LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il Regolamento UE n.2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente

CLAUDIA OGRISEG
Università degli Studi di Milano

vol. 2, no. 2, 2016

ISSN: 2421-2695

LaBoUR & Law Issues
Rights | Identity | Rules | Equality

Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente

CLAUDIA OGRISEG
Università degli Studi di Milano
C.ogriseg@studiomansi.com

ABSTRACT

The essay examines the EU Regulation n. 2016/679, that will enter into force as from 2018, ponting out its impact on the Data Protection for workers.

The Author assesses the UE Regulation key topics: the need of Risk Analysis and Impact Privacy Assessment with the assistance of a Data Protection Officer; the Controller obligation to design and adopt "adequate" measures for Data Protection; the worsening of penalities.

In the conclusions it is said that employee's privacy will be enforced by the EU Regulation.

Keywords: privacy; data protection officer; Jobs Act; privacy by design; privacy by default; privacy impact assessment; Regulation EU 2016/679.

Il Regolamento UE n. 2016/679 e la protezione dei dati personali nelle dinamiche giuslavoristiche: la tutela riservata al dipendente

SOMMARIO: 1. Introduzione. L'attenzione per la protezione dei dati personali nelle dinamiche giuslavoristiche. – 2. La graduale "sostituzione" della direttiva n. 95/46/CE con il Regolamento UE n. 2016/679. – 3. Il nuovo campo di applicazione territoriale e materiale. – 3.1. La puntualizzazione di principi già noti nel campo di applicazione cd. materiale. – 3.2. … e la loro portata nelle relazioni giuslavoristiche. – 3.3. Le novità che ci attendono nel campo di applicazione territoriale e materiale. – 3.4. ... e il loro impatto nel contesto occupazionale. – 4. Il potenziamento del diritto alla protezione dei dati personali. – 4.1. La puntualizzazione di principi già noti: i nuovi requisiti dell'informativa e il diritto di accesso ai propri dati. – 4.2 …. e il loro impatto nel contesto occupazionale. – 4.3. I nuovi diritti di rettifica, all'oblio, alla portabilità dei dati. – 4.4. … e la loro portata nelle dinamiche giuslavoristiche. – 5. I nuovi obblighi per i Titolari e i Responsabili del trattamento dei dati personali – 5.1. La proceduralizzazione degli obblighi di protezione dei dati personali. – 5.2. … i connessi adempimenti documentali. – 5.3. …. e l'impatto sull'organizzazione aziendale. – 6. Il riconoscimento agli Stati del potere di declinare nuovi obblighi di protezione dei dati personali nel contesto occupazionale. – 7. I nuovi poteri delle Autorità Nazionali Garanti della Protezione dei Dati Personali. – 8. Il nuovo assetto dei rimedi e delle sanzioni. – 8.1. La tutela dell'interesse ad agire in caso di violazione dei diritti alla riservatezza. – 8.2. La nuova declinazione delle sanzioni. – 9. Conclusioni.

1. Introduzione. L'attenzione per la protezione dei dati personali nelle dinamiche giuslavoristiche

Lo scorso 4 maggio ha finalmente "visto la luce" la prima parte di un ambizioso pacchetto normativo sulla protezione dei dati destinato alla ridefinizione di norme da tempo ritenute ormai obsolete ([1]). Si tratta del

([1]) La direttiva madre n.95/46/CE è stata elaborata ben prima della massiva diffusione dei *big data*, dei *social media* e dei nuovi sistemi di conservazione dati su *cloud* e gli sviluppi del terrorismo internazionale che necessitano di regole sullo *scambio di dati personali trattati da autorità pubbliche ai fini di prevenzione, indagine, accertamento e perseguimento di reati* adeguate alle esigenze di cooperazione giudiziaria e di polizia in materia penale. Il "*progresso tecnologico costante, l'evoluzione delle modalità di raccolta e di trattamento dei dati e le divergenze tra i diversi Stati membri nell'attuazione della direttiva del 1995*" da anni avevano suggerito alla Commissione Europea un intervento di riforma per garantire una più intesa tutela al "diritto alla protezione dei dati personali" Cfr. Provvedimento del Garante Privacy del 18 dicembre 2014, doc. web n.3736353. Cfr. per una ricostruzione della disciplina la pubblicazione Agenzia dell'Unione Europea per i diritti fondamentali – Consiglio Europeo (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, 2014 su http://www.echr.coe.int

Regolamento (UE) n. 2016/679 del Parlamento Europeo e del Consiglio del 27 aprile 2016 *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE*.

Elaborato dopo un lungo *iter* di negoziati tra Consiglio e Parlamento Europeo, il *Regolamento* in questione è atto "*self-executing*" ossia disciplina immediatamente esecutiva nell'ordinamento degli Stati membri (art. 288 TFUE); tuttavia per una sua espressa previsione sostituirà la disciplina previgente della direttiva madre solo nel 2018 (considerando 171 e art. 99, Reg. UE n. 2016/679).

Gli Stati membri avranno dunque a disposizione per l'aggiornamento della disciplina interna due anni, un termine adeguato per verificare quali discipline interne continueranno ad avere efficacia e quali dovranno essere archiviate e "riscritte" ([2]). Gli Stati membri inoltre potranno precisare le nuove norme anche con riguardo al trattamento di categorie particolari di dati determinando con maggiore precisione le condizioni alle quali il trattamento dei dati personali possa ritenersi lecito (considerando 10 Reg. UE n. 2016/679). In molti passaggi nel Regolamento ci si limita a declinare in maniera più puntuale e attenta molti principi già presenti nella previgente normativa adeguandoli all'elaborazione della giurisprudenza; in molti altri passaggi invece si tutela la riservatezza, secondo un nuovo sistema di responsabilità intra-aziendale, dedicando attenzione anche alle dinamiche giuslavoristiche.

L'interesse per la protezione della riservatezza nel contesto delle relazioni di lavoro è maturato in questi ultimi anni. Nella direttiva madre n. 95/46/CE non si prevedeva alcuna disciplina peculiare per il trattamento dei "dati personali" dei dipendenti. La tutela era riservata a chiunque fosse titolare di dati personali utilizzati per scopi commerciali da altri e ci si limitava a promuovere l'elaborazione di codici di condotta per la corretta applicazione delle disposizioni generali in presenza di specificità settoriali (art.27 Dir. n. 95/46/CE).

Durante l'*iter* dei negoziati tra Consiglio e Parlamento Europeo per il Regolamento, nell'aprile 2015 in seno al Consiglio d'Europa la tutela della riservatezza nel contesto lavorativo diviene oggetto della Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri. L'attenzione degli Stati membri del Consiglio d'Europa viene richiamata in merito all'esigenza di tutelare i dati

([2]) Cfr. Ciccia Messina A. – Bernardi N., *Privacy e Regolamento Europeo 2016/679*, Milano Ipsoa, 2016, 82.

personali del dipendente nei diversi ambiti in cui vengono raccolti e trattati (si pensi ai dati raccolti in occasione dell'assunzione per l'adempimento di obblighi di legge ovvero a quelli raccolti per scopi di lavoro anche tramite ICT oppure sistemi di videosorveglianza) ([3]).

Nello stesso periodo il Governo italiano è impegnato nell'adozione dei decreti legislativi sulla «*revisione della disciplina dei controlli a distanza sugli impianti e sugli strumenti di lavoro, tenendo conto dell'evoluzione tecnologica e contemperando le esigenze produttive ed organizzative dell'impresa con la tutela della dignità e della riservatezza del lavoratore*» secondo l'art. 1 co. 7, l. n. 183/2014 (c.d. Jobs Act). Nell'autunno nell'ordinamento italiano, i limiti datoriali al controllo sull'attività del dipendente vengono ridefiniti riconoscendo centralità al cd. Codice della *Privacy* ossia prescrivendo l'esigenza di contemperare il potere datoriale di controllo con i diritti della personalità (*i.e.* riservatezza, identità, protezione dei dati personali, vita privata, dignità) ([4]). Nel novellare l'art.4, legge n. 300/1970 il Governo italiano prevede che le informazioni sull'operato del dipendente registrate in documenti audiovisivi, in *file* di *log* attinenti all'attività svolta tramite *computer* o in *cookies* relativi alla navigazione *web* (pacificamente riconducibili alla nozione di dato personale) possano essere raccolte, utilizzate "*a tutti i fini del rapporto*" e conservate dal datore di lavoro qualora il dipendente sia adeguatamente informato sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli, nel rispetto dei dettami del d. lgs. n. 196/2003 ([5]). "*Il canone di generale utilizzabilità dei dati registrati dagli strumenti di controllo, telematici e informatici subisce due ordini di limiti in corrispondenza delle condizioni poste dal c. 3, art. 4 St. lav, consistenti nelle circostanze che il datore di lavoro abbia fornito al lavoratore «adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli» e, su di un altro versante, che i controlli medesimi avvengano «nel rispetto di quanto disposto dal d.lgs. 30 giugno 2003, n. 196»"* ([6]). Due condizioni concorrenti

([3]) Cfr. Deregibus V - Machì G., *Raccomandazione del Consiglio d'Europa CM/Rec(2015)5 e Jobs Act: profili di compatibilità e prospettive di tutela* in *Bolletino ADAPT* 26 marzo 2015.

([4]) Il Codice della Privacy "*garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali con particolare riferimento ma non esclusivamente al diritto di riservatezza, all'identità personale e alla protezione dei dati personali*" (art. 2, d. lgs. n. 196/2003). Sulla definizione del diritto alla protezione dei dati personali si veda sul punto G. Finocchiaro, *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Utet Torino, 2014, 151 e in particolare 152.

([5]) Cfr. art.4, co. 3, St. lav. così come modificato dall'art.23, d. lgs. n. 151/2015.

([6]) Così C. Gamba, *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove* LLI, 2016, vol. 2, no 1, § 5

che valorizzano la portata giuslavoristica dell'intero impianto normativo a tutela della protezione della riservatezza, pur con qualche incertezza ([7]).

L'indissolubile intreccio tra protezione dei dati personali e tutela alla persona nell'ambito della relazione lavorativa viene riconosciuta formalmente anche nel *Regolamento generale sulla protezione dei dati personali*. Nel nuovo "ordinamento europeo della *privacy*" si abrogano adempimenti formali, si rimodulano quelli di tutela sostanziale prescrivendo un nuovo modo di concepire la protezione dei dati personali in cui viene fortemente responsabilizzato il Titolare del trattamento. E, per quanto a noi qui interessa, si affida a ciascuno Stato membro il compito di prevedere, tramite leggi o contratti collettivi, discipline più specifiche per assicurare la protezione dei diritti e delle libertà con riferimento al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (art. 88, co. 1, Reg. UE n. 2016/679).

Nell'analisi che segue si esaminerà l'impianto delle disposizioni del Regolamento evidenziando il loro impatto giuslavoristico. Si analizzeranno le nuove norme a tutela della riservatezza che si limitano a puntualizzare principi già contenuti nella previgente disciplina e quelle che "rivoluzionano" il sistema di protezione della persona anche nel "contesto occupazionale" imponendo un cambiamento di prospettiva e di organizzazione aziendale.

2. La graduale "sostituzione" della direttiva n. 95/46/CE con il Regolamento UE n. 2016/679

Si è detto che il *Regolamento generale sulla protezione dei dati personali*, entrato in vigore lo scorso 24 maggio 2016, è destinato ad abrogare la previgente disciplina contenuta nella direttiva (art. 99, Reg. UE n. 2016/679) ([8]). Nella iniziale proposta di Regolamento formulata dalla Commissione Europea si intendeva perseguire l'obiettivo di dare nuovi strumenti di tutela ai diritti fondamentali dell'Unione alla protezione dei dati personali e al rispetto della

([7]) Osservano le difficoltà di comprensione del "perimetro normativo" dei limiti all'utilizzabilità dei dati M.T. Carinci, *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D lgs. 151/2015): spunti per un dibattito*, LLI, 2016, vol. 2, no 1, § 2; si rinvia inoltre alle puntuali osservazioni di I. Alvino, LLI, 2016, vol. 2, no 1, § 1, 10.

([8]) Nelle disposizioni finali si legge che solo a far data dal 2018, le norme contenute nella direttiva madre n.95/46/CE risulteranno abrogate e i riferimenti alla direttiva madre si intenderanno come riferiti al Regolamento stesso, lasciando inalterate le previsioni della direttiva cd. figlia (direttiva n.2002/58/CE cfr. art.94-95, Reg. UE n.2016/679).

vita privata ([9]). Ciò è stato realizzato nell'ambito di una faticosa procedura di co-decisione tra Parlamento Europeo, Consiglio e Commissione ([10]): il testo definitivo del Regolamento *generale sulla protezione dei dati* modifica le fonti derivate dell'ordinamento europeo sulla materia ([11]) secondo le indicazioni della Corte di Giustizia Europea (CGE) ([12]) e della Corte Europea dei Diritti dell'Uomo (CEDU) ([13]). Le modifiche all'*acquis* comunitario entrate in vigore lo scorso 24 maggio sono dotate di impatto diretto negli ordinamenti degli Stati membri, fatti salvi margini di flessibilità per le legislazioni nazionali su specifiche disposizioni di attuazione ([14]).

A una prima lettura del Regolamento UE n. 2016/679 emerge che l'impianto normativo a tutela della protezione dei dati personali presenta una discreta ampiezza e maggiore complessità rispetto alla disciplina contenuta nella direttiva madre n. 95/46/CE. Del resto le norme Regolamentari UE sono disposizioni di immediata applicazione negli ordinamenti degli Stati membri la cui finalità è quella di regolare una materia e non individuarne i requisiti minimi per un'armonizzazione come quelle proprie delle Direttive ([15]).

L'operazione volta alla "sostituzione" di una Direttiva con un Regolamento terrà gli interpreti impegnati a lungo: solo nel 2018 le disposizioni italiane di recepimento della direttiva n. 95/46/CE contenute nel d.lgs. n. 196/2003 saranno private di fondamento e dovranno essere disapplicate qualora in contrasto con le previsioni del *Regolamento generale sulla*

([9]) Cfr. art.7 e 8 Carta dei Diritti dell'Unione Europea oggi parte del Trattato di Lisbona; art.8 CEDU Convenzione Europea per la salvaguardia dei Diritti dell'Uomo e le Libertà fondamentali; art. 16 TFUE.

([10]) Le norme del Trattato attinenti all'iter procedurale seguito sono gli artt. 288, 289 e 294 TFUE Trattato sul Funzionamento dell'Unione Europea)

([11]) Ci si riferisce alla Direttiva madre n. 95/46/CE e alle direttive cd. figlie n. 2002/58/CE e n. 2009/136/CE.

([12]) Sull'annullamento della direttiva in materia di conservazione dei dati (cd. *data retention*) per il contrasto con le previsioni della Carta dei Diritti fondamentali dell'Unione CGCE 8 aprile 2014, cause riunite C-293/12 e C-594/12, *Digital Right Ireland e Seitlinger* et a.; sul diritto all'oblio CGCE 13 maggio 2014, C-131/12, *Google inc e Google Spain c. Agencia Española de Protección de Datos (AEPD) e Mario Costeja Gonzales;* sull'individuazione del diritto applicabile, nonché sulla competenza dell'autorità di controllo designata ad esercitare il potere sanzionatorio ai sensi della direttiva n. 95/46/CE CGCE 1 ottobre 2015, Causa C-230/14, Weltimmo s. r. o./Nemzeti Adatvédelmi és Információszabadság Hatóság. In dottrina cfr. O. Pollicino, *Interpretazione o manipolazione? La Corte di Giustizia definisce un nuovo diritto alla privacy digitale*, in Federalismi.it Focus TMT 24 novembre 2014 n. 3/2014 consultabile in http://www.federalismi.it/document/25112014121445.pdf

([13]) Corte Europea dei Dritti dell'Uomo, 12 gennaio 2016, C.61496/08, Barbulescuc. Romania consultabile sul sito http://www.echr.coe.int

([14]) Vedi F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino Giappichelli, 2016, 34-35

([15]) Cfr. F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, op. cit.

protezione dei dati personali ([16]). Nel biennio di "transizione" le previsioni del Regolamento conviveranno con quelle della direttiva madre e, della disciplina nazionale di recepimento (d.lgs. n. 196/2003) talvolta puntualizzandone i contenuti, talaltra sostituendole ma solo nel maggio del 2018. E ciò anche nel particolare ambito della tutela della riservatezza nel contesto delle relazioni giuslavoristiche, in cui come vedremo si attribuiscono ai legislatori nazionali importanti spazi flessibilità.

Nell'analisi del Regolamento che qui si intende proporre si esaminerà quanto previsto nel Regolamento UE n. 2016/679 confrontando con quanto codificato nella direttiva n. 95/46/CE. In attesa della ulteriore riforma del *corpus* normativo *in materia di protezione dei dati personali* che attende i settori della polizia, giustizia e sicurezza ([17]), l'obiettivo è quello di stabilire quali principi e dettami trovino conferma e quali invece presentino profili di novità, dedicando particolare attenzione alla protezione della riservatezza nel contesto delle relazioni giuslavoristiche.

3. Il nuovo campo di applicazione territoriale e materiale

Il Regolamento UE n. 2016/679 si occupa di disciplinare il trattamento dei dati personali, nonché la loro circolazione nel rispetto del diritto alla protezione dei dati considerato come diritto e libertà fondamentale anche perseguendo scelte di extraterritorialità per garantire la tutela dei propri cittadini.

3.1. La puntualizzazione di principi già noti nel campo di applicazione cd. materiale

Venendo a una disamina precisa di quanto contenuto nel Regolamento UE n. 2016/679 si evidenzia come le disposizioni con cui si puntualizzano principi già noti, sono in ogni caso dotate di rilevante impatto. Si tratta di norme che adeguano la disciplina dettagliando in maniera importante termini talora già utilizzati nella direttiva madre n. 95/46/CE e nel Codice della *Privacy*

([16]) Si tratta di una tecnica normativa spesso utilizzata nell'Unione, nonostante la diversa natura delle fonti comunitarie cfr. da ultimo al Regolamento (UE) n. 2016/425 che disciplina la conformità dei dispositivi di protezione individuale (DPI), nonché gli obblighi di Fabbricanti, Mandatari, Importatori e Distributori di DPI che ha abrogato la Direttiva n.89/686/CEE

([17]) Si tratta dell'ulteriore parte del cd. "pacchetto protezione dati" presentato dalla Commissione nel gennaio 2010. Vedi F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Torino Giappichelli, 2016, 34-35

italiano, altre volte assenti nell'una o nell'altra fonte ma coerenti con i principi portanti.

Quanto al campo di applicazione cd. materiale della disciplina a protezione dei dati personali si segnala l'ampio aggiornamento della nozione di "dato personale" contenuta nel Regolamento UE n. 2016/679, che si richiama quella contenuta nell'art.2, lett. a) Dir. n. 95/46/CE già ispirata alla precedente codificata nell'art.2, lett. a) Convenzione n. 108/1981 ([18]), recependo i risultati delle riflessioni del Gruppo di lavoro dell'art. 29 ([19]). Nel Regolamento UE n. 2016/679 il "dato personale" contiene anche un identificativo *on line* e rinvia a una più attenta definizione di identità ([20]). In continuità con la direttiva n. 95/46/CE, l'identificabilità dell'interessato alla luce di criteri oggettivi continua ad essere presupposto per la distinzione tra informazione anonima e "dato personale" anche nel Regolamento UE n. 2016/679 ([21]). Il "dato personale" rileva ai fini del Regolamento UE n. 2016/679 se contiene una "qualsiasi informazione" (*id est* informazioni di tipo oggettivo come un dato biometrico; di tipo soggettivo come una opinione, una tendenza, una valutazione) che abbia con una persona fisica "identificata o identificabile" nell'ambito di un gruppo più esteso una relazione di "contenuto" (ossia riguardi una persona) di "finalità" (ossia attenga alla persona e sia finalizzata a valutarla) di "risultato" (ossia possa avere un impatto rispetto alla persona a cui si riferisce) (art.4, n. 1, Reg. UE n. 2016/679). Presentano carattere di novità, ma sempre in continuità con quanto previsto nella *Direttiva n.95/46/CE*, le nozioni di "dato genetico" e "dato biometrico" (art. 4, n. 10-11, Reg. UE n.2016/679) ([22]). L'operazione di

([18]) La Convenzione n. 108 del Consiglio d'Europa, adottata a Strasburgo il 28 gennaio 1981 tratta la protezione dei dati delle persone fisiche rispetto all'elaborazione automatizzata ed elenca alcuni principi fondamentali sulla qualità e sicurezza delle informazioni personali e sui trattamenti cfr. P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffré, 2002, 49 e ss.).

([19]) L'ampia definizione recepisce le indicazioni del parere n.4/2007 del "Gruppo di lavoro dell'art.29" sulla nozione di dato personale adottato il 20 giugno 2007 WP 29 n.136.

([20]) Cfr. art.4, n.1, Reg. UE n. 2016/679 secondo cui per dato personale si intende "*qualsiasi informazione concernente una persona fisica identificata o identificabile, l'"interessato"; si considera identificabile la persona che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo* on line *o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale".*

([21]) Nel Regolamento si recepisce quanto elaborato dal "Gruppo di Lavoro dell'art.29" prescrivendo il riferimento a due fattori cd. oggettivi come i costi e il tempo necessario all'individuazione. Cfr. Reg. UE n. 2016/679 considerando (23). In dottrina sull'anonimato si veda per tutti G. Finocchiaro (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in Galgano (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, XLVIII, Cedam, 2008

([22]) Cfr. Reg. UE n. 2016/679 considerando (…) (25 bis) È opportuno che per dati genetici si intendano i dati personali relativi alle caratteristiche genetiche di una persona fisica che siano ereditarie o acquisite, ottenuti dall'analisi di un campione biologico della persona in questione, in particolare dall'analisi dei cromosomi, dell'acido desossiribonucleico (DNA) e dell'acido ribonucleico (RNA) ovvero dall'analisi di qualsiasi altro elemento che consenta di ottenere informazioni equivalenti.

puntualizzazione e aggiornamento delle definizioni contenute nella Direttiva madre n. 95/46/CE viene realizzata altresì per la nozione di "trattamento" ([23]) che viene ampliata e aggiornata con la forma particolarmente invasiva della cd. Profilazione ([24]). Ulteriore novità si segnala nella definizione di "pseudonimizzazione" (art.4, Reg. UE n. 2016/679).

3.2. …. e la loro portata nelle relazioni giuslavoristiche.

Nella prospettiva di un'analisi della portata giuslavoristica delle novità, si evidenzia come qualunque dato e/o informazione attinente a un lavoratore/collaboratore identificabile direttamente o indirettamente nonché qualunque valutazione riferibile al suo comportamento in costanza di rapporto lavorativo risulterà compresa nella nozione di "dato personale" e continuerà a essere meritevole di tutela anche nel Regolamento UE n. 2016/679. Per quanto a noi qui interessa, la protezione non riguarda solo le informazioni raccolte in occasione dell'assunzione e/o della gestione del rapporto lavorativo come dati sanitari, affiliazioni sindacali, dati giudiziari (si pensi alla disciplina in tema di assunzioni di personale impiegato in attività a contatto con minori d.lgs. 4 marzo 2014, n. 39, attuazione della dir. n. 2011/93/EU) bensì anche le informazioni lasciate durante le navigazioni sul *web* tramite strumenti elettronici forniti dall'azienda, le informazioni connesse all'uso delle *mail* nonché le informazioni salvate in profili personali dei *social network* e riferibili al dipendente (*Facebook; twitter; istagram; linkedin*).

Pacificamente nella nozione di "trattamento" rientrano non solo tutte le operazioni del datore di lavoro di gestione del rapporto lavorativo come la raccolta, la memorizzazione, l'organizzazione, la conservazione dei dati nonché la loro estrazione, consultazione. Ma altresì le operazioni che

([23]) La nozione di trattamento include "*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 memorizzazione, 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*" (art.4, n.3 Reg. UE n. 2016/679).

([24]) La profilazione è quella "*forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti nella misura in cui ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona*" (art.4, n.3 bis Reg. UE n.2016/679). Cfr. altresì i considerando 21, 48, 51, 57, 59, 59 bis, 71)Reg. UE n. 2016/679 nonché il considerando (58) (…) la "profilazione", che consiste in una forma di trattamento automatizzato dei dati personali che valuta aspetti personali concernenti una persona fisica, in particolare al fine di analizzare o prevedere aspetti riguardanti il rendimento professionale, la situazione economica, la salute, le preferenze o gli interessi personali, l'affidabilità o il comportamento, l'ubicazione o gli spostamenti nella misura in cui ciò produca effetti giuridici che la riguardano o incida in modo analogo significativamente sulla sua persona.

comportino la comunicazione, diffusione o qualunque altra messa a disposizione dei dati personali rilevanti nei casi di distacco o di somministrazione del personale. Particolari limiti e divieti sono previsti qualora si trattino in modo automatizzato dati riferibili al dipendente concernenti la persona fisica al fine di analizzarne o prevederne aspetti riguardanti ad esempio il rendimento professionale, l'affidabilità nello svolgimento delle mansioni (cd. profilazione) (art.21-22 Reg. UE n. 2016/679). La stessa cancellazione o distruzione del dato personale rientra nella nozione di trattamento, con inevitabili riflessi sui comportamenti dell'azienda in occasione della conclusione del rapporto in relazione alla gestione della distruzione dei dati personali inevitabilmente contenuti sui *personal computer* e *devices* aziendali ove concessi in dotazione al lavoratore.

La tutela della protezione dei dati personali del dipendente, che potrà essere speciale e derogatoria rispetto a quella generale, definirà quindi nuovi limiti esterni al potere datoriale di controllo e disciplinare.

3.3. Le novità che ci attendono nel campo di applicazione territoriale e materiale.

Tra le novità più significative del *Regolamento* che stravolgono la disciplina contenuta nella Direttiva n.95/46/CE, si segnala quella inserita nel Capo I e attinente all'estensione del campo di applicazione territoriale della disciplina sulla protezione dei dati personali. Si tratta della codificazione della migliore elaborazione giurisprudenziale della Corte di Giustizia Europea ([25]) e degli approfondimenti svolti dal "*Gruppo di lavoro articolo 29*" ([26]). La novità comporterà l'estensione della protezione dei dati personali a tutti coloro che si trovano nell'Unione indipendentemente dal luogo in cui sia effettuato il trattamenti dei dati personali ([27]). Il principio consentirà una tutela anche ai

([25]) CGCE 13 maggio 2014, *Google inc e Google Spain c. Agencia Española de Protección de Datos e Mario Costeja Gonzales* e parere n. 8/2010 così F. Pizzetti, *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, cit., 80.

([26]) Il "Gruppo dell'articolo 29" è un organismo con funzioni consultive composto da un rappresentante dell'Autorità Nazionali di controllo designato da ciascuno Stato membro e da un rappresentante dell'Autorità per le Istituzioni e gli organismi comunitari nonché da un rappresentante della Commissione. Sulla funzione e natura giuridica delle ricerche del "Gruppo dell'articolo 29" cfr. P. Pallaro, *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Milano Giuffré, 2002, 139 e ss.

([27]) Cfr. Reg. UE n. 2016/679 considerando (21) È opportuno che anche il trattamento dei dati personali degli interessati che si trovano nell'Unione ad opera di un responsabile del trattamento o di un incaricato del trattamento non stabilito nell'Unione sia soggetto al presente regolamento quando è riferito al controllo del comportamento di detti interessati, quest'ultimo inteso all'interno dell'Unione europea. Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le operazioni che questi esegue su Internet sono tracciate,

trattamenti effettuati da Titolari non stabiliti nell'Unione Europea se avrà ad oggetto dati personali di interessati che si "trovano" (anche virtualmente) nell'Unione e riguarderà l'offerta di beni o servizi e/o con monitoraggio dei loro comportamenti all'interno dell'Unione (art.3 Reg. UE n.2016/679). Analogamente finalizzate a una maggior protezione dei dati e dell'identità personali rispetto al monitoraggio di comportamenti tenuti all'interno dell'Unione Europea si segnala l'introduzione di nuove definizioni in tema di "stabilimento principale" del Titolare e del Responsabile del trattamento ([28]) e in tema di "impresa" e di "gruppo imprenditoriale" costituito da impresa controllante e controllate ([29]). Ma altresì la previsione delle "norme vincolanti d'impresa" (*Binding Corporate Rules*) ossia delle politiche in materia di protezione dei dati personali applicate dal Titolare o dal Responsabile stabilito nel territorio di uno Stato membro dell'Unione o altresì delle politiche in materia di trasferimento di dati personali nell'ambito di gruppi societari a imprese situate in Paesi terzi ([30]). Le norme del Regolamento avranno una sostanziale "extraterritorialità" dell'efficacia del Regolamento: il Regolamento troverà applicazione se il soggetto a cui si riferiscono i dati "si trovi" realmente o virtualmente nel territorio europeo ovvero se il Titolare o il Responsabile del trattamento è stabilito nell'Unione (anche se il trattamento venga effettuato all'esterno dell'Unione stessa).

Quanto al campo di applicazione materiale si anticipa qui che ci attende una riduzione di protezione. Nel Regolamento UE n. 2016/679 il "dato personale" risulta oggetto di tutela unicamente nella misura in cui riguardi le sole persone fisiche: non si rinviene più la previsione contenuta nella *Direttiva Madre n.95/46/CE* che consentiva a ciascuno Stato di introdurre una disciplina nazionale che estendesse la tutela della riservatezza anche alle persone giuridiche, sfruttata dall'Italia ma fino al 2012 (cfr. art.40, d. l. n. 201/2011 conv. in l. n. 214/2011 che abroga l'estensione della tutela per le persone

compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati volte alla profilazione dell'utente, in particolare per prendere decisioni che lo riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali.

([28]) Cfr. Reg. UE n. 2016/679 considerando (27).

([29]) Un gruppo societario o un gruppo di imprese che svolge un'attività economica comune dovrebbe poter applicare le norme vincolanti d'impresa approvate per i trasferimenti internazionali dall'Unione agli organismi dello stesso gruppo societario o gruppo d'imprese, purché tali norme contemplino tutti i principi fondamentali e diritti azionabili che costituiscano adeguate garanzie per i trasferimenti o categorie di trasferimenti di dati personali.

([30]) Cfr. artt.43-44-45, Reg. UE n. 2016/679 sulle *Binding Corporate Rules* (BCR) e sulle clausole contrattuali standard M. Soffientini (a cura di), *Privacy. Protezione e trattamento dei dati*, Ipsoa, 2016, 293.

giuridiche nell'ambito delle misure di semplificazione delle imprese) ([31]). Né si rinvengono nel Regolamento UE n. 2016/679 le specifiche nozioni di dato personale "sensibile" o dato personale "giudiziario": negli artt.9 e 10 tali dati si individuano in maniera generale e si introduce una nuova definizione dei "dati relativi alla salute".

Tuttavia, un vero mutamento di prospettiva nel cd. campo di applicazione materiale si rinviene nell'assetto delle responsabilità delineato nel Regolamento UE n. 2016/679. Nella parte iniziale del Regolamento emerge come persistano le posizioni di garanzia del Titolare del trattamento su cui gravano le responsabilità fondamentali a cui peraltro si affiancano nuove figure, espressione di nuovi ruoli e funzioni organizzative.

Il Titolare del trattamento (*Controller*) rimane la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali (art.4, n.7) Reg. UE n. 2016/679). Persiste la presenza, che diviene anzi obbligatoria, del Responsabile (*Processor*) la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che tratta dati personali per conto del Titolare del trattamento tramite nomina documentata per iscritto e assoggettamento al potere di controllo e disciplinare (art.4, n.8) Reg. UE n. 2016/679). Spariscono invece i riferimenti specifici all'Incaricato del trattamento presenti nel d.lgs. n. 196/2003, pur permanendo la facoltà del Titolare di nominare Terzi che operino sotto la sua diretta responsabilità o di quella del Responsabile e siano "persone autorizzate al trattamento" sia fisiche sia giuridiche ([32]).

Viene poi introdotta una figura totalmente nuova: il *Responsabile della protezione dei dati* (*Data Protection Officer*) professionista con elevate e particolari competenze che dovrà essere designato dal Titolare del trattamento per affiancarlo nella gestione della protezione dei dati personali in presenza di situazioni di particolare rischio (art. 37, Reg. n. 2016/679). La presenza di questo nuovo professionista, che diverrà obbligatoria nel 2018, si accompagna alle nuove previsioni che saranno analizzate più nel dettaglio nel prosieguo volte alla proceduralizzazione degli obblighi di protezione dei dati personali e

([31]) E. Bassoli, *La sicurezza dei sistemi informativi aziendali: norme protettive, oneri e misure minime obbligatorie*, in G. Cassano - G. Scorza - G. Vaciago, *Diritto dell'internet*, Cedam, 2013, 831 e ss.

([32]) Cfr. Reg. UE n. 2016/679 considerando (29). Osserva che nel Regolamento si omette la precisazione che il Terzo sia persona "fisica" consentendo un'interpretazione capace di includere anche le persone giuridiche A.C. Messina – N. Bernardi, *Privacy e Regolamento* Europeo, Ipsoa, 2016, 10. Riflette sulle criticità che deriveranno per la disciplina interna italiana a seguito della mancata previsione dell'incaricato del trattamento Ferri S., *Come gestire gli ex-incaricati del trattamento?*, in *Privacy News*, n.1, 2016, 53

alla promozione della consapevolezza su tutti i temi della *Privacy* nei diversi livelli aziendali anche grazie a obblighi informativi/formativi del personale (cfr. art.37 e considerando (30), Reg. n. 2016/679).

3.4. ... e il loro impatto nel contesto occupazionale.

Le descritte novità, come vedremo nel prosieguo, sono emblematiche di un nuovo approccio alla tutela della protezione dei dati personali. Nel Regolamento UE n. 2016/679 si abbandona lo schema dirigistico adottato nella Direttiva madre n. 95/46/CE che comportava precisi interventi del Garante in caso di trattamenti particolarmente "a rischio". Emblematico del mutamento organizzativo imposto dal Regolamento UE n. 2016/679 sarà l'affiancamento al Titolare di una figura professionalmente competente, dotata delle risorse e del potere di spesa per poter assolvere ai compiti assegnati (art.39 Reg. UE n. 2016/679). La forte responsabilizzazione del Titolare, rispetto alla protezione dei dati personali dei dipendenti, imporrà una condivisione della nuova normativa a tutti i livelli, con l'acquisizione da parte dei dipendenti di nuove consapevolezze e aspettative di tutela.

Nel Regolamento si adotta un nuovo approccio sistemico in cui si promuovono analisi e valutazioni preventive sui possibili rischi per la sicurezza dei dati, oltre all'adozione di procedure organizzative/accordi infrasocietari conosciuti o conoscibili anche agli interessati per le implicazioni sulle modalità di esercizio dei diritti di accesso. La modifica di prospettiva nella protezione dei dati personali si pone in linea con una valorizzazione di modelli organizzativi adottata da ultimo in tema di responsabilità amministrativa delle imprese (d.lgs. n. 231/2001). Un cambiamento che imporrà di "ripensare" la tutela dei dati nelle relazioni giuslavoristiche nel solco di quanto è avvenuto nella disciplina a tutela della sicurezza e igiene sul lavoro con la proceduralizzazione degli obblighi e l'imposizione di un'organizzazione aziendale (dir. n. 89/389 e d.lgs. n. 626/1994). Particolare attenzione potrà essere dedicata dai singoli Stati membri alla declinazione delle nuove norme in considerazione delle diverse categorie di aziende secondo le nozioni di micro, piccola e media impresa contenute nell'art. 2 Allegato Raccomandazione 2003/361/CE della Commissione ([33]) che considerano soglie occupazionali (10-50-250 persone) e di bilancio annuo (2-10-50 milioni di euro) ([34]).

([33]) Cfr. Reg. UE n. 2016/679 considerando (13) (…) "Per tener conto della specifica situazione delle micro, piccole e medie imprese, il presente regolamento prevede una deroga per le organizzazioni che hanno meno di 250 dipendenti per quanto riguarda la conservazione delle registrazioni. Inoltre, le istituzioni e gli organi dell'Unione e gli Stati membri e le loro autorità di controllo sono invitati a considerare le esigenze specifiche delle micro, piccole e medie imprese

L'estensione del campo di applicazione territoriale risulterà poi di notevole importanza per i lavoratori di società appartenenti a gruppi societari multinazionali. Essa consentirà una protezione della riservatezza dei dipendenti che lavorano o vivono nell'Unione, anche nelle ipotesi in cui Titolari e Responsabili del trattamento non avranno sedi legali, né sedi secondarie nell'Unione Europea ([35]). Non sarà più ammissibile escludere l'applicabilità della disciplina a tutela della *Privacy* qualora il trattamento dei dati del dipendente sia effettuato da altra società consociata e avente sede fuori dall'Unione Europea. Il Regolamento troverà applicazione anche ai "*gruppi di imprese*" ([36]) e qualora le attività di trattamento incideranno o potranno incidere su più interessati in diversi Stati membri sarà possibile individuare l'Autorità Garante capofila nell'Autorità Garante dello Stato nel quale è presente lo stabilimento principale del titolare al trattamento e/o lo stabilimento unico dell'incaricato al trattamento ha lo stabilimento unico (cd. *one stop shop*) ([37]). Pertanto i "gruppi di imprese" e in ogni caso le società che invieranno in distacco i propri dipendenti per garantire un "livello adeguato" di protezione per la circolazione dei dati personali dei dipendenti (art. 44, Reg. UE n. 2016/679) saranno indotti a prevedere Norme Vincolanti d'Impresa (*Binding*

---

nell'applicare il presente regolamento. La nozione di micro, piccola e media impresa dovrebbe ispirarsi all'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione"

([34]) Art.2 Allegato Raccomandazione 2003/361/CE della Commissione rubricato *Effettivi e soglie finanziarie che definiscono le categorie di imprese* così recita "co. 1. La categoria delle microimprese delle piccole imprese e delle medie imprese (PMI) è costituita da imprese che occupano meno di *250 persone*, il cui fatturato annuo non supera i *50 milioni di EUR* oppure il cui totale di bilancio annuo non supera i 43 milioni di EUR. Co. 2. Nella categoria delle PMI si definisce piccola impresa un'impresa che occupa meno di *50 persone* e realizza un fatturato annuo o un totale di bilancio annuo non superiori a *10 milioni di EUR*. Co. 3. Nella categoria delle PMI si definisce microimpresa un'impresa che occupa meno di *10 persone* e realizza un fatturato annuo oppure un totale di bilancio annuo non superiori a *2 milioni di EUR*."

([35]) Resta escluso dal campo di applicazione il trasferimento dei dati personali dall'Unione Europea verso gli Stati Uniti materia oggetto del recente accordo del 02 febbraio 2016 denominato EU-US Privacy Shield. M. Soffientini, *Dal* Safe Harbor *al* Privacy shield*: la svolta dell'Unione Europea*, in Privacy News, n.1/2016, 26.

([36]) I gruppi di imprese vengono definiti come "*persone fisiche o giuridiche, indipendentemente dalla forma giuridica rivestita, che esercitano un'attività economica, comprendente le società di persone o le associazioni che esercitano regolarmente un'attività economica*" all'interno di un "*gruppo costituito da un'impresa controllante e dalle imprese da questa controllate*" e delle "*norme vincolanti d'impresa*" ossia "*le politiche in materia di protezione dei dati personali applicate da un responsabile del trattamento o incaricato del trattamento stabilito nel territorio di uno Stato membro dell'Unione"* (art. 4, nn.15-16-17, Reg. UE n. 2016/679). Cfr. altresì Reg. UE n. 2016/679 considerando (28) e considerando (38 bis).

([37]) Unica eccezione sarà quella dei trattamenti effettuati da autorità pubbliche oppure da organismi privati che agiscono sulla base dell'art.6, par.1, lett.c) lett.e), Reg. n.2016/679 Cfr. Reg. UE n. 2016/679 considerando (97-98). Specifiche norme disciplinano poi i rapporti tra le diverse Autorità Garanti Nazionali e artt.54 bis, 55, 56 Reg. UE n. 2016/679.

Corporate Rules) ([38]) (art. 47 Reg. UE n. 2016/679) o a stipulare accordi commerciali secondo quanto indicato nelle Decisioni della Commissione Europea (*Standard Contractual Clauses*) ([39]).

4. Il potenziamento del diritto alla protezione dei dati personali

All'espansione del campo di applicazione sostanziale con l'ampliamento del significato semantico della nozione di "dato personale" e "trattamento" nel Regolamento UE n. 2016/679 si puntualizzano prescrizioni già codificate nella previgente disciplina per i Titolati del trattamento con riconoscimento dei diritti all'autodeterminazione informativa e al controllo sui trattamenti svolti sui dati personali.

L'effetto complessivo sarà un generale potenziamento dei diritti della personalità. Nella *Direttiva madre n.95/46*/CE il Capo II includeva le condizioni generali di trattamento: i principi relativi alla qualità dei dati e alla legittimazione del trattamento dei dati, le categorie particolari di trattamenti; l'informazione della persona interessata, il diritto di accesso ai dati da parte della persona interessata, deroghe e restrizioni; diritto di opposizione della persona interessata; riservatezza e sicurezza dei trattamenti; notificazione. Nel Regolamento UE n.2016/679 la disciplina è organizzata diversamente con innovazioni significative ma non in contrasto con i principi già riconosciuti: il Capo II è dedicato ai Principi applicabili al trattamento dei dati personali mentre il Capo III è dedicato ai Diritti dell'interessato (Trasparenza e modalità di trattamento; Informazioni e accesso ai dati; Rettifica e cancellazione).

L'impianto dei diritti dei *data subjects* viene confermato e continua a non trovare applicazione per le informazioni anonime, vale a dire per quelle informazioni che non si riferiscono a una persona fisica identificata o identificabile (considerando 26 e art.4, Reg. UE n. 2016/679). Nel Regolamento UE n. 2016/679 trovano inoltre conferma i principi posti a fondamento della liceità del trattamento. Il consenso dell'interessato continua a rappresentare la principale condizione di liceità del trattamento, salvo deroghe (art.7, Reg. UE n. 2016/679). Si vieta il trattamento dei dati che, nella

([38]) Per le BCR per i gruppi d'imprese infra europei si vedano i lavori del Gruppo ex art.29 *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules"* cfr. http://www.garanteprivacy.it/documents/10160/10704/ARTICLE+29+-+WP107

([39]) Si tratta delle Decisioni della Commissione Europea n.2004/915/CE cfr. http://www.garanteprivacy.it/documents/10160/10704/1151941 e della Decisione n. 2010/87/UE cfr. 111http://www.garanteprivacy.it/documents/10160/10704/1767001.

direttiva madre n.95/46/CE erano definiti i dati "sensibili" (artt.5-6, Reg. UE n. 2016/679), salvo casi specifici elencati nell'art.9, Reg. UE n.2016/679. In ogni caso gli Stati membri potranno mantenere o introdurre ulteriori condizioni e/o limitazioni nel definire la liceità del trattamento di dati genetici, biometrici o relativi alla salute (art. 9, co. 4, Reg. UE n. 2016/679). In caso di trattamento dei dati relativi a condanne penali e reati o connesse a misure di sicurezza trova conferma il principio della necessità che il trattamento avvenga sotto il controllo dell'autorità pubblica o comunque ove autorizzato dal diritto dell'Unione Europea o degli Stati membri che preveda garanzie appropriate per gli interessati (art.10, Reg. UE n. 2016/679).

4.1. La puntualizzazione di principi già noti: i nuovi requisiti dell'informativa e il diritto di accesso ai propri dati

Nel Regolamento UE n. 2016/679 si continuano a prevedere una serie di presupposti di liceità del trattamento tra cui il consenso (artt. 5-11 Reg. n.2016/679) ([40]). Viene inoltre riservato particolare interesse ai criteri da rispettare per la redazione delle informative, anche finalizzate a ottenere un valido consenso "informato" e "consapevole" (art.12, Reg. UE n. 2016/679). Puntualità, efficacia, intellegibilità e comprensibilità delle informazioni fornite sulle modalità di trattamento dei dati sono requisiti fondamentali che potranno essere raggiunti anche grazie all'utilizzo di moduli, schemi e disegni idonei a informare e diffondere le notizie sulla correttezza dei trattamenti da parte dei Responsabili (artt.14 e 14bis Reg. UE n. 2016/679). Particolari contenuti dovrà avere l'informativa finalizzata a ottenere il consenso per la cd. profilazione (trattamento facilitato dalla diffusione dei *big data*, particolarmente invasivo e sempre considerato vietato ove comporti una discriminazione) (artt.21-23, Reg. UE n. 2016/679).

La funzione essenziale dell'informativa, già riconosciuta pacificamente nel quadro complessivo del sistema generale di tutele predisposto dalla Direttiva madre n. 95/46 ([41]) e anche dal Codice della *Privacy* italiano (art. 13, d.lgs. n. 196/2003), viene valorizzata e potenziata nel Regolamento UE n. 2016/679. Nel nuovo contesto normativo il diritto a ricevere un'adeguata

([40]) Eccezioni alla necessità dell'esistenza di un valido consenso dell'interessato sono costituite dalla necessità di eseguire un contratto o misure precontrattuali; dall'esistenza di un obbligo legale; dalla necessità di salvaguardia di interessi vitali dell'interessato o di altra persona fisica; dall'esercizio di compiti di interesse pubblico; dalla presenza di un legittimo interesse del titolare del trattamento a condizione che non prevalga su diritti e libertà fondamentali dell'interessato specie se minore.

([41]) A. Stizia, *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, 2013, 158

informativa acquisisce autonoma rilevanza (rispetto all'esigenza di ottenere il consenso al trattamento da parte dell'interessato) (artt. 12, Reg. UE n. 2016/679). I contenuti dell'informativa vengono inoltre distinti a seconda che i dati siano raccolti presso l'interessato oppure no, con la previsione di informazioni aggiuntive in questo secondo caso (artt.13 e 14, Reg. UE n. 2016/679). I dati di contatto del Responsabile della protezione dei dati personali (*Data Protection Officer*); la base giuridica del trattamento a corredo delle finalità del trattamento; la specificazione di quali siano i legittimi interessi perseguiti dal Titolare del trattamento qualora il trattamento di basi sulla necessità di perseguire un legittimo interesse del titolare o di terzi; l'ambito del trasferimento all'estero dei dati; il periodo di conservazione dei dati; l'esistenza del diritto alla portabilità dei dati; il diritto a revocare il consenso in ogni momento; il diritto di proporre reclamo al Garante; l'esistenza di un processo decisionale automatizzato; la fonte da cui hanno origine i dati personali; le categorie di dati personali oggetto del trattamento (art. 14, Reg. UE n. 2016/679).

L'attenzione riservata alle informazioni da fornire contribuirà inoltre a rendere effettivo e a potenziare il "diritto di accesso" al fascicolo contenente i propri dati personali, già previsto nella Direttiva madre n. 95/46/CE, codificato nell'art.7 d.lgs. n. 196/2003 e ora declinato con maggior puntualità nell'art. 15, Reg. UE n. 2016/679. Nelle nuove norme, qualora l'interessato eserciti il diritto di accesso al proprio fascicolo il Titolare sarà tenuto a informare l'interessato entro un mese dal ricevimento della richiesta ei n caso di ritardo il Titolare sarà obbligato a darne giustificazione precisandone i motivi e precisando la facoltà di proporre reclamo all'Autorità Garante e/o ricorso all'autorità giudiziaria (art. 12 e art.15 Reg. UE n. 2016/679).

4.2. … e la loro portata nelle relazioni giuslavoristiche

Il combinato disposto delle norme a garanzia del diritto all'informativa e al diritto di accesso ai dati personali detenuti dal datore di lavoro e riferiti all'intera carriera professionale di un dipendente è destinato a rafforzare la posizione del lavoratore nella relazione contrattuale giuslavoristica. La corretta e trasparente informazione in merito ai controlli e alla tipologia dei "dati personali" raccolti e detenuti dal datore di lavoro (si pensi alle valutazioni sull'operato e/o alle informazioni sui comportamenti del dipendente anche desumibili da navigazioni sul *web* e/o vita "virtuale" sui *social network*) potrà consentire al dipendente un pieno esercizio dei propri diritti.

Nel Regolamento n. 2016/679 l'obbligo di informativa acquista una autonoma rilevanza, anche nelle fattispecie in cui non è necessario ottenere il consenso per procedere al trattamento. Si tratta di un capovolgimento della tradizionale prospettiva della disciplina della *Privacy* in cui l'informativa era prevista solo qualora il trattamento fosse legittimo in presenza del consenso dell'interessato ([42]).

L'interessato avrà diritto a essere informato dell'esistenza di un qualsivoglia trattamento da parte del datore di lavoro, delle sua finalità, dell'esistenza di una eventuale profilazione e delle conseguenze di essa anche ai fini della valutazione della persona in termini di rendimento e/o altro. Si tratta di informazioni che dovranno essere fornite in combinazione con icone standardizzate per consentire un'agevole intelligibilità del quadro d'insieme del trattamento stesso.

Le disposizioni che prescrivono precisi contenuti di "adeguatezza" delle informative avranno un impatto nel contesto delle relazioni giuslavoristiche. Le aziende saranno spinte a "ripensare" alle informative da consegnare ai lavoratori sulle modalità d'uso degli strumenti e sull'effettuazione dei controlli ([43]).

Significativo per il dipendente risulterà altresì il rinvigorimento del diritto di accesso ai "dati personali" (incluse le relazioni predisposte dal datore di lavoro e inserite nel fascicolo personale in quanto contenenti notizie, informazioni o elementi idonei a fornire un contributo aggiuntivo di conoscenza sul lavoratore).

Pare opportuno ricordare che nel nostro ordinamento il diritto di accesso al fascicolo personale detenuto dal datore di lavoro pure codificato nel Codice della *Privacy* sin'ora è stato oggetto di interesse prevalentemente nel rapporto di lavoro di pubblico impiego. Inizialmente riconosciuto dalla giurisprudenza italiana come mero diritto-civico di accesso ai procedimenti amministrativi ai sensi dell'art. 24, legge n. 241/1990 e del d.P.R. n. 184/2006 ([44]), nel rapporto di impiego privato l'attenzione a questi profili è stata meno

([42]) Si esprime nello stesso senso M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e dei trattamenti dei dati (del lavoratore),* cit., 27.

([43]) Sul punto M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e dei trattamenti dei dati (del lavoratore),* cit., 27.

([44]) Cfr. Consiglio di Stato, Sez. VI, 12 gennaio 2011 consultabile su http://www.ilsole24ore.com/pdf2010/SoleOnLine5/_Oggetti_Correlati/Documenti/Norme%20e%20Tributi/2011/05/guida-privacy/consiglio-di-stato-116-2011.pdf; T.A.R. Lazio-Roma, Sez. I quater, 10 marzo 2006, n.1862 ritiene che il dipendente sia titolare di una posizione giuridicamente tutelata in relazione alla conoscenza degli atti contenuti nel suo fascicolo personale; T.A.R. Abruzzo - Pescara, sez. I, 18 ottobre 2007, n. 821 riconosce al pubblico dipendente la titolarità di una posizione giuridicamente tutelata in relazione alla conoscenza degli atti contenuti nel suo fascicolo personale,

intensa. Solo l'Autorità Garante della *Privacy* si era espressa sulla questione ripetutamente. Più volte aveva ribadito l'obbligo per le aziende di consentire e facilitare l'accesso del dipendente al complesso di tutti i dati personali presenti negli archivi aziendali e contenuti in atti diversi dalle schede identificative o anagrafiche del dipendente (quali i giudizi, le note di qualifica o i risultati degli esami di accertamento). Nei Provvedimenti l'Autorità aveva puntualizzato che qualora il dipendente non fosse riuscito a consultare le informazioni alle quali aveva diritto di accesso, avrebbero trovato applicazione le sanzioni penali previste dalla legge sulla *privacy*, nonché l'obbligo di risarcimento delle spese eventualmente sostenute dal collaboratore a causa dell'illecito contegno dell'azienda ([45]).

Solo da ultimo è stato considerato dalla Suprema Corte come vero e proprio diritto soggettivo del dipendente ad accedere al proprio fascicolo personale radicato nel contratto di lavoro ([46]). E recentemente la Cassazione ha confermato la fonte contrattuale del diritto soggettivo del lavoratore di accedere al proprio fascicolo personale ([47]). Secondo la Corte l'obbligo del datore di lavoro di consentire al dipendente pieno accesso a tutti i dati detenuti deriva dai generali obblighi di buona fede e correttezza che incombono sulle parti del rapporto di lavoro ai sensi degli artt.1175 e 1375 c.c.; inoltre trova conferma nelle disposizioni di molti contratti collettivi in cui si dispone l'obbligo per il datore di lavoro di conservare in apposito fascicolo, tutti gli atti e i documenti, prodotti dall'ente o dallo stesso dipendente, che attengono al percorso professionale, all'attività svolta e ai fatti più significativi che lo riguardano e il diritto per il dipendente di prendere visione liberamente degli atti e documenti inseriti nel proprio fascicolo personale ([48]).

Come approfondiremo oltre, resta inteso che i descritti rafforzamenti dei diritti della riservatezza dei dipendenti prescritti nelle nuove norme regolamentari potranno garantire una più effettiva protezione dei dati personali del dipendente a patto che si provveda a una puntuale regolamentazione anche delle conseguenze anche processuali

---

senza che ricorra la necessità per il medesimo di esternare espressamente la presenza di un concreto ed immediato interesse.

([45]) Cfr. Provvedimento dell'Autorità Garante della Privacy 27 dicembre 2001 [40987] http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/40987; Provvedimento dell'Autorità Garante della Privacy - Decisione del 10 luglio 2000

([46]) Così Cass. S.U. 4 febbraio 2014, n.2397 consultabile su http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20140205/snciv@sU0@a2014@n02397@tS.clean.pdf.

([47]) Cass. 7 aprile 2016, n. 6775

([48]) Cass. 7 aprile 2016, n. 6775

dell'inutilizzabilità per il datore di lavoro delle informazioni acquisite in violazione della disciplina della *privacy*.

4.3. I nuovi diritti di rettifica, all'oblio, alla portabilità dei dati

All'espansione del campo di applicazione territoriale/materiale e al nuovo approccio delle modalità di tutela della protezione dei dati riferibili a persone fisiche identificate o identificabili nel Regolamento UE n. 2016/679 si affiancano nuove prescrizioni per i Titolati del trattamento. L'effetto complessivo, quantomeno sulla carta, parrebbe quello di un generale potenziamento dei diritti della personalità.

Indiretto ma non meno importante sarà l'impatto della disposizione in cui si riconosce un "diritto di rettifica" ossia di modifica dei dati personali "senza ingiustificato ritardo" (art. 16, Reg. UE n. 2016/679), nonché della disposizione in cui, recependo la migliore elaborazione della Corte di Giustizia Europea ([49]), si codifica il "diritto all'oblio" ossia di veder cancellati o deindicizzati (eliminati dai motori di ricerca) dati personali dopo un determinato periodo di tempo, fatta salva l'esistenza di motivi legittimi di conservazione (ad esempio per rispettare obblighi di legge, per garantire diritto di cronaca o per finalità documentaristiche) (art. 17 Reg. UE n. 2016/679). La cancellazione potrà essere pretesa "senza ingiustificato ritardo" se i dati non siano più necessari rispetto alle finalità per cui sono stati raccolti ovvero se sia stato ritirato il consenso o fatta opposizione al trattamento, in assenza di motivi legittimi che lo giustifichino oppure se i dati sono stati trattati illecitamente oppure se la cancellazione è prescritta al responsabile del trattamento da un obbligo di legge (art. 17, Reg. n. 2016/679). Alla previsione in cui si definisce il "diritto di limitazione di trattamento" (art. 18, Reg. UE n. 2016/679). Nonché a quella in cui si delinea un vero e proprio "diritto alla portabilità del dato" (art.20 Reg. UE n. 2016/679) consentendo un più semplice trasferimento dei propri dati personali. Resta inteso che il Titolare del trattamento che avesse reso pubblici i dati personali sarà obbligato a cancellarli tenendo conto della tecnologia disponibile e dei costi di attuazione.

4.4. … e la loro portata nel contesto delle relazioni giuslavoristiche

Le nuove disposizioni imporranno una maggiore attenzione alle aziende non solo con riferimento alle attività di trattamento dei dati personali riferibili

([49]) Corte di Giustizia 13 maggio 2014, C-131/12 Mario Costeja Gonzalese e AEPD contro Google Spain e Google Inc http://curia.europa.eu/juris/document/document.jsf?docid=152065&doclang=IT.

ai propri dipendenti, ma anche alle attività di conservazione ed eventuale cancellazione dei dati riferibili alla loro "storia lavorativa". Si pensi anche alle necessarie e indispensabili cautele che dovranno essere osservate nella distruzione dei dati contenuti nei *pc* e *personal devices* concessi in dotazione dalle aziende ai propri dipendenti.

Le descritte novità potranno avere rilevanza altresì per i lavoratori impiegati in gruppi societari multinazionali che risulteranno maggiormente protetti grazie al più esteso campo di applicazione territoriale, al rafforzamento degli obblighi di informativa e dei diritti di accesso ai dati inseriti nel fascicolo personale e agli obblighi di notifica in caso di rettifica, cancellazione o limitazioni del trattamento codificati con maggiore attenzione nel Regolamento UE n. 2016/679.

Resta inteso che la previsione di questi nuovi diritti di rettifica e/o cancellazione dei dati, previsti nel Regolamento UE n. 2016/679, potranno avere rilevanza per garantire l'effettività della protezione dei dati personali dei dipendenti sempre che si provveda a una puntuale regolamentazione anche processuale del principio dell'inutilizzabilità delle informazioni trattate in violazione della disciplina della *privacy* (sul punto vedi oltre § Conclusioni).

5. I nuovi obblighi per i Titolari e i Responsabili del trattamento dei dati personali

L'impianto normativo del Regolamento UE n. 2016/679 riservato all'individuazione degli obblighi dei Responsabili del trattamento dei dati contenuto nel Capitolo IV e articolato in ben cinque Sezioni si presenta decisamente innovativo. Rispetto alla disciplina a tutela della *Privacy* contenuta nella Direttiva madre n. 95/46/CE il Regolamento UE n. 2016/679 presenta un capovolgimento di prospettiva destinando la parte più significativa della disciplina a tutela della riservatezza non più ai diritti dei *data subjects*, ma ai doveri dei Titolari e dei Responsabili del trattamento e alle misure di sicurezza adottabili o da adottare alla luce di un nuovo approccio ([50]).

([50]) In tal senso anche F. Pizzetti, Privacy *e diritto Europeo alla protezione dei dati personali. Dalla Direttiva 95/46 al nuovo Regolamento europeo*, cit., 154.

5.1. La proceduralizzazione degli obblighi di protezione dei dati personali

La protezione dei dati personali trova un importante e ulteriore rafforzamento nella proceduralizzazione degli obblighi di Titolari e Responsabili, che risultano pesantemente aggravati, ma ove rispettati capaci di assicurare un elevato livello di sicurezza dei trattamenti.

Nel Regolamento UE n. 2016/679 si obbligano i Titolari del trattamento a un'Analisi e Valutazione dei Rischi ([51]) e alla conseguente adozione di Misure di Sicurezza Tecniche e Organizzative "adeguate" (e non più "minime" come nella precedente disciplina della direttiva madre n. 95/46/CE e negli artt.33 e ss. d.lgs. n. 196/2003 e declinate nell'Allegato B) (art. 5 e 32, Reg. UE n.2016/679) ([52]).

Resta inteso che una preventiva analisi dei rischi era implicita anche nella disciplina previgente per consentire al Titolare di adottare le misure di sicurezza prescritte per legge. Tuttavia nell'impianto del nuovo Regolamento l'analisi e valutazione dei rischi, unitamente a una valutazione d'impatto sulla protezione della riservatezza (cd. *Privacy Impact Assessment*) diverrà una procedura obbligatoria e indispensabile per processi considerati dal Regolamento, dalle Autorità Garanti o dal Comitato Europeo come "pericolosi" per i dati personali ([53]).

Nel nuovo Regolamento si individuano alcuni ambiti per i quali la valutazione d'impatto sulla *privacy* viene imposta per la "pericolosità" del trattamento per i diritti e le libertà delle persone, considerata la natura, il campo di applicazione, il contesto e le finalità del trattamento, ma sarà riconosciuta alle singole Autorità di controllo degli Stati membri individuarne di ulteriori (art. 35-36, Reg. UE, n. 2016/679) ([54]). Le valutazioni d'impatto dovranno essere antecedenti allo sviluppo di un prodotto/servizio/processo e della sua definizione, nonché periodiche sullo stato di applicazione del sistema di privacy aziendale e/o di processo. Risulteranno così aggravati gli adempimenti per enti pubblici/privati che svolgeranno quale attività primaria, non accessoria, trattamenti con monitoraggio regolare e sistematico degli interessati con tecnologie innovative in grado di realizzare profilazioni

([51]) Sull'analisi dei rischi cfr. Reg. UE n. 2016/679 considerando (60 bis), sulla valutazione dei rischi Reg. UE n. 2016/679 considerando (60 ter) e (66).

([52]) Cfr. Reg. UE n. 2016/679 considerando (61).

([53]) "In caso di rischio elevato per i diritti e le libertà delle persone fisiche il Titolare del Trattamento coadiuvato dal Responsabile dovrà predisporre una valutazione d'impatto sulla protezione dei dati per determinare l'origine, la natura, la particolarità e la gravità di tale rischio" Così A. Paro, Impact Assessment: *cosa cambia per le aziende*, in *DPL*, 28/2016, 1701.

([54]) Cfr. Reg. UE n. 2016/679 considerando (66 bis).

dettagliate (art.35 Reg. UE n. 2016/679). Ove vi siano trattamenti "rischiosi" per la riservatezza dei dati diventerà obbligatorio non solo analizzare e valutare preventivamente i rischi per la riservatezza ma altresì valutare l'impatto sulla *privacy* di soluzioni tecnico-organizzative adottate nell'azienda in relazione non solo a macro-processi ma anche a singole aree di produzione o micro-processi (cd. *Privacy Impact Assessment*). Quanto all'adeguatezza delle misure di protezione si precisa che diventerà inoltre obbligatoria la previsione e conseguente adozione di misure tecniche organizzative adeguate per attuare in modo efficace i principi di protezione dei dati sin dalla loro progettazione (cd. "*privacy by design*") con impostazioni di *Privacy* predefinite chiuse e non aperte (cd. "*privacy by default*") affinché siano trattati solo i dati personali necessari per ogni specifica finalità e non siano resi accessibili se non a un numero definito di persone (considerando 78 e art.25, Reg. UE n. 2016/679). Da ultimo diverranno obbligatori controlli periodici sull'adeguatezza ed effettività delle misure predisposte.

Le realtà che effettueranno trattamenti più "a rischio" dovranno nominare Responsabile della protezione dei dati, un consulente specializzato (cd. *Data Protection Officer*), comunicandolo all'Autorità Nazionale Garante per la Protezione dei Dati Personali (art.37, Reg. UE n. 2016/679) ([55]). Il *Data Protection Officer* potrà essere interno e/o esterno all'organizzazione del Titolare del trattamento ma dovrà essere dotato di particolari poteri sì da assicurare la conformità delle aziende alle nuove regole (art.38 Reg. UE n. 2016/679). Tale professionista dovrà essere "tempestivamente" ed "adeguatamente" coinvolto in tutte le questioni riguardanti la protezione dei dati personali e sarà tenuto ad informare e fornire consulenza al Titolare o al Responsabile del trattamento; sorvegliare l'osservanza del regolamento inclusa l'attribuzione di responsabilità, la sensibilizzazione e la formazione del personale; fornire pareri sulla valutazione d'impatto delle misure adottate; cooperare con l'Autorità di controllo anche fungendo da contatto con la stessa per questioni attinenti al trattamento dei dati (art.37 co. 1 e art.39, Reg. UE n. 2016/679) ([56]).

5.2. … i connessi adempimenti documentali

La descritta responsabilizzazione e proceduralizzazione dovrà inoltre essere accompagnata da precisi adempimenti documentali, ciò in sostituzione

([55]) Cfr. Reg. UE n. 2016/679 considerando (75).

([56]) Vedi la sintesi contenuta nel documento informativo predisposto dall'Autorità Garante Italiana http://194.242.234.211/documents/10160/0/Data+Protection+Officer+-+Scheda+infomativa

dei meccanismi autorizzativi con preventivi obblighi di notifica/autorizzazione ai trattamenti di dati personali all'Autorità Nazionale Garante della Protezione dei Dati Personali ([57]). Il Titolare del trattamento e il Responsabile del trattamento dovranno tenere dei registri. Si tratta di doveri di documentazione degli adempimenti e procedure attinenti ciascun trattamento con la conservazione di documenti (riferimenti dei responsabili interni/esterni; rappresentanti all'estero; finalità ambiti di comunicazione e diffusione; misure di sicurezza adottate – Registro dei trattamenti art.30, Reg. UE n. 2016/679) e di comunicazione entro termini brevi (dalle 48 alle 72 ore) agli interessati e all'Autorità Garanti delle eventuali violazione dei dati e/o incidenti informatici (*personal data breach*) (artt.33-34, Reg. UE n. 2016/679) ([58]).

Nel Regolamento gli obblighi documentali connessi alla corretta gestione della protezione dei dati personali saranno anche finalizzati a rendicontare gli adempimenti e a dimostrare la *Compliance Privacy* delle operazioni svolte. Il Registro delle attività di trattamento che dovrà essere redatto dal Titolare ed esibito su richiesta del Garante, con obbligo di conservazione della documentazione dei trattamenti effettuati con indicazione di una serie dettagliata di informazioni (art.30, Reg. UE n. 2016/679). Tale Registro sarà obbligatorio per imprese o organizzazioni con più di 250 dipendenti ovvero per imprese di dimensioni inferiori qualora il trattamento dalle stesse effettuato possa presentare un rischio per i diritti e le libertà dell'interessato, non sia occasionale o includa i trattamenti di dati che nella precedente regolamentazione erano definiti come sensibili o giudiziari (art.30, co. 5, Reg. UE n. 2016/679).

5.3. …. e l'impatto sull'organizzazione aziendale

Le norme qui descritte comporteranno un profondo cambiamento di prospettiva nella tutela della protezione dei dati personali con responsabilizzazione delle figure a cui vengono affidate posizioni di garanzia (cd. principio di *accountability*) che richiama la rivoluzione apportata in passato in seguito all'adozione della dir. n. 89/389 a garanzia della tutela dell'igiene e della sicurezza nei luoghi di lavoro che ha prescritto una proceduralizzazione degli obblighi con affiancamento del datore di lavoro si figure professionali specializzate nella prevenzione.

([57]) Cfr. Reg. UE n. 2016/679 considerando (70).

([58]) Si tratta di adempimenti già introdotti nel 2012 nel Codice della Privacy italiano ma solo per alcuni operatori del settore delle comunicazioni elettroniche, anche puntualizzati in provvedimenti specifici dell'Autorità Garante Italiana sulla biometria e i dossier sanitari elettronici nel 2014.

Nel tentativo di diffondere buone prassi nel Regolamento si dedica attenzione ai codici di condotta e al sistema di certificazione volontaria. La Sezione V del Capo IV del Regolamento UE n. 2016/679 è dedicata alle Linee Guida per l'adempimento delle nuove regole (artt.40-41, reg. UE n. 2016/679)([59]) e alla promozione di sistemi di certificazione, destinati a essere monitorati dall'Autorità di Controllo, capaci di dare immediata visibilità agli interessati del livello di protezione dei dati dei relativi prodotti e servizi (artt. 42 e 43, Reg. UE n. 2016/679) ([60]).

Nel nuovo Regolamento si chiede alle aziende di adottare un nuovo modello organizzativo con meccanismi di responsabilizzazione interna (cd. principio di *accontability*) ([61]). L'approccio organizzativo delle nuove norme a tutela della sicurezza dei dati personali richiama, per la parte di *compliance*, due recenti *standard* internazionali: la ISO 19600 che introduce un approccio sistemico alla conformità aziendale per tutte le obbligazioni e la nuova ISO 9001 che richiede un'analisi del contesto in diversi settori, il coinvolgimento dei portatori di interessi e un'analisi dei rischi. I meccanismi di certificazione proposti nel Regolamento dovrebbero facilitare l'utente nella comprensione dei contenuti e della tipologia di trattamento dei dati personali fornendo garanzie circa la correttezza, la liceità e la responsabilità del Titolare, anche tenendo conto delle realtà di ridotte dimensioni ([62]).

Analogamente a quanto è avvenuto nella materia della salute e tutela della sicurezza sul lavoro (dir. n. 389/89) e nella disciplina della responsabilità amministrativa dell'impresa (d.lgs. n. 231/2001 e l. n. 123/2007), nella gestione della tutela della riservatezza si promuove la diffusione di modelli organizzativi assistiti da precisi sistemi documentali. Come vedremo, i poteri di accreditamento degli Organismi di certificazione, individuazione dei criteri di certificazione e di rilasciare certificazioni saranno affidati all'Autorità di Controllo che potrà altresì graduare le sanzioni amministrative pecuniarie in caso di adesione a modelli organizzativi certificati.

([59]) Cfr. Reg. UE n. 2016/679 considerando (60 *quater*).

([60]) Cfr. Reg. UE n. 2016/679 considerando (77).

([61]) M. Soffientini, *Protezione dei dati personali: nuovo Regolamento UE*, in *DPL*, 2016, n. 26, 1565.

([62]) Il Progetto Europeo *Privacy Flag*, sostenuto dai fondi del Programma Horizon 2020, è finalizzato a creare uno strumento rivolto alle piccole imprese che trattano dati personali per autovalutarsi e comprendere il loro livello di conformità alla disciplina europea. Vedi C. Bistolfi, Internet of things, accountability *e certificazioni: tutte le novità* in *Privacy News*, n.1/2016, 31

6. Il riconoscimento agli Stati del potere di declinare nuovi obblighi di protezione dei dati personali nel contesto occupazionale

Venendo alla protezione dei dati personali riservata al dipendente si è già osservato come nella direttiva madre n. 95/46/CE non si prevedesse alcuna disciplina peculiare per il trattamento dei "dati personali" nel rapporto di lavoro. Ci si limitava a promuovere nei settori specifici l'elaborazione di codici di condotta per la corretta applicazione delle disposizioni generali della direttiva (art.27 Dir. n. 95/46/CE). Peraltro, già nella previgente disciplina, il Garante della Privacy italiano aveva elaborato una puntuale disciplina a garanzia della dignità del dipendente rispetto all'esercizio del potere datoriale di controllo ([63]).

Tale approccio muta nel Regolamento UE n. 2016/679. Accanto a norme generali sulla protezione dei dati personali si riserva a ciascuno Stato membro la facoltà di prevedere, tramite leggi o contratti collettivi, discipline più specifiche rispetto a quelle generali descritte nei paragrafi precedenti per assicurare la protezione dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro (art.88, co. 1, Reg. UE n. 2016/679). Le norme speciali potranno essere introdotte "*per finalità di assunzione, esecuzione del contratto di lavoro, compreso l'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi, di gestione, pianificazione e organizzazione del lavoro, parità e diversità sul posto di lavoro, salute e sicurezza sul lavoro, protezione della proprietà del datore di lavoro o del cliente e ai fini dell'esercizio e del godimento, individuale o collettivo, dei diritti e dei vantaggi connessi al lavoro, nonché per finalità di cessazione del rapporto di lavoro*" (art.88, co. 1, Reg. UE n. 2016/679). Discipline nazionali potranno introdurre "*misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro"* (art.88, co. 2, Reg. UE n.2016/679).

Resta inteso che nell'elaborazione delle discipline speciali ciascuno Stato sarà tenuto ad adottare una politica conforme a quanto previsto nella Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri già sopra richiamato (cfr. § 1). La Raccomandazione, atto di indirizzo del Consiglio d'Europa, non potrà essere del tutto disattesa in quanto attuazione dell'art. 8

([63]) Per una ricostruzione dei limiti ai controlli datoriali a tutela dei dati personali si veda da ultimo E. Barraco - A. Sitzia, *Potere di controllo e* privacy. *Lavoro, riservatezza e nuove tecnologie*, Wolters Kluwer, 2016

CEDU norma a tutela del diritto alla vita privata più volte richiamata nel preambolo e nel corpo dell'atto. "La legislazione nazionale che fosse manifestamente contrastante con i (…) (principi in essa contenuti) potrebbe (…) essere passibile di sanzione innanzi alla Corte, in quanto violazione diretta di quel "*right to private life*" tutelato dalla Convenzione e la cui interpretazione estensiva di "diritto a stabilire relazioni con altri esseri umani", include le relazioni di lavoro o di affari (Corte europea diritti dell'uomo, sez. III, 25 ottobre 2007, V.V. C. Paesi Bassi)" ([64]).

Nella prima parte della Raccomandazione (artt. 1 – 13) si richiamano i principi generali in materia di protezione dei dati personali dei lavoratori già contenuti nella direttiva madre e successivamente ribaditi nel Regolamento n. 2016/679 e si prescrivono norme volte a diminuire al massimo la circolazione dei dati e a garantire la maggior trasparenza possibile nel loro utilizzo. Nella seconda parte della Raccomandazione (artt. 14 – 21) si individuano con maggior precisione le "possibili forme di controllo derivanti dall'utilizzo delle nuove tecnologie, ponendo diverse garanzie a favore dei lavoratori, soprattutto in materia di trasparenza e giustificatezza del trattamento dei dati personali connessi all'uso di *Internet* e posta elettronica" ([65]). In particolare, si chiarisce che l'estrazione dei dati relativi al traffico *internet*; l'accesso allo scambio di comunicazioni elettroniche; l'analisi delle informazioni di geolocalizzazione sono assimilabili a un trattamento dei dati personali del dipendente. E tali attività se realizzate tramite "strumenti di lavoro" dovranno essere assoggettate ai medesimi limiti vigenti per la protezione dei dati (informativa preventiva del diretto interessato; principio di trasparenza; rispetto dei principi di necessità, pertinenza, proporzionalità e non eccedenza del trattamento) mentre se realizzate tramite "strumenti di controllo" dovranno essere assoggettate a ulteriori vincoli in coordinamento con le logiche collettive di protezione sindacale (consultazione autorizzativa delle rappresentanze sindacali).

Nella Raccomandazione non si preclude a ciascuno Stato di consentire al datore di lavoro di accedere ai dati relativi alle navigazioni *internet* dei propri dipendenti previa informativa e in presenza di un ragionevole motivo, né di accedere alle comunicazioni elettroniche in quanto necessario per motivi di sicurezza o altre legittime ragioni, previa informativa e adozione di misure finalizzate a evitare accessi abusivi (art. 14, Raccomandazione

([64]) Efficacemente così è stato chiarito da V. Deregibus - G. Machì, *Raccomandazione del Consiglio d'Europa CM/Rec(2015)5 e Jobs Act: profili di compatibilità e prospettive di tutela* in *Bolletino ADAPT* 26 marzo 2015.

([65]) Così V. Deregibus - G. Machì, *Raccomandazione del Consiglio d'Europa CM/Rec(2015)5 e Jobs Act: profili di compatibilità e prospettive di tutela* in *Bolletino ADAPT* 26 marzo 2015.

CM/Rec(2015)5). E si legittima, previa consultazione sindacale, l'uso di apparecchiature di videosorveglianza se volto a tutela della salute, della produzione, della sicurezza e dell'efficiente organizzazione della produzione e solo indirettamente consenta un controllo sull'attività dei lavoratori (art.15, Raccomandazione CM/Rec(2015)5).

Con particolare riguardo al nostro ordinamento, l'adeguamento alle nuove disposizioni del Regolamento Europeo interesserà solo il Testo Unico sulla *Privacy* d.lgs. n. 276/2003, senza imporre alcuna modifica a quanto disposto nel d.lgs. n. 81/2015 già coerente con i principi contenuti nella Raccomandazione del Consiglio d'Europa. Peraltro potrebbe consentire la soluzione di alcune criticità emerse in merito al generale rimedio dell'inutilizzabilità dei dati acquisiti e/o trattati in violazione della disciplina della Privacy.

7. I nuovi poteri delle Autorità Nazionali Garanti della Protezione dei Dati Personali

Significativamente potenziati nel Regolamento UE n. 2016/679 risultano il ruolo e i poteri riconosciuti alle Autorità Garanti e all'*European Data Protection Board*.

Nella *Direttiva madre* il Capo VI era dedicato all'Autorità di controllo e gruppo per la tutela delle persone con riguardo al trattamento dei dati personali e si prescriveva un obbligo generale di notifica alle Autorità di controllo del trattamento dei dati personali. Tali oneri amministrativi e finanziari erano stati ritenuti ingiustificati dalla Commissione Europea poiché dette notifiche non avevano di fatto contribuito a migliorare la protezione dei dati personali.

Nel Regolamento UE n. 2016/679 la disciplina dedicata alle Autorità Garanti e alle loro forme di cooperazione a livello europeo è contenuta nel Capo VI e VII e consta di una ventina di articoli (artt. 51-76 Reg. UE n. 2016/679). La profonda diversità tra la nuova disciplina e quella contenuta nella Direttiva madre n. 95/46 ben si comprende qualora si consideri che le Autorità Garanti sono state istituite dalla Direttiva e molti principi contenuti nel Regolamento UE sono stati elaborati grazie all'importante contributo fornito dalle Autorità Garanti Nazionali anche riunite nel "Gruppo di lavoro articolo 29" ([66]).

([66]) F. Pizzetti, cit., 166-167.

Nel Regolamento viene prescritto che a tutte le Autorità Nazionali siano riconosciuti stessi poteri di intervento e controllo e sia garantito un potere maggiore di Autorità capofila a quella Autorità garante riferibile al Paese del responsabile del trattamento (cd. *one stop shop* art. 54 e art.56, Reg. UE n. 2016/679)([67]). Vengono individuati requisiti di indipendenza (art.51, Reg. UE n. 2016/679) e potenziati ambiti di intervento e poteri delle Autorità Garanti Nazionali per il controllo dell'effettivo rispetto delle norme ([68]) che saranno autorizzate a fornire adeguata protezione ai cittadini in merito all'utilizzo dei propri dati personali e dovranno essere consultate in caso di adozione di strumenti normativi con impatto sulla protezione dei dati personali (art. 55 e art. 58, Reg. n. 2016/679). Inoltre si prevede che alle Autorità Garanti dovranno essere riconosciuti poteri di indagine, di intervento nonché autorizzativi e consuntivi tra cui il potere di accreditare Organismi di certificazione, rilasciare certificazioni e approvare i criteri di certificazione (art. 58, co. 3, lett.e-f), Reg. UE n. 2016/679).

Nel Regolamento UE n. 2016/679 da ultimo si regolamentano i rapporti tra Autorità dei diversi Paesi (artt. 61-65, Reg. UE n. 2016/679) e si istituisce il Comitato europeo per la protezione dei dati composto dai vertici di ciascuna Autorità di controllo per ciascuno Stato membro e dal Garante Europeo per la protezione dei dati (artt. 68 e ss., Reg. UE n. 2016/679).

L'entrata in vigore in Italia del Regolamento imporrà di potenziare i poteri e il ruolo dell'Autorità Garante che, in merito alla protezione dei dati personali nel rapporto di lavoro che a noi qui interessa, ha svolto un'importante attività di precisazione delle disposizioni contenute nel Codice della *Privacy* elaborando Linee Guida ([69]) nonché Provvedimenti Generali ([70]).

([67]) Cfr. Reg. UE n.2016/679 considerando (100).

([68]) Cfr. Reg. UE n.2016/679 considerando (94), (95) e (96)

([69]) Cfr. http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1772725 Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro alle dipendenze di datori di lavoro privati del 23 novembre 2006; Linee guida del Garante per posta elettronica e internet del 1 marzo 2007; Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico del 14 giugno 2007; Linee guida in materia di riconoscimento biometrico e firma grafometrica del 12 novembre 2014.

([70]) Cfr. altresì http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/3755203 Provvedimento generale sulla video sorveglianza dell'8 aprile 2010; Provvedimento generale prescrittivo in tema di biometria del 12 novembre 2014.

8. Il nuovo assetto dei rimedi e delle sanzioni

Un ulteriore profilo che caratterizza il Regolamento UE n. 2016/679 e distingue la nuova disciplina da quella delineata nella Direttiva madre n. 95/46/CE è quello attinente al sistema dei rimedi e delle sanzioni.

8.1. La tutela dell'interesse ad agire in caso di violazione dei diritti alla riservatezza

Nella direttiva madre n. 95/46/CE il Capo III era dedicato ai ricorsi giurisdizionali. Nel Regolamento la materia è regolata nel Capo VIII ove trova conferma il principio della responsabilità risarcitoria per il cd. "danno da trattamento", ma con una codificazione più puntuale ([71]),. Nelle disposizioni regolamentari si rinviene una più precisa definizione dei meccanismi di ripartizione del risarcimento tra Titolare, co-titolare e Responsabile del trattamento con previsione specifica di azioni di regresso reciproche e meccanismi di esonero (art.82, Reg. UE n. 2016/679).

Nel Regolamento si riconosce il diritto di proporre reclamo all'Autorità di controllo e/o ricorso all'autorità giudiziaria nello Stato membro in sui risiede abitualmente oppure del luogo in cui si è verificata la presunta violazione (art. 77 e art. 79, Reg. UE n. 2016/679). Sono altresì previste norme processuali destinate a regolare la competenza delle diverse Autorità in caso connessione, continenza contemporanea pendenza di ricorsi sugli stessi fatti innanzi ad Autorità Nazionali diverse che prevalgono in quanto specifiche rispetto alle previsioni processuali contenute nel più generale Reg. UE n. 1215/2012.

Trova conferma il diritto di ricorrere all'autorità giudiziaria avverso le decisioni dell'Autorità di controllo (art. 78, Reg. UE n. 2016/679). Nel Regolamento UE si sancisce dunque il diritto di impugnazione delle decisioni delle Autorità di Controllo Nazionali che producono effetti direttamente nei confronti delle persone fisiche/giuridiche (come ad esempio l'esercizio di poteri di indagine, correttivi e autorizzativi da parte dell'autorità di controllo o l'archiviazione o il rigetto dei reclami) innanzi alle autorità giurisdizionali dello Stato in cui l'Autorità è stabilita e secondo le regole processuali dello Stato di appartenenza.

([71]) Nell'art.15, d.lgs. n.196/2003 si prevede che chiunque cagiona danno ad altri per effetto del trattamento di dati personali è tenuto al risarcimento ai sensi dell'art.2050 c.c.. Per una ricostruzione dell'elaborazione giurisprudenziale si veda E. Bassoli, *La sicurezza dei sistemi informativi aziendali: norme protettive, oneri e misure minime obbligatorie*, cit., 861 e ss.

Ulteriore rafforzamento della protezione di colui che ritenga di aver subito trattamenti illegittimi si rinviene nel riconoscimento della facoltà di dare mandato a presentare reclamo e/o a ricorrere da parte di organizzazioni/associazioni che abbiano tra gli scopi statutari la difesa dei diritti dei propri associati (art. 80, Reg. UE n. 2016/679).

8.2. La nuova declinazione delle sanzioni

Nella direttiva madre n.95/46/CE il Capo III era dedicato alle responsabilità e alle sanzioni. Nell'attuare la disciplina dell'Unione Europea il d.lgs. n.196/2003 aveva declinato nel nostro ordinamento un sistema costituito da sanzioni amministrative (art. 163, d.lgs. n. 196/2003) e penali (art. 169, d.lgs. n. 196/2003) in caso di trattamento illecito di dati personali e omessa adozione di misure di sicurezza. Ulteriori sanzioni erano previste dallo Statuto dei Lavoratori art.38, legge n.300/1970 in caso di violazione della riservatezza negli ambienti di lavoro tramite controlli a distanza.

Ai descritti illeciti erano connessi profili di responsabilità civile per attività pericolosa (art. 2050 c.c.) in presenza di danni (art. 15, d.lgs. n. 196/2003)([72]) di esclusiva competenza del giudice ordinario (art.152 d.lgs. n. 196/2003)([73]).

Il sistema sanzionatorio previsto nel Regolamento UE n. 2016/679 appare notevolmente inasprito rispetto a quello adottato nel nostro ordinamento dagli artt.161 e ss. d.lgs. n. 196/2003 in recepimento della direttiva madre n. 95/46/CE ([74]).

([72]) Cfr. G. Corasaniti, *La responsabilità civile da reato informatico* in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Utet Torino, 2014, 703 e sul punto 728-738.

([73]) Si veda M. Franzoni, *Responsabilità derivante da trattamento dei dati personali* in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Utet Torino, 2014, 829. Sulla giurisdizione esclusiva del giudice ordinario in tema di risarcimento del danno pacificamente il Garante ha sempre sostenuto che "*Deve essere dichiarata inammissibile la richiesta contenuta nel ricorso al Garante di risarcimento del danno derivante dall'illecito trattamento dei dati personali, non avendo la legge attribuito all'Autorità alcuna competenza in merito. La domanda può essere eventualmente riproposta dall'interessato, ove ne ricorrano i presupposti, dinanzi alla competente autorità giudiziaria"* così Provvedimento Garante, 30 dicembre 2003 [doc. web n.1084799], in F. Garri, L. Pecora,G. Staglianò, *Massimario 1997 - 2001. I principi affermati dal Garante nei primi cinque anni di attività*, consultabile su http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1591839. Nello stesso senso da ultimo si è espressa Cass. 7 aprile 2016, n.6775 consultabile su http://www.italgiure.giustizia.it/xway/application/nif/clean/hc.dll?verbo=attach&db=snciv&id=./20160408/snciv@sL0@a2016@n06775@tS.clean.pdf

([74]) "*La legge articola una serie di sanzioni per determinate fattispecie che vanno dalla infedele notificazione degli atti al trattamento illecito di dati personali, fatti al fine di trarre profitto o di recare altrui danno ed ancora all'omessa adozione di misure necessarie alla sicurezza dei dati*" Si veda E. Bassoli, *La sicurezza dei sistemi informativi aziendali: norme protettive, oneri e misure minime obbligatorie*, cit., 864 e ss.

Quanto alle sanzioni amministrative i trattamenti illeciti di dati personali e/o la violazione degli obblighi previsti nel Regolamento UE n. 2016/679 dovranno essere puniti con sanzioni amministrative pecuniarie anche commisurate a percentuali del fatturato lordo mondiale dell'impresa e soglie massime estremamente elevate (art. 83, Reg. UE n. 2016/679) ([75]). Nel Regolamento non si prevedono minimi edittali e le sanzioni amministrative pecuniarie sono distinte in tre fasce di gravità (art. 83, commi 4,5,6 Reg. UE n. 2016/679). Nella prima si contemplano sanzioni fino a un massimo di 10.000.000 euro e 2% del fatturato sono puniti la violazione degli obblighi del titolare e del responsabile del trattamento (artt. 8 e11; artt. 25-39; artt. 42-43 Reg. UE n. 2016/679); la violazione degli obblighi dell'organismo di certificazione (artt. 42-43 Reg. UE n. 2016/679); la violazione degli obblighi dell'Organismo di controllo (art. 41, par. 4, Reg. UE n. 2016/679). Nella seconda si contemplano sanzioni fino a un massimo di 20 000 000euro e 4% del fatturato sono puniti la violazione dei principi di base del trattamento comprese le condizioni relative al consenso (artt. 5,6,7 e 9 Reg. UE n. 2016/679); la violazione dei diritti degli interessati (artt. 12-22 Reg. UE n. 2016/679); i trasferimenti di dati a un destinatario in un paese terzo o organizzazione internazionale (artt. 44-49, Reg. UE n. 2016/679); la violazione di qualsiasi obbligo previsto dalle legislazioni degli Stati membri a norma del capo IX; l'inosservanza di un ordine, di una limitazione provvisoria o definitiva di trattamento o di un ordine di sospensione dei flussi dei dati dell'Autorità di Controllo ai sensi dell'art. 58 par. 2 o art. 58 par.1 Reg. UE n. 2016/679); l'inosservanza di un ordine da parte dell'Autorità di Controllo di cui all'art. 58, par. 2 Re. UE n. 2016/679.

Nel Regolamento inoltre si definiscono i criteri che l'Autorità di Controllo dovrà utilizzare nella graduazione delle sanzioni, che per quanto a noi qui interessa sono diversi rispetto a quelli previsti dalla legge n. 689/91. L'Autorità graduerà le sanzioni rispetto: a) la natura, la gravità e la durata della violazione tenendo conto della natura dell'oggetto e della finalità del trattamento, del numero dei soggetti lesi e del livello del danno subito; b) l'elemento soggettivo della violazione; c) le misure adottate per attenuare il danno subito dagli interessati; d) il grado di responsabilità del titolare e del responsabile del trattamento tenendo conto delle misure tecniche e organizzative adottate; e) eventuali precedenti violazioni; f) il grado di cooperazione con l'Autorità di Controllo; g) la categoria dei dati personali

([75]) Cfr. considerando (118 ter) e (119).

violati; h) le modalità con cui l'Autorità di Controllo è venuta a conoscenza della violazione e l'avvenuta notifica della violazione da parte del titolare e del responsabile del trattamento; i) il rispetto di precedenti provvedimenti dell'Autorità di Controllo; j) l'adesione a codici di condotta o sistemi di certificazione volontaria; k) eventuali altri fattori come ad esempio benefici finanziari conseguiti direttamente o indirettamente quale conseguenza della violazione (art. 83, co. 1, Reg. UE, n. 2016/679). Purtroppo all'adozione di modelli di certificazione volontaria non viene riconosciuta alcuna efficacia esimente da responsabilità, né alcuna presunzione di *compliance*, depotenziando l'effettiva dissuasività del sistema sanzionatorio a causa dell'incertezza del precetto ([76]). Si tratterà di verificare se l'Autorità di Controllo potrà/vorrà riconoscere alle certificazioni volontarie su questa materia valenza analoga a quella riconosciuta ai modelli organizzativi dall'art. 30, d.lgs. n. 231/2001.

Quanto alle sanzioni penali, il Regolamento affida a ciascuno Stato membro l'individuazione delle "altre" sanzioni per le violazioni al testo del Regolamento che in ogni caso dovranno essere *effettive, proporzionate e dissuasive*, nonché l'adozione dei provvedimenti *necessari per assicurarne l'applicazione* (art. 84, Reg. UE n. 2016/679).

Per quanto a noi qui interessa, resterà da verificare come verrà modificato in Italia il reato di trattamento illecito dei dati personali attualmente previsto all'art. 167, d. lgs. n. 196/2003. Resta inteso che, alla luce del consolidato orientamento della Corte Europea dei Diritti dell'Uomo e della Corte di Giustizia in merito al principio del *ne bis in idem*, la medesima condotta non potrà essere punita sia con sanzioni amministrative sia con sanzioni penali ([77]).

9. Conclusioni

L'analisi del Regolamento suggerisce che la protezione dei dati personali risulterà rafforzata nel contesto occupazionale grazie alla promozione di una "*nuova cultura organizzativa"* estesa anche oltre i confini

([76]) Sugli effetti negativi dell'incertezza del precetto sulla effettività e dissuasività dei sistemi sanzionatori mi sia consentito di rinviare a C. Ogriseg, *L'incertezza nella tutela della salute e sicurezza del lavoro*, in Perone - Vallebona (a cura di), *La certificazione dei contratti di lavoro*, Giappichelli, 2004, 43.

([77]) Cfr. CEDU, Grande Stevens c. Italia 4 marzo 2014 e vedi Relazione del Massimario della Cassazione http://www.cortedicassazione.it/cassazione-resources/resources/cms/documents/Relazione_pen_35_2014.pdf.

dell'Unione secondo l'orientamento della CGCE (art. 4 e art. 83, co. 2, Reg. UE n. 2016/679).

Supportate da un pesante aggravamento delle sanzioni pecuniarie amministrative, le norme a tutela della riservatezza proceduralizzano gli obblighi promuovendo la diffusione nelle aziende di un sistema organizzativo complesso. Un sistema capace di garantire l'adozione di "adeguate" misure di protezione individuate grazie analisi e valutazioni del rischio o di impatto. Codici di condotta, Linee Guida e modelli organizzativi previsti da sistemi di certificazione volontaria hanno il compito di diffondere il mutato approccio alla protezione dei dati personali, codificato nel *Regolamento generale* n. 2016/679 con potenziamento dei diritti personali fondamentali anche nelle relazioni di lavoro.

La tutela della riservatezza nel contesto occupazionale risulterà rafforzata dalla conferma dei principi già contenuti nella previgente disciplina e dalla previsione nel Regolamento di nuovi obblighi generali. La nuova declinazione del generale diritto a essere informati in maniera semplice ed efficace sul trattamento dei propri dati comporterà una maggiore consapevolezza per i dipendenti, garantendo maggiori opportunità di esercizio del diritto di accesso ai contenuti del proprio fascicolo personale (cfr. art. 15 Reg. UE n. 2016/679), con evidenti ripercussioni sull'effettività dei diritti costituzionali di difesa in sede di procedimento disciplinare. La previsione di obblighi di tutela anche in caso di trasferimenti di dati personali tra società garantirà inoltre una più intensa tutela del dipendente inviato in distacco.

Nel prossimo biennio, sarà quindi opportuno per le aziende italiane prevedere specifiche "Norme vincolanti d'impresa" (*Binding Corporate Rules*) e ridefinire la modulistica elaborata per l'assolvimento degli obblighi di informazione e trasparenza (anche attinenti ai controlli) declinandone il testo *in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro* (artt. 14 e 14bis Reg. UE n. 2016/679) ([78]). Nel nostro ordinamento, solo il rispetto delle disposizioni in tema di informativa del lavoratore e della disciplina sulla protezione dei dati personali consentirà l'utilizzabilità del dato personale acquisito "*a tutti i fini del rapporto di lavoro*" (ossia a fini retributivi o disciplinari) (art. 4, St. lav., novellato dall'art.23, d. lgs. n. 151/2015).

Resta da capire se, il legislatore italiano nell'introdurre "*misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali"* dei lavoratori (art. 88, co. 2, Reg. UE n. 2016/679) e nel

([78]) Cfr. M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e dei trattamenti dei dati (del lavoratore)*, WP C.S.D.L.E. "Massimo D'Antona" IT n. 300/2016, pag.28-29

prevedere dissuasive sanzioni (art. 84 Reg. UE n. 2016/679), provvederà a riconoscere effettività al principio dell'inutilizzabilità dei dati personali del dipendente illecitamente raccolti (art. 4, l. n. 300/1970 novellato dall'art. 23, d. lgs. n. 151/2015) e l'Autorità di Controllo eserciterà i propri poteri autorizzativi e consultivi riconoscendo alle aziende certificate in tema di privacy una ragionevole aspettativa di non incorrere in sanzioni amministrative pecuniarie.

Il rimedio generale dell'inutilizzabilità, già introdotto nel vigente Codice della *Privacy* (cfr. art. 11, co. 2, d. lgs. n. 196/2003) ([79]), è stato in passato pesantemente depotenziato dalla giurisprudenza. Le Corti italiane, in assenza di specifiche disposizioni processuali sulla validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti basati su un trattamento di dati non conforme nell'ambito del processo, avevano dato una lettura "riduttiva" della norma ([80]). Si registrava così una forte resistenza giurisprudenziale al riconoscimento dei "*limiti di ammissibilità istruttoria delle informazioni e dei dati acquisiti in violazione delle norme di legge*" a tutela della *privacy* ([81]). Nonostante il disposto di legge contenuto nell'art. 11, d.lgs. n. 196/2003, le Corti penali riconoscevano l'utilizzabilità processuale e l'ammissibilità di mezzi istruttori precostituiti fondati sugli stessi in considerazione del principio di prevalenza de "*l'esigenza di ordine pubblico relativa alla prevenzione dei reati*" rispetto alle disposizioni a tutela della riservatezza ([82]). Viceversa, le Corti civili riconoscevano l'inutilizzabilità anche processuale dei dati illegittimamente raccolti e dei mezzi istruttori basati sugli stessi nei casi in cui le informazioni illegittimamente raccolte comprovassero meri illeciti di natura civilistica ([83]).

Il generale rimedio dell'inutilizzabilità del dato, di fatto depotenziato per l'assenza di norme aventi natura sostanziale e processuale ([84]), non

([79]) Vedi A. Maietta, *Commento* sub *art.11*, in S. Sica – P. Stanzione (a cura di), *La nuova disciplina della privacy*, Bologna Zanichelli, 2004

([80]) Secondo il d.lgs. n.196/2003 Codice della *Privacy* "*la validità, l'efficacia e l'utilizzabilità di atti, documenti e provvedimenti nel procedimento giudiziario basati sul trattamento di dati personali non conforme a disposizioni di legge o di regolamento restano disciplinate dalle pertinenti disposizioni processuali nella materia civile e penale*" (art. 160 d.lgs. n. 196/2003).

([81]) Così C. Gamba, *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove* LLI, 2015, vol.1, num., § 5.

([82]) In tal senso Cass. pen., sez.V, 16 marzo 2016 in http://www.cassazione.net; Cass. pen. sez. II, 25 novembre 2009 in *DPL*, 2010, p.451. In dottrina cfr. P. Tullini, *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, in *RIDL*, 2011, II, 89.

([83]) Così C. Gamba, *op.cit.*, § 5 che richiama Cass. civ., 1 agosto 2013, n.18443 in *Nuova Giur. Civ.*, 2014, 103.

([84]) Norme di natura sostanziale ossia volte a stabilire la natura del vizio del provvedimento datoriale basato sul dato personale illegittimamente trattato; norme di natura processuale ossia volte a stabilire l'inammissibilità in giudizio di istanze istruttorie volte all'introduzione di documenti (prove precostituite) e testimonianze (prove costituende) basate su dati personali illecitamente acquisiti.

consente di garantire nel contesto occupazionale la necessaria dissuasività al sistema sanzionatorio a tutela della *privacy*.

L'auspicio è che durante il biennio di transizione il potenziamento dei *data protection* (artt. 12-22 Reg. UE n. 2016/679) venga affiancato da un sistema di rimedi declinato con norme interne effettive e dissuasive nel rispetto del diritto dell'Unione Europea (cfr. art. 84, Reg. UE n. 2016/679). Un sistema che, nel contesto delle relazioni di lavoro, implicherebbe non solo e non tanto un più pesante assetto delle sanzioni, quanto una definizione dei profili sostanziali e processuali dell'inutilizzabilità dei dati personali del dipendente illecitamente acquisiti/trattati dal datore di lavoro e la previsione di un regime di presunzioni capace di garantire alle aziende virtuose certificate una ragionevole aspettativa di non incorrere in sanzioni.

Bibliografia.

Agenzia dell'Unione Europea per i diritti fondamentali – Consiglio Europeo (a cura di), *Manuale sul diritto europeo in materia di protezione dei dati*, 2014 su http://www.echr.coe.int

Alvino I., *I nuovi limiti al controllo a distanza dell'attività dei lavoratori nell'intersezione fra le regole dello Statuto dei lavoratori e quelle del Codice della privacy, LLI*, 2016, vol. 2, 1, 1-45.

Barraco E. – Sitzia A., *Potere di controllo e* privacy. *Lavoro, riservatezza e nuove tecnologie*, Milano Wolters Kluwer, 2016.

Bassoli E., *La sicurezza dei sistemi informativi aziendali: norme protettive, oneri e misure minime obbligatorie*, in G.Cassano – G. Scorza – G. Vaciago, Diritto dell'internet, Cedam, 2013, 831 e ss.

Bistolfi C., Internet of things, accountability *e certificazioni: tutte le novità*, in *Privacy News*, n.1/2016, 31.

Carinci M.T., *Il controllo a distanza dell'attività dei lavoratori dopo il "Jobs Act" (art. 23 D lgs. 151/2015): spunti per un dibattito*, *LLI*, 2016, vol. 2, 1, I.

Ciccia Messina A. – Bernardi N., *Privacy e Regolamento Europeo 2016/679*, Milano Ipsoa, 2016

Corasaniti G., *La responsabilità civile da reato informatico* in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Utet Torino, 2014, 703.

Del Ninno A., *Il Regolamento UE Generale sulla protezione dei dati personali n.679/2016: analisi pratica del quadro generale di insieme e nuovi adempimenti privacy* apparso in data 17 maggio 2016 in http://www.DirittoeGiustizia.it

Del Punta R., *La nuova disciplina dei controlli a distanza sul lavoro,* in *RIDL,* 2016, I, n. 1.

Deregibus V- - Machì G., *Raccomandazione del Consiglio d'Europa CM/Rec(2015)5 e Jobs Act: profili di compatibilità e prospettive di tutela* in *Bolletino ADAPT* 26 marzo 2015.

Di Filippo Novario, *La progettazione della privacy* in *DPL*, 2016, n.27, 1633.

Ferri S., *Come gestire gli ex-incaricati del trattamento?*, in *Privacy News,* n.1, 2016, 53.

Finocchiaro G. (a cura di), *Diritto all'anonimato. Anonimato, nome e identità personale*, in Galgano (diretto da), *Trattato di diritto commerciale e diritto pubblico dell'economia*, vol XLVIII, Cedam, 2008.

Finocchiaro G., *La protezione dei dati personali e la tutela dell'identità*, in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Utet, 2014, 151.

Franzoni M., *Responsabilità derivante da trattamento dei dati personali* in G. Finocchiaro – F. Delfini (a cura di), *Diritto dell'informatica*, Utet, 2014, 829.

Gamba C., *Il controllo a distanza delle attività dei lavoratori e l'utilizzabilità delle prove*, *LLI*, 2016, vol. 2, 1, 120-157.

Garri F. - Pecora L. - Staglianò G., *Massimario 1997 - 2001. I principi affermati dal Garante nei primi cinque anni di attività*, consultabile su http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1591839Maietta A., *Commento* sub *art.11*, in S. Sica – P. Stanzione (a cura di), *La nuova disciplina della privacy*, Bologna, 2004.

Majo V., *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica,* in *ADL,* 2015, n. 6, pag. 1186.

Marazza M., *Dei poteri (del datore di lavoro), dei controlli (a distanza) e dei trattamenti dei dati (del lavoratore),* WP C.S.D.L.E. "Massimo D'Antona" IT n.300/2016.

Maresca A.*, Jobs Act, come conciliare potere di controllo e tutela della dignità e riservatezza del lavoratore* in *http://www.ipsoa.it/documents/lavoro-e-previdenza/rapporto-di-lavoro/quotidiano/2016/02/22/jobs-act-come-conciliare-potere-di-controllo-e-tutela-della-dignita-e-riservatezza-del-lavoratore* consultato in data 26 febbraio 2016.

Messina A.C. - Bernardi N., *Privacy e Regolamento* Europeo, Ipsoa, 2016.

Pallaro P., *Libertà della persona e trattamento dei dati personali nell'Unione Europea*, Giuffré, 2002.

Paro A.*, Impact Assessment: cosa cambia per le aziende,* in *DPL,* 2016, n.28, 1701.

Pizzetti F., *Privacy e il diritto europeo alla protezione dei dati personali. Dalla direttiva 95/46 al nuovo Regolamento europeo*, Giappichelli, 2016.

Salimbeni M. T.*, La riforma dell'art. 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore,* in *RIDL,* 2015, n. 4, 589.

Soffientini M. (a cura di), *Privacy. Protezione e trattamento dei dati*, Ipsoa, 2016.

Soffientini M., *Dal* Safe Harbor *al* Privacy shield*: la svolta dell'Unione Europea*, in *Privacy News*, n.1/2016, 26.

Soffientini M., *Protezione dei dati personali: nuovo Regolamento UE*, in *DPL*, 2016, n.26, 1565

Stizia A., *Il diritto alla "privatezza" nel rapporto di lavoro tra fonti comunitarie e nazionali*, Cedam, 2013.

Tullini P., *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, in *RIDL*, 2011, II, 89.