lavoro può avvalersi di programmi che utilizzano questa tecnologia per ricavare delle informazioni, per esempio, dal computer del dipendente (navigazioni in siti sospetti, accesso alla mail personale...).

[43] Letteralmente "B*ring Your Own Device*", si intende l'utilizzo di dispositivi propri del lavoratore per svolgere la prestazione lavorativa. L'implementazione efficace del BYOD può comportare una serie di vantaggi per i dipendenti, tra cui migliore soddisfazione del lavoro degli impiegati, aumento generale del morale, aumento dell'efficienza lavorativa e maggiore flessibilità ma anche la rischiosità per datori di lavoro di elaborare informazioni non aziendali su tali dipendenti.

[44] AGOSTINI, C., 2017. *Dati personali dei lavoratori: il WP29 aggiorna le regole del trattamento alla luce delle nuove tecnologie informatiche e del GDPR*"[online]. Disponibile su: http://www.replegal.it/it/privacy-data-protection1/item/1387-dati-personali-dei-lavoratori-il-wp29-aggiorna-le-regole-del-trattamento-alla-luce-delle-%E2%80%A6%206/6 [data di accesso: 01/08/2018].

[45] WORKING PARTY 29 (2017); "OPINION 2/2017 ON DATA PROCESSING AT WORK". *"ICT usage outside the workplace has become more common with the growth of homeworking, remote working and "bring your own device" policies. The capabilities of such technologies can pose a risk to the private life of employees, as in many cases the monitoring systems existing in the workplace are effectively extended into the employees' domestic sphere when they use such equipment"*

3.3 Caso particolare: la geolocalizzazione attraverso il GPS

Le tecnologie di *Mobile Device Management* consentono ai datori di lavoro di individuare i dispositivi da remoto, cancellare i dati, configurare e istallare programmi. L'uso più comune è la geolocalizzazione del dispositivo in tempo reale. Il Gruppo di lavoro art.29, nelle Linee Guida, ha richiesto espressamente l'elaborazione della DPIA prima dell'impiego di qualsiasi tecnologia di questo tipo. Se l'obbiettivo è quello di un trattamento lecito dei dati, la valutazione d'impatto dovrebbe mostrarsi conforme ai principi di proporzionalità e sussidiarietà, le finalità dovrebbero essere elaborate per uno scopo specifico e non con l'unico obiettivo di monitoraggio dei dipendenti. Suggerimento delle linee guida è quello di adottare sistemi di tracciamento che registrano i dati senza predisporre una struttura di consultazione diretta: la consultazione dovrebbe rendersi disponibile solo nelle circostanze in cui il dispositivo venga segnalato, rubato oppure perso. [46]

Altro punto importante è l'informazione istantanea dei dipendenti: devono essere a conoscenza che *in quel momento* e *tramite quello strumento* è in atto un tracciamento del dispositivo. A tal proposito, si segnala il provvedimento n. 232 del 18 aprile 2018 del Garante per la protezione dei dati personali, che ha confermato la possibilità di geolocalizzazione, attraverso smartphone e tablet, del personale di una società che effettua servizi di vigilanza privata. A tutela dei lavoratori l'Autorità ha, tuttavia, richiesto di posizionare sul dispositivo di geolocalizzazione un'icona che indichi l'attivazione della localizzazione e di configurare il sistema in modo tale da oscurare la posizione geografica del dipendente decorso un periodo di inattività dell'operatore sul monitor della centrale operativa. L'Autorità ha ritenuto che la questione in oggetto seguisse i criteri di liceità, proporzionalità e necessità; è scontata la consegna dell'informativa che indichi le modalità di funzionamento del dispositivo. I dati raccolti riguardano le coordinate del GPS e la velocità del veicolo. Il periodo di conservazione stabilito dal Garante è fissato come "non superiore alle 24 ore", salvo esigenze particolari; l'accesso in tempo reale ai dati è previsto esclusivamente in caso di allarme segnalato dalla guardia giurata, furto o smarrimento del veicolo.

[46] ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017. Opinion 2/2017 on data processing at work [online]. Disponibile su: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169>*:*
"Mobile device management enables employers to locate devices remotely, deploy specific configurations and/or applications, and delete data on demand. An employer may operate this functionality himself, or use a third party to do so. MDM services also enable employers to record or track the device in real-time even if it is not reported stolen".

3.4 Caso particolare : *the internal auditing*

Il soggetto che ricopre la funzione di *audit* interno ha il compito di verificare le procedure interne dell'azienda e di analizzarle, con lo scopo di rendere i processi più efficienti. Solitamente la posizione è ricoperta da un dipendente dell'azienda. Il potere di analisi dell'*audit* comprende al suo interno anche il controllo della prestazione lavorativa degli altri dipendenti, attività che concerne sicuramente il trattamento dei dati degli stessi; la categoria dei dati raccolti può variare (esempi a riguardo potrebbero essere il tempo impiegato per la lavorazione di un determinato prodotto, la durata delle pause ecc...). Il Garante per la protezione dei dati si è espresso in merito indicando la necessità di autorizzare, come "incaricato del trattamento", l'audit interno; altri adempimenti sono la consegna dell'informativa con indicazione delle modalità di trattamento dei dati raccolti ma soprattutto la predisposizione di sistemi di sicurezza dei dati raccolti e la raccolta del consenso. In merito a quest'ultima raccomandazione si deve pensare che l'analisi ai fini dell'efficienza aziendale non riguarda direttamente il rapporto di lavoro; le finalità e i mezzi del trattamento sono diversi. E' necessario quindi il consenso perché l'analisi esula dal mero rapporto di lavoro stipulato tramite contratto.

3.5 Caso particolare : il *badge*

L'art. 4 comma 2 dello Statuto dei lavoratori non prevede (oltre che per gli strumenti di lavoro) la necessità di accordo con le rappresentanze sindacali o l'autorizzazione della DTL, anche per gli "strumenti di registrazione delle presenze". Nel caso in cui il badge, oltre ad essere uno strumento di rilevazione delle presenze, abbia anche altre funzionalità, allora in questo caso è ritenuto strumento di controllo a distanza dei lavoratori e ricadrebbe nel comma 1. A proposito si porta come esempio la sentenza della Suprema Corte n. 17.531/2017, che ha stabilito che la rilevazione dei dati di entrata e uscita dall'azienda abbinata alla captazione di altri dati (quali le sospensioni, i permessi, le pause) mediante un'apparecchiatura di controllo predisposta dal datore di lavoro con sistema RFID[47] rientri nella fattispecie prevista dall'articolo 4, comma 1, L. 300/1970, che richiede l'accordo sindacale ovvero l'autorizzazione dell'Ispettorato del lavoro.

[47] Letteralmente "*Radio Frequency Identification*". E' un sistema di radiofrequenza passivo che registra i movimenti del badge trasmettendo onde radio dal chip inserito nel dispositivo al rilevatore.

CONCLUSIONI

E' risaputo che il lavoratore è la parte debole nel contratto li lavoro e proprio per questo motivo è tutelato non solo dall'art.4 dello Statuto dei Lavoratori ma anche dalla normativa Privacy. Il datore di lavoro, dal canto suo, ha diritto ad ottenere l'adempimento dell'obbligazione lavorativa e di tutelare i propri interessi nel caso in cui il lavoratore sia inadempiente. Prima del Regolamento UE 2016/679 il datore di lavoro poteva fare affidamento sul completamento di una "checklist" per essere conforme alla disciplina privacy, senza rischiare di rendere inutilizzabili i dati raccolti dagli impianti audiovisivi istallati secondo le modalità dell'art.4 o dagli strumenti di lavoro. La sensazione attuale è molto diversa dal passato: l'usanza era quella di non prestare molta attenzione alla privacy; attualmente sembra invece che il potere disciplinare del datore di lavoro sia stato investito completamente dalla riforma e ne sia per alcuni lati anche "sottomesso". I nuovi adempimenti richiedono risorse e spendita di tempo sostanziosi e l'esborso in termini relativi è sicuramente maggiore per le piccole-medie imprese che non godono di sistemi adatti a far fronte a cambiamenti così repentini della normativa. Molto probabilmente il Garante Europeo era da un lato indirizzato a colpire i "colossi" del momento, che trattano quantità di dati mastodontiche, anche se dall'altro mirava a predisporre un quadro uniforme della materia. Ovviamente il Regolamento è disponibile già dall'anno 2016 e in molti altri Paesi europei gli organi competenti hanno attivato già da tempo il processo di adeguamento; in Italia, forse a causa di problematiche economiche più ampie, l'attenzione si è concessa solo a ridosso della scadenza e adesso si cerca di porre rimedio anche se il decreto di attuazione è ancora in fase di elaborazione (per ora la data di rimando è il 21 agosto 2018). L'autorità francese (CNIL) ha ufficializzato, tramite comunicato, che nei primi 6 mesi di entrata in vigore del Regolamento ci sarà tolleranza purché i titolari del trattamento dimostrino l'avvio del processo di adeguamento; anche se informalmente, il Garante italiano ha condiviso la presa di posizione del Cnil[48]. Tuttavia, con la deliberazione n. 437 del 26 luglio 2018, ha stabilito che per il periodo che va da luglio a dicembre 2018 sono programmati n. 30 accertamenti ispettivi effettuati anche a mezzo della Guardia di Finanza. La delibera informa anche la possibilità dell'Ufficio di avviare ulteriori attività istruttorie di carattere ispettivo in relazione a segnalazioni o reclami proposti.

[48] IMPERIALI, R., a cura di., 2018. Nei primi sei mesi ci sarà tolleranza. Il Sole 24ORE, Norme & Tributi (25 aprile), pag.3.

La superficialità con la quale si è sempre affrontata la materia della privacy è la conseguenza delle sanzioni forse non troppo salate. Il sistema sanzionatorio prima dell'avvento del Regolamento era composto da:

- per le violazioni dello Statuto dei Lavoratori: ammenda da € 154,00 ad € 1.549,00 o arresto da 15 giorni ad un anno, salvo che il fatto non costituisca un reato più grave[49]; ammessa prescrizione *ex* art. 15, D.lgs. 124/2004 di euro € 387,25 (non applicabile per i "casi più gravi" individuati dal Ministero del Lavoro[50]);
- per le violazioni del Codice Privacy: in caso di trattamento illecito dei dati acquisiti si applicava l'art.167 D.lgs. n.196/2003[51] (reato penale tipico); nel caso di difetto dell'informativa la sanzione prevista era da € 6.000,00 ad € 30.000,00[52].

Il reato penale in caso di trattamento illecito dei dati, considerando che il GDPR sostituisce di fatto il Codice Privacy (che peraltro dovrebbe essere abrogato dal decreto attuativo), cesserebbe di esistere, salvo intervento specifico del legislatore. La stessa deduzione vale anche per il reato legato alla violazione delle norme sul controllo a distanza dei lavoratori dove la sanzione penale rimanda alle sanzioni dell'art.38 dello Statuto dei Lavoratori. Si capisce palesemente che l'intervento legislativo per evitare dubbi è necessario, per non dire obbligatorio.

Per quanto riguarda l'omessa o l'inidonea elaborazione dell'informativa, la sanzione ha fatto "un balzo" dal massimo previsto dal Codice Privacy, ovvero € 30.000,00, alla possibilità di vedersi applicare fino a venti milioni di euro o, per le imprese, il 4% del fatturato. Che sia un deterrente o la situazione effettiva, è sicuramente consigliata la rielaborazione delle informative e l'attenzione ai casi in cui la consegna è obbligatoria, soprattutto quando si parla di strumenti di lavoro.

Ci si trova quindi in una posizione di stallo: è meglio elaborare un programma di adeguamento ponderato, che richiede più tempo, o cercare di sistemare quello che già si era predisposto per gli anni precedenti in modo disordinato? Sicuramente il suggerimento risiede della prima parte della domanda, ma per chi in materia di privacy ne sa poco oppure niente, destreggiarsi in un contesto poco chiaro, e per alcuni aspetti non ancora ben definito, può

[49] Art. 38, Legge 20 maggio 1970, n. 300.

[50] MINISTERO DEL LAVORO (2016) "nota n. 4343/2016". I casi indicati riguardano, in sintesi, violazioni pesanti del lavoratore come la ripresa nelle zone di pausa aziendali, la rilevazione di dati idonei a individuare l'origine razziale, la vita, le abitudini sessuali... (e in generale tutti i c.d. dati sensibili).

[51] Prevista la reclusione da sei a diciotto mesi; in casi di diffusione dei dati la reclusione si estende per un periodo da sei a ventiquattro mesi; in caso di profitto derivante da nocumento (Danno che altera o interrompe la funzionalità o l'efficacia di un fatto naturale) la reclusione va da uno a tre anni.

[52] Art. 161, D. Lgs. 30 giugno 2003, n. 196.

comportare la possibilità di incappare in situazioni tutt'altro che gradite. A tal proposito, la risposta del mercato ha visto la proliferazione di società e di professionisti che offrono assistenza e formazione in materia nonché il debutto di software per la gestione della privacy. In particolare, i nuovi software permettono di elaborare documenti standardizzati (come gli atti di nomina, la valutazione d'impatto, il registro dei trattamenti ecc...) sulla base dei dati inseriti attraverso una procedura guidata che individua, in base alle caratteristiche aziendali, gli adempimenti obbligatori e quelli facoltativi. Sicuramente, l*'assistente privacy* potrebbe essere una valida opportunità di business soprattutto per quei professionisti (avvocati e commercialisti) che vogliono costruire un portafoglio di servizi completo, costituito certamente dai servizi "base" identificativi della loro professione, ma anche dall'offerta di assistenza ad aspetti che concernono altri lati della vita aziendale. Potrebbe essere anche un "aiuto" alla redditività degli studi professionali che hanno visto ridimensionarsi le attività a causa di nuovi strumenti normativi quali la fatturazione elettronica e la dichiarazione precompilata.

Nell'epoca del cambiamento, il *General Data Protection Regulation* costituisce sicuramente una rivoluzione culturale, soprattutto per quelle aziende che hanno trattato il tema della privacy con superficialità e indifferenza; se da un lato, la modifica dell'art.4 dello Statuto dei Lavoratori aveva comportato un ridimensionamento delle tutele dei lavoratori, dall'altro, la mano del Legislatore europeo ha cercato, in qualche modo, di riequilibrare l'ago della bilancia.

Si attende adesso l'intervento del Legislatore italiano: il fatto vanificherà i nobili ideali del Regolamento o ci sarà un adeguamento effettivo alla disciplina?

Parole Totali: 13.528

Bibliografia

BARRACO, E., 2016. *POTERE DI CONTROLLO E PRIVACY 2016. 1° ed. Milano:* Wolters Kluver Italia

BOTTINI, A., & PUCCI, P., a cura di., 2018. Conto alla rovescia per la nuova privacy. *Il Sole 24ORE, Norme & Tributi* (25 aprile), pag. 14.

CANDINI, A., & FINOCCHIARO, G., a cura di., 2018. Conto alla rovescia per la nuova privacy. *Il Sole 24ORE, Norme & Tributi* (25 aprile), pag. 11.

CARDARELLO, C., D' AMORA, F., & FIORE, F., a cura di., 2018. *Adempimenti privacy per professionisti e aziende.* Milano: Giuffrè Editore. Pag. 213-216.

COLOMBO, D., a cura di., 2018. Privacy, rischi da valutare subito. *Il Sole 24ORE, Norme & tributi* (23 aprile), pag. 31.

CORAGGIO, G., a cura di., 2018. L'ufficio legale va coinvolto sin dalla fase di progettazione. *Il Sole 24ORE,* Lavoro (25 aprile), pag. 9.

DE NICOLA, A., PIZZETTI, F., & ROTUNNO, I., a cura di., 2018. L'ESPERTO RISPONDE - Privacy. Le nuove regole tra opportunità e sfide. *Il Sole 24ORE,* #135 (21 maggio), pag. 3 - 15.

FINOCCHIARO, G., & RATTI, M., a cura di., 2018. Dati personali ad ampio spettro, sono compresi anche quelli del GPS. *Il Sole 24ORE, Norme & Tributi* (25 aprile), p. 4.

IMPERIALI, R., a cura di., 2018. Nei primi sei mesi ci sarà tolleranza. *Il Sole 24ORE, Norme & Tributi* (25 aprile), pag. 3.

INGRAO, A., 2017. Il controllo disciplinare e la privacy del lavoratore dopo il Jobs Act. *Rivista Italiana del Diritto del Lavoro,* fasc.1, pag 46-51.

LAMBROU, M., 2018. Dati da proteggere nel lavoro agile. *Il Sole 24ORE, Norme & Tributi* (4 giugno), pag. 30.

POLETTI, D., 2017. IL C.D. DIRITTO ALLA DISCONNESSIONE NEL CONTESTO DEI « DIRITTI DIGITALI ». *Responsabilita' Civile e Previdenza, fascicolo 1-2017,* pag. 7-10.

ROTONDI, F.. 2018. *PRIVACY E HUMAN RESOURCES, La selezione del personale La gestione dei rapporti di lavoro L'accesso ai dati dei dipendenti Strumenti di controllo.* Milano: Wolters Kluwer Italia.

VALLEBONA, A., (2017). *Breviario di diritto del lavoro.* Torino: Giappichelli, 2017.

Sitografia

AGOSTINI, C., 2017. *Dati personali dei lavoratori: il WP29 aggiorna le regole del trattamento alla luce delle nuove tecnologie informatiche e del GDPR.* Disponibile su: <http://www.replegal.it: http://www.replegal.it/it/privacy-data-protection1/item/1387-dati-personali-dei-lavoratori-il-wp29-aggiorna-le-regole-del-trattamento-alla-luce-delle-%E2%80%A6%206/6> [data di accesso: 01/08/2018].

ARTICLE 29 DATA PROTECTION WORKING PARTY, 2017. *Opinion 2/2017 on data processing at work* [online]. Disponibile su: <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610169> [data di accesso: 26/07/2018].

BIANCHI, D., 2017. COMUNICAZIONE DATI AL TERZO. LA PRIVACY UE NON OBBLIGA LO STATO MEMBRO [online]. Ridare.it, fascicolo 7 (nota a sentenza Corte giustizia UE , 04 maggio 2017, n.13, sez. I). Disponibile su: <https://www.iusexplorer.it/Dejure/Dottrina?idDocMaster=6306243&idDataBanks=99&idUnitaDoc=0&nVigUnitaDoc=1&pagina=0&NavId=1149429260&pid=19&IsCorr=False> [data di accesso: 25/06/2018].

BUTTARELLI, G.. 2018. *La rivoluzione copernicana del 25 maggio 2018 in materia di privacy La imminente applicazione del Regolamento europeo (GDPR) sulla protezione dei dati personali* [online]. Lavoro, Diritti, Europa - Rivista nuova del diritto del lavoro, estratto 1, pag. 5. Disponibile su: <https://www.lavorodirittieuropa.it/images/articoli/pdf/ARTICOLO_BUTTARELLI.pdf> [data di accesso: 30/06/2018].

CASSARO, M., 2018. *Aspetti pratico-operativi e riflessi del nuovo GDPR nell'ambito del rapporto di lavoro* [online]. Disponibile su:

<http://ilgiuslavorista.it/articoli/focus/aspetti-pratico-operativi-e-riflessi-del-nuovo-GDPR-nell'-ambito-del-rapporto-di-lavoro> [data di accesso 25/06/2018].

CASSARO, M., 2018. *Impianti audiovisivi ed altri strumenti di controllo: chiarimenti dell'Ispettorato Nazionale del Lavoro* [online]. Disponibile su: <http://ilgiuslavorista.it/node/8967?ticket=AQIC5wM2LY4Sfcy6M43K> [data di accesso: 25/06/2018].

CNIL (s.d.). *Sous traitance: exemple de clauses*.Disponibile su <https://www.cnil.fr/fr/sous-traitance-exemple-de-clauses> [data di accesso: 28/07/2018].

CYBERLAWS, 2018. *Bozza aggiornata (10 mag.) del nuovo Codice Privacy 2018. Schema del decreto* [online]. Disponibile su: <https://www.cyberlaws.it/wp-content/uploads/2018/05/Nuova_Bozza_Decreto_Privacy_CyberLaws.pdf> [data di accesso: 25/06/2018].

DA VALLE, G., 2016. La riforma dell'art. 4 dello "Statuto dei Lavoratori": i punti fermi e le incertezze interpretative della nuova disciplina sui controlli a distanza [online]. Disponibile su: < https://www.entilocali-online.it/la-riforma-dellart-4-dello-statuto-dei-lavoratori-i-punti-fermi-e-le-incertezze-interpretative-della-nuova-disciplina-sui-controlli-a-distanza/> [data di accesso: 19/08/2018]

FESTA, M., & ROMANO, C., 2018. *Dispositivi aziendali: il trattamento dei dati mediante sistemi di localizzazione geografica* [online]. Disponibile su: <http://www.quotidianogiuridico.it/documents/2018/06/11/dispositivi-aziendali-il-trattamento-dei-dati-mediante-sistemi-di-localizzazione-geografica> [data di accesso: 25/06/2018].

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2018. *Guida all'applicazione del Regolamento Europeo in materia di protezione dei dati personali* [online]. Disponibile su: <https://www.garanteprivacy.it/documents/10160/0/Guida+all+applicazione+del+Regolamento+UE+2016+679.pdf> [data di accesso 28/06/2018].

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2018. *Provvedimento n. 437 del 26 luglio 2018* [online]. Disponibile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9025338 [data di accesso 01/08/2018].

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI, 2018. *Provvedimento n. 232 del 18 aprile 2018* [online]. Disponibile su: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9358266 [data di accesso 30/06/2018].

GAROFALO, L., 2018. *Impronte digitali per i furbetti del cartellino. L'idea della ministra Bongiorno fa discutere ma è a prova di privacy* [online]. Disponibile su: <https://www.key4biz.it/impronte-digitali-contro-i-furbetti-del-cartellino-lidea-della-ministra-bongiorno-fa-discutere-ma-e-a-prova-di-privacy/225350/> [data di accesso: 25/06/2018].

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, 2014. *Parere 6/2014 sul concetto di interesse legittimo del responsabile del trattamento ai sensi dell'articolo 7 della direttiva 95/46/CE* [online]. Disponibile su: <*http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_it.pdf*> [data di accesso 29/06/2018].

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, 2017. *Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato"* [online]. Disponibile su: <https://www.garanteprivacy.it/documents/10160/0/WP+248+-+Linee-guida+concernenti+valutazione+impatto+sulla+protezione+dati> [data di accesso 28/06/2018].

GRUPPO DI LAVORO ARTICOLO 29 PER LA PROTEZIONE DEI DATI, 2017. *Linee guida sui responsabili della protezione dei dati* [online]. Disponibile su: <https://www.garanteprivacy.it/documents/10160/0/WP+243+-+Linee-guida+sui+responsabili+della+protezione+dei+dati+%28RPD%29.pdf> [data di accesso: 12/07/2018].

HUGE, S., 2017. *L'art. 4 Statuto dei Lavoratori dopo la riforma di cui D.Lgs 151/2015: vecchie e nuove prospettive*. [online]. Disponibile su: <www.giuslavoristi.it/wp-content/uploads/2017/02/Sara-Huge-Art.-4-S.L.-07.03.2017.pdf> [data di accesso: 07/07/2018].

ISPETTORATO NAZIONALE DEL LAVORO (s.d). *Circolare n.5 del 19 febbraio 2018* [online]. Disponibile su: <https://www.ispettorato.gov.it/it-

it/orientamentiispettivi/Documents/Circolari/INL-Circolare-n-5-del-19-febbraio-2018-Videosorveglianza-signed.pdf> [data di accesso 02/07/2018].

MINISTERO DEL LAVORO E DELLE POLITICHE SOCIALI (s.d). *Comunicato stampa del 18 giugno 2015* [online]. Disponibile su: < http://www.lavoro.gov.it/stampa-e-media/Comunicati/Pagine/20150618-Controlli-a-distanza.aspx> [data di accesso 19/08/2018].

PEDRONI, F., 2018. *Posizionamento delle telecamere e difensività come condizioni di liceità del controllo a distanza non autorizzato* [online]. Disponibile su: <http://ilgiuslavorista.it/node/8788?ticket=AQIC5wM2LY4Sfcy6M43K> [data di accesso: 26/06/2018].

SAETTA, B., 2018. *European Data Protection Board (WP29)* [online]. Disponibile su: <https://protezionedatipersonali.it/gruppo-di-lavoro-art-29> [data di accesso: 28/07/2018].

VICARELLI, C., 2016. *Jobs Act, controllo del lavoratore e utilizzabilità dei dati* [online]. Disponibile su: < https://www.cristina-vicarelli.it/blog/privacy-protezioni-dati-personali/jobs-act-controllo-del-lavoratore-utilizzabilita> [data di accesso: 19/08/2018].

ZAPPATERRA, G., & ROSATI, E., 2018. *GDPR: il legittimo interesse rende lecito il trattamento dei dati* [online]. Disponibile su: <http://www.quotidianogiuridico.it/documents/2018/06/14/gdpr-il-legittimo-interesse-rende-lecito-il-trattamento-dei-dati> [data di accesso: 25/06/2018].

ZICCARDI, G., 2016. *Jobs Act e modifiche allo Statuto dei Lavoratori: problemi applicativi* [online]. Disponibile su: < http://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-di-lavoro/quotidiano/2016/02/25/jobs-act-e-modifiche-allo-statuto-dei-lavoratori-problemi-applicativi#> [data di accesso: 19/08/2018].

Fonti normative

Regolamento (UE) 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)

L. 20 maggio 1970, n. 300 - Statuto dei Lavoratori

L. 10 dicembre 2014, n. 183.

L. 25 ottobre 2017, n. 163

D.l. 30 giugno 2003, n. 196 - Codice in materia di protezione dei dati personali

D.l. 14 settembre 2015, n. 151

Giurisprudenza

Cass. sez. lav., 3 aprile 2002, n. 4746 in *Lavoro nella Giur., 2005, 9, 837*

Cass. sez. lav., 23 febbraio 2012, n. 2722 in *Dir. e Pratica Lav., 2017, 19, 1166 (*commento alla normativa)

Cass. sez. lav., 17 febbraio 2015, n. 3122 in *Ilgiuslavorista.it del 31/03/2015*

Cass. sez. lav., 14 luglio 2017, n. 17531 in *Ilgiuslavorista.it del 29/09/2017*

Corte Europea dei Diritti dell'Uomo, sez. III, 9 gennaio 2018, (ricorsi n. 1874/13 e 8567/13) in *Argomenti Dir. Lav., 2018, 2, 499* (nota a sentenza)

Conferenze

SCHIAVIONE, R., 2018. Master di specializzazione erogato da Euroconference – Centro Studi Lavoro e Previdenza. *"Gestione della privacy nei rapporti di lavoro*"; Venezia, in data 23/05/2018 e 30/05/2018.