La tutela della privacy del lavoratore controllato a distanza

Borsa di Studio "Costanzo Iorio"
Evoluzione e Identità Digitale

Prefazione di Massimo Miani

Presentazione di Andrea Foschi

Consiglio Nazionale
dei Dottori Commercialisti
e degli Esperti Contabili

Fondazione
Nazionale dei
Commercialisti

La tutela della privacy del lavoratore controllato a distanza

Borsa di Studio “Costanzo Iorio”
Evoluzione e Identità Digitale

ISBN 978-88-99517-20-5

Questa borsa di studio è dedicata al dott. Costanzo Iorio, nato in Foggia il 13 dicembre 1940, assassinato il 6 giugno 2008 nel compimento del proprio dovere di curatore fallimentare. Iscritto nell'Albo dell'Ordine dei Dottori Commercialisti di Foggia a far tempo dal 26 febbraio 1970, ha sempre svolto il proprio lavoro di libero professionista facendosi apprezzare come uomo di principio e rispettoso delle regole.

Aveva una grande passione civile che ha messo al servizio della sua terra, tanto sul piano dell'impegno professionale quanto nella partecipazione alla vita politica, avendo – tra i molteplici incarichi – ricoperto anche la carica di Difensore Civico presso l'Ente Provinciale di Foggia.

Tra le Sue passioni private, ricordo che era amante e cultore della musica Jazz. Sovente organizzava indimenticabili concerti per gli amici in una tavernetta privata nel centro della Città. Nello stesso luogo, venivano anche organizzati degli incontri, con la Sua presenza e quella di tanti colleghi, tra i quali voglio ricordare due presidenti Giorgio Sannoner e Marisa Cavaliere, per discutere del futuro della professione e di come Noi giovani dovevamo costruire un Ordine, quello di Foggia, al passo con i tempi.

La sua uccisione ha privato la comunità in cui ha vissuto di una figura professionale apprezzata in ogni ambito. A ricordo della sua persona e del suo sacrificio, presso il Tribunale di Foggia, gli è stata dedicata l'aula dei curatori fallimentari.

Giuseppe Laurino

Consigliere del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Indice

Prefazione

Sono ormai prossime le celebrazioni del cinquantenario dello "Statuto dei lavoratori", il corpus normativo che più di tutti ha caratterizzato il diritto del lavoro del '900 e che è assurto a riferimento "sistematico" di ogni operatore del diritto impegnato nello studio della materia.

L'approvazione della legge n. 300 del 20 maggio 1970 ha consentito nei luoghi di lavoro l'inveramento di valori condivisi, garantendo ai lavoratori l'effettivo godimento dei diritti e delle libertà fondamentali sanciti dalla Carta costituzionale. La ratio legis fu esplicitata nella relazione "Brodolini" di accompagnamento allo Statuto, il cui articolato era deputato a colmare la carenza di "disposizioni precise di attuazione" dei principi garantiti nella Carta costituzionale, al contempo, contemperando le esigenze dell'impresa con i valori della persona.

Tra queste, lo Statuto ha introdotto una specifica regolamentazione volta a salvaguardare il diritto fondamentale alla riservatezza del lavoratore che ha innovato per la prima volta la legislazione italiana in materia di tutela delle informazioni personali. Con molti anni di anticipo rispetto alla introduzione del "Codice privacy", la normativa statutaria ha reso illegittimi i controlli personali e la raccolta di informazioni che esulano dall'ambito funzionale del rapporto di lavoro, vietando senza eccezioni ogni accertamento datoriale (ex art. 5 e 8, St. Lav.), ben oltre il perimetro di tutela di quelli che in seguito saranno chiamati "dati sensibili".

In ambito funzionale, la disciplina statutaria (ex art. 4 St. Lav.) ha pre¬visto il divieto di predisporre impianti aventi per finalità "diretta" il controllo a distanza dei lavoratori, mentre ha subordinato le forme di controllo "indiretto" alla presenza di interessi meritevoli del datore di lavoro.

Al momento della sua introduzione, la disciplina normativa ha mostrato il suo carattere fortemente innovativo e, messa alla prova dell'evoluzione dei tempi, si è mostrata a lungo di grande attualità. L'incessante progresso tecnologico e la crescente informatizzazione dei luoghi di lavoro ha imposto al legislatore nazionale un restyling normativo in una prospettiva di semplificazione e adattamento alle nuove modalità di organizzazione del lavoro, avvenuto con l'attuazione del Jobs act (art. 1, c. 7, lett. f, l. d. 10 dicembre 2014, n. 183 e art. 23 d.lgs. 151/2015).

A distanza di poco tempo, il legislatore europeo è intervenuto a riformare la disciplina sulla protezione dei dati personali delle persone fisiche, con l'adozione del Regolamento 2016/679/UE sulla protezione dei dati personali delle persone fisiche che ha sostituito

la Direttiva n. 95/46/CE, incidendo sulla normativa interna di attuazione, ossia il d.lgs. 196/2003.

Gli interventi di "manutenzione" normativa hanno avuto un notevole impatto sull'esercizio della libertà d'iniziativa economica. Su quest'ultima, difatti, si fonda la legittimità delle attività di controllo datoriali e di organizzazione del lavoro, in ambiti nevralgici della gestione del personale a cui i commercialisti del lavoro e gli altri operatori del diritto sono sovente preposti.

A partire dalle novità introdotte con le riforme (del lavoro e della privacy), il presente lavoro mira alla individuazione delle principali problematiche poste dall'ordinamento vigente offrendo, al contempo, possibili soluzioni interpretative e suggerimenti operativi quali validi strumenti per l'esercizio della nostra professione.

Massimo Miani

Presidente del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presentazione

“La tutela della privacy del lavoratore controllato a distanza” è un lavoro di studio strutturato in tre parti, finalizzato alla analisi delle principali problematiche giuridiche in materia, sia di carattere dogmatico che operativo.

Nella prima parte è sinteticamente ricostruita la disciplina giuridica dell’esercizio del potere di controllo del datore di lavoro. Viene tratteggiata l’evoluzione normativa in materia di attività di controllo nei luoghi di lavoro dall’introduzione dello Statuto dei lavoratori (legge n. 300 del 20 maggio 1970) fino alle ultime riforme del lavoro (Jobs Act), con particolare attenzione alla novella dell’art. 4 dello Statuto, introdotta dall’art. 23 d.lgs. 151/2015.

La riscrittura dell’art. 4 della l. n. 300/1970 ha introdotto elementi di grande innovazione in termini di semplificazione delle procedure autorizzatorie alla installazione degli impianti tecnologici di controllo, di utilizzazione ai fini del rapporto di lavoro dei dati trattati, nonché di armonizzazione normativa.

Sotto quest’ultimo aspetto, infatti, il legislatore tramite un rinvio espresso al d.lgs. n. 196/2003 (codice “pri¬vacy”), opera una definitiva “saldatura” tra i due plessi normativi, con una contestuale ponderazione dell’autonomia organizzativa e dell’esercizio del potere di controllo con i presidii giuridici posti a salvaguardia dei valori della persona. In questa prospettiva lo studio prende in debita considerazione i mutamenti di contesto giuridico sovranazionale che hanno di poco seguito le riforme dell’ordinamento interno. Infatti, a circa un anno dalla manutenzione della norma statutaria, il Parlamento europeo e il Consiglio hanno adottato il Regolamento 2016/679/UE, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, che condiziona l’esercizio del potere di controllo del datore di lavoro.

La seconda parte dello studio condotto mira proprio alla comprensione dei limiti posti alle attività di controllo nei luoghi di lavoro rinvenienti dall’intreccio della disciplina lavoristica con quella privacy. In conseguenza della centralità assunta dalla disciplina privacy nel nuovo testo dell’art. 4 St. Lav., si è posto in debita evidenza come l’esercizio del potere di controllo del datore di lavoro sia assoggettato al rispetto delle regole e dei principi generali attualmente enunciati dall’art. 5 GDPR: i principi di finalità e mi¬nimizzazione del trattamento che impongono al titolare di garantire che i dati personali siano “raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità”, a cui fanno da corollario i principi di adeguatezza, pertinenza e limitatezza a quanto necessario rispetto alle finalità per le quali si è inteso operare il controllo.

La terza parte dello studio, infine, è rivolta all'analisi delle principali prassi operative e amministrative del Garante della privacy, sia italiano che europeo.
L'approfondimento intende essere un supporto tecnico pratico ai commercialisti del lavoro delegati alla gestione e supervisione delle attività di controllo datoriali nei luoghi di lavoro.

Andrea Foschi
Segretario Generale della Fondazione Nazionale dei Commercialisti
Consigliere del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

La tutela della privacy del lavoratore controllato a distanza, alla luce della nuova disciplina sulla protezione dei dati personali

1. Premessa

La rivoluzione tecnologica e digitale che connota l'odierna società dell'informazione sta inevitabilmente impattando sul modo di fare impresa e, conseguentemente, sulle modalità di esecuzione del contratto di lavoro[1]. Da un lato, l'organizzazione del lavoro nell'impresa di tipo industriale prevede in misura crescente l'adozione di strumenti tecnologici e informatici necessari per l'esecuzione della prestazione lavorativa, dall'altro, le nuove imprese operanti nel settore dei servizi e del terziario utilizzano l'informazione non soltanto per rendere maggiormente efficiente il proprio processo produttivo ma quale bene commerciale utile a generare valore nel mercato della conoscenza.

Il processo di modernizzazione tecnologica, inoltre, si è sviluppato assieme ad un processo di flessibilizzazione organizzativa che ha avuto come principale riflesso una destrutturazione dei rapporti di lavoro subordinato rispetto alla durata, ai tempi e ai luoghi dell'esecuzione del contratto. In ambito giuslavoristico le risposte alle istanze di flessibilizzazione e adeguamento modernizzatore sono state fornite principalmente attraverso tre "epocali" passaggi normativi: il d.lgs. n. 276/2003 (riforma "Biagi"), la l. n. 92/2012 (riforma "Fornero"), la l. n. 183/2014 ("Jobs Act")[2]. Con essi si è segnato un allontanamento dal modello tradizionale di lavoro subordinato (*ex* art. 2094 c.c.), spesso accentuando quell'asimmetria di potere esistente tra datore e prestatore di lavoro che il legislatore storico aveva cercato di bilanciare con l'approvazione dello Statuto dei lavoratori (l. n. 300/1970). Un'asimmetria di potere insita nelle prerogative riconosciute al datore di lavoro imprenditore nell'esercizio della libertà di iniziativa economica (di cui all'art. 41 Cost.) e, dunque, nell'autonomia organizzativa garantitagli dall'ordinamento. È rispetto a tali attribuzioni giuridiche che occorre porre la maggiore attenzione nel definire

1 Per un'analisi sulle ricadute della rivoluzione digitale sulla politica attiva e passiva del lavoro cfr. D. Garofalo, *Rivoluzione digitale e occupazione: politiche attive e passive*, in *Il lavoro nella giurisprudenza*, 2019, n. 4, pag. 329 ss.

2 V. A. Riccardi, *Flessibilizzazione dei rapporti di lavoro e destrutturazione del sistema di tutela*, in Annali 2017 del Dipartimento Jonico in *Sistemi Giuridici ed Economici del Mediterraneo*, Università degli studi di Bari "Aldo Moro", Edizioni DJSGE, Taranto, 2017, vol. V, pp. 501-515.

il perimetro di tutela dei lavoratori inseriti nell'organizzazione di impresa affinché sia correttamente operato quel bilanciamento tra i principi fondamentali dell'ordinamento necessario ad impedire che il potere di iniziativa dell'imprenditore non si svolga in contrasto con l'utilità sociale o in modo da recare danno alla sicurezza, alla libertà e alla dignità umana[3]. D'altronde, si è già lucidamente stigmatizzato come "le violazioni dei diritti di libertà consumate nelle aziende non avvengono tanto nel segno dell'autonomia contrattuale, ma piuttosto nel segno dell'autonomia organizzativa"[4].

Così, le nuove tecnologie dell'informazione nell'ambiente di lavoro, ormai inteso in senso lato poiché dal confine sempre meno afferrabile, consentono nuove tipologie di trattamento di dati che hanno come effetto "collaterale" quello di ampliare a dismisura le possibilità datoriali di controllo sulle attività lavorative. Tali circostanze spingono a "interrogarsi su quali debbano essere i limiti entro cui il datore di lavoro può liberamente scegliere come strutturare la sua impresa"[5].

Ormai quotidianamente, la cronaca porta alla luce casi limite in cui l'introduzione di strumentazioni tecnologiche, seppure finalizzate a soddisfare legittime esigenze aziendali appaiono lesive della dignità del lavoratore. Sensori di presenza fisica, impianti di monitoraggio a distanza, sistemi di videosorveglianza "intelligente", braccialetti indossabili per la rilevazione dei movimenti fisici e software in grado di misurare i tempi di ogni attività lavorativa: gli esempi empirici sono innumerevoli e chiariscono l'urgenza di un cambio di mentalità e di approccio alla problematica.

Gli ultimi interventi del legislatore nazionale ed europeo vanno in tale direzione, dettando una impostazione regolativa che, senza alcuna ambiguità, richiede all'operatore del diritto una valutazione integrata della disciplina lavoristica e di quella *privacy*. Innanzitutto, con il regolamento Ue n. 679/2016, il legislatore europeo ha inteso prescrivere per tutti gli stati membri gli *standard* di tutela contro le minacce ai diritti e alle libertà fondamentali dei cittadini in materia di *privacy*, costringendo i paesi membri ad uniformare e armonizzare le discipline interne. Per altro verso, la riscrittura dell'art. 4 della l. n. 300/1970 (c.d. Statuto dei lavoratori), intervenuta circa un anno prima dell'emanazione del regolamento UE, ha condizionato l'esercizio del potere di controllo al rispetto della normativa sul trattamento dei dati personali, tramite un rinvio espresso al d.lgs.

---

3 V. C. cost. 9 marzo 1989, n. 103, in *Riv. It. Dir. Lav.*, 1989, II, pag. 389.

4 Cit. U. Romagnoli, *sub art. 1*, in G. Ghezzi, F. Mancini, L. Montuschi, U. Romagnoli, *Commento allo Statuto dei diritti dei lavoratori*, Zanichelli, 1979, pag. 4.

5 Cit. V. Nuzzo, *La protezione del lavoratore dai controlli impersonali*, Editoriale Scientifica, 2018, pag. 32.

n. 196/2003 (codice "privacy")[6], operando una definitiva "saldatura" tra i due plessi normativi.

Alla luce del nuovo contesto normativo l'autonomia organizzativa e l'esercizio del potere di controllo del datore di lavoro necessitano di un'attenta ponderazione con i presidii giuridici posti a salvaguardia dei valori della persona. In assenza di formante giurisprudenziale, sono ancora numerose le incertezze interpretative che non consentono la definitiva comprensione dei limiti posti alla libertà economica del datore di lavoro.

Nel corso della trattazione si cercherà di offrire un breve resoconto dell'evoluzione normativa in materia di potere di controllo del datore di lavoro, con particolare attenzione alla regolamentazione del trattamento dei dati personali, nel tentativo di offrire soluzioni interpretative e nuove chiavi di lettura utili a determinare le regole di condotta del datore di lavoro titolare del trattamento appropriate al caso concreto. Il documento tiene conto dei pareri e delle linee di indirizzo degli organi consultivi europei per la protezione dei dati[7], nonché delle prassi decisorie dell'Autorità garante per la protezione dei dati personali italiana[8].

---

6 Il decreto è entrato in vigore il 1° gennaio 2004, ad eccezione degli articoli 156, 176, commi 3, 4 ,5 e 6, e 182, entrati in vigore il 30 luglio 2003, e da ultimo è stato modificato dal d. lgs. n. 101 del 10 agosto 2018, per esigenze di armonizzazione con il Regolamento (UE) 2016/679.

7 Le funzioni consultive e di indirizzo in materia di protezione dei dati personali venivano svolte, in vigenza della direttiva 95/46/CE, dal Gruppo di lavoro *ex* art. 29, detto anche *Working Party* art.29 (a cui ci si riferisce con l'acronimo WP29), ovvero un organismo indipendente, composto da un rappresentante delle varie autorità nazionali in materia, in ambito europeo. A seguito dell'entrata in vigore del Regolamento Europeo n. 679/2016, il WP29 è stato sostituito dal Comitato europeo per la protezione dei dati (Edbp), che è un organo europeo indipendente avente oltre alle medesime funzioni consultive e di indirizzo ulteriori compiti di garanzia della uniforme applicazione del regolamento in ambito europeo anche attraverso la promozione della cooperazione tra le autorità competenti per la protezione dei dati dell'UE. Il Comitato europeo si è riunito per la prima volta il 25 maggio 2018 approvando gli orientamenti relativi al regolamento generale sulla protezione dei dati (GDPR) forniti dal WP29, al contempo cessandone di fatto le attività.

8 Il ruolo del Garante nazionale, già centrale in forza della direttiva 95/46/CE, risulta rafforzato dal Reg. Ue n. 679/2016, in una duplice prospettiva: da un lato, per le funzioni delle quali è titolare, con riferimento ai poteri di indagine, correttivi, autorizzativi e consultivi (art. 58); dall'altro relativamente ai profili di stretta cooperazione con le Autorità degli altri Stati membri e all'istituzione del Comitato europeo (artt. 60 ss.). Il D.lgs. 196/2003, come novellato dal D.Lgs. 101/2018 allo scopo di armonizzarne le disposizioni al GDPR, prevede all'art. 154 i seguenti compiti in capo al Garante: a) controllare se i trattamenti sono effettuati nel rispetto della disciplina applicabile, anche in caso di loro cessazione e con riferimento alla conservazione dei dati di traffico; b) trattare i reclami presentati ai sensi del regolamento, e delle disposizioni del codice, anche individuando con proprio regolamento modalità specifiche per la trattazione, nonché fissando annualmente le priorità delle questioni emergenti dai reclami che potranno essere istruite nel corso dell'anno di riferimento; c) promuovere l'adozione di regole deontologiche, nei casi di cui all'articolo 2-*quater*; d) denunciare i fatti configurabili come reati perseguibili d'ufficio, dei quali viene a conoscenza nell'esercizio o a causa delle funzioni; e) trasmettere la relazione, predisposta annualmente ai sensi dell'articolo 59 del Regolamento, al Parlamento e al Governo entro il 31 maggio dell'anno

2. Il potere datoriale di controllo a distanza

È con la promulgazione della legge n. 300 del 20 maggio 1970, il cosiddetto "Statuto dei lavoratori" (da ora anche "St. Lav.") che la legislazione italiana in materia di tutela delle informazioni personali ha conosciuto la sua prima significativa innovazione[9]. L'intervento normativo rispondeva, con molti anni di anticipo rispetto alla introduzione del "Codice *privacy*", a specifiche esigenze di protezione della persona che lavora e agisce in uno spazio di vita sociale soggetto a regole di potere. L'impresa, infatti, si connota come una organizzazione di tipo gerarchico nella quale il lavoratore ha il dovere di collaborare in forza dell'effetto giuridico tipico connesso alla sottoscrizione del contratto di lavoro[10]. L'adempimento dei doveri di lavorare comporta il necessario inserimento dell'obbligato in una struttura di potere (l'organizzazione di impresa) in cui il rischio di compressione della libertà e della dignità individuale è alto, in considerazione dell'autorità legale riconosciuta al "capo dell'impresa"[11]. Nello specifico, riguardo ai principali aspetti connessi alla tutela della riservatezza del lavoratore, che di seguito ci si propone di analizzare, non si è mai dubitato che il datore di lavoro avesse il potere di controllare a distanza il lavoratore per la migliore "realizzazione del suo interesse tecnico-organizzativo"[12]. Insomma, come affermato dalla dottrina più autorevole, l'impresa "non potrà mai essere democratica", da qui la necessità di introdurre specifici contrappunti di tipo legale al

---

successivo a quello cui si riferisce; f) assicurare la tutela dei diritti e delle libertà fondamentali degli individui dando idonea attuazione al Regolamento e al presente codice; g) provvedere altresì all'espletamento dei compiti ad esso attribuiti dal diritto dell'Unione europea o dello Stato e svolgere le ulteriori funzioni previste dall'ordinamento. Per considerazioni sul ruolo del Garante, si veda V. Cuffaro, *Il diritto europeo sul trattamento dei dati personali*, in Contratto e Impresa 3/2018, pagg. 1117-1119.

9 I. Alvino, *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*, in *Labour&Law Issues*, vol. 2, n.1, 2016, pag. 8,9, ricorda come la normativa sia stata introdotta con 25 anni di anticipo rispetto alla legge n. 675 del 31 dicembre 1996 (c.d. Codice *privacy*); in proposito cfr. S. Rodotà, *Tecnologie e diritti*, Il Mulino, 1995.

10 Cfr. M. Barbieri, *L'utilizzabilità delle informazioni raccolte: il Grande Fratello può attendere (forse)*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, pag. 183.

11 È l'art. 2086 c.c. che definisce l'imprenditore come "il capo dell'impresa" e ne legittima la posizione gerarchica ("da lui dipendono gerarchicamente i suoi collaboratori"). Benché la parola "capo" sia stata epurata in via interpretativa "della sua originaria incrostazione pubblicistica, propria dell'ideologia corporativa", come affermato in modo ineccepibile da R. Voza, *La tutela del contraente forte nel diritto del lavoro*, in *Riv. It. Dir. Lav.*, fasc. 1, 2015, pag. 15, la relazione contrattuale tra l'impresa ed il lavoro "manifesta un'insopprimibile peculiarità, ossia quella di fondare e legittimare la supremazia di un contraente sull'altro e, quindi, una posizione di autorità privata o, se si preferisce, di potere privato".

12 Cit. 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*, in *Labour&Law Issues*, vol. 1, n.1, 2015, pag. III.

potere di controllo del datore di lavoro, per evitare che il lavoratore potesse essere sottoposto a controlli continui e pervasivi, sia dentro l'ambiente di lavoro che fuori[13]. Un rischio, questo, reso tangibile dal massiccio ricorso alla tecnologia nei luoghi di lavoro[14].
La *ratio* della norma statutaria del 1970 si rinviene nella risposta a tali bisogni di protezione tramite la limitazione dell'esercizio del potere di controllo. Infatti, benché ne riconosca per la prima volta in modo formale l'esistenza in capo al datore di lavoro, lo Statuto dei lavoratori ne prescrive le ipotesi di divieto e detta un suo preciso regime vincolistico.
Innanzitutto, il legislatore statutario ha dichiarato illegittimi i controlli che esulano dall'ambito funzionale del rapporto di lavoro, vietando senza eccezioni ogni accertamento datoriale, sia in fase preassuntiva che nel corso dello svolgimento del rapporto, "sulla idoneità e sulla infermità per malattia o infortunio del lavoratore dipendente" (v. art. 5, St. Lav.), "sulle opinioni politiche, religiose o sindacali del lavoratore, nonché su fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore" (v. art. 8, St. Lav.), persino, andando oltre la protezione di quelli che decenni dopo saranno chiamati "dati sensibili"[15].
In secondo luogo, è fatto obbligo a ciascun datore di lavoro di comunicare ai lavoratori interessati i nominativi e le mansioni specifiche del personale addetto alla vigilanza dell'attività lavorativa, così vietando i controlli personali di tipo occulto.
Infine, in ambito funzionale, la disciplina statutaria (*ex* art. 4 St. Lav. *ante* novella), ha previsto il divieto di predisporre impianti aventi per finalità "diretta" il controllo a distanza dei lavoratori, mentre ha subordinato le forme di controllo "indiretto" alla presenza di interessi meritevoli del datore di lavoro. Il legislatore avrebbe "disegnato una tassonomia funzionale dei dispositivi utilizzabili dal datore di lavoro", al contempo assoggettandone l'installazione ad un regime autorizzatorio incentrato essenzialmente sul controllo sindacale o, in mancanza, amministrativo[16]. L'art. 4 della legge n. 300/1970, dunque, condensa il giudizio di disvalore rispetto ai controlli condotti a distanza effettuati per

13 Cit. U. Romagnoli, *Il lavoro in Italia. Un giurista racconta*, il Mulino, 1995, pag. 156, secondo l'A. l'inversione dei ruoli tra governo e opposizione nell'impresa è impossibile.

14 Fra i numerosi casi denunciati dalla cronaca in passato, destò scalpore l'attività di controllo realizzata dalla Fiat negli anni '50 e '60 attraverso uno specifico organo di vigilanza deputato alla raccolta di informazioni di ogni genere sui propri dipendenti, sugli aspiranti tali, oltre che su chiunque si trovasse ad avere con la Fiat rapporti politici e commerciali. Per un approfondimento sul caso cfr. B. Giudetti Serra, *Le schedature Fiat. Cronaca di un processo e altre cronache*, Rosenberg & Sellier, 1984.

15 L'osservazione puntuale è di M. Barbieri, *op. cit.*, pag. 184, che pone in risalto la lungimiranza del legislatore statutario nel garantire ai lavoratori il diritto alla riservatezza.

16 Così V. Nuzzo, *op. cit.*, pag. 34, definisce la funzionalizzazione degli strumenti (dai quali possa derivare come effetto collaterale il controllo dei lavoratori) al soddisfacimento degli interessi aziendali qualificati.

il tramite di dispositivi tecnologici che, proprio a causa della loro impersonalità, sono percepiti come invasivi e potenzialmente lesivi della dignità umana[17]. La disposizione statutaria, però, ha mostrato con l'andare del tempo i suoi limiti, considerato che il sistema di garanzia con essa istituito si limitava di fatto a prescrivere l'accordo sindacale o il provvedimento autorizzativo della Direzione provinciale del lavoro (ora della Direzione territoriale dell'Ispettorato nazionale del lavoro), quale condizione di legittimità dei controlli datoriali a distanza, senza prevedere specifiche misure di prevenzione degli abusi della *privacy*[18].

La disciplina legale, infatti, configurava tuttalpiù la possibilità che l'accordo o il provvedimento potessero prevedere prescrizioni riguardo l'uso degli strumenti e degli impianti (non finalizzati al controllo diretto dei lavoratori ma comunque idonei a realizzarlo), ma nulla sulla modalità di trattamento dei dati personali raccolti. Sotto questo aspetto, l'art. 4, St. Lav., si era mostrato inadatto ai bisogni di protezione del lavoratore, in quanto la neutralizzazione di ogni effetto giuridico negativo delle azioni (disciplinari) del datore di lavoro nei confronti del lavoratore, quale esito dell'illegittimo (perché non autorizzato) controllo a distanza datoriale, non ha offerto garanzie sufficienti a tutelare la riservatezza del lavoratore e si è mostrato rimedio efficace soltanto sul piano individuale del rapporto di lavoro[19].

L'evoluzione del contesto tecnologico durante i decenni successivi alla introduzione dello Statuto dei lavoratori ha reso inevitabile un ripensamento della disciplina regolativa in tema di controlli sia per l'incapacità della norma legale di "intercettare" le nuove forme di controllo sia per la necessità di una armonizzazione alle disposizioni del codice *privacy*. L'inadeguatezza della norma storica appare di tutta evidenza se soltanto si considera che, con riferimento a specifiche mansioni, le nuove strumentazioni sono reputate con sempre maggiore frequenza indispensabili per l'esecuzione della prestazione lavorativa. In tali casi, si era sostenuta l'inapplicabilità dell'originario art. 4, St. Lav., che

---

17 Per un approfondimento sull'originaria disciplina statutaria, *ex pluris* cfr. B. Veneziani, *I controlli dell'imprenditore ed il contratto di lavoro*, Cacucci, 1975; G. Pera, Art. 4, in C. Assanti, G. Pera (a cura di), *Commento allo Statuto dei diritti dei lavoratori*, Padova, 1972; D. Napoletano, *Lo Statuto dei lavoratori*, Napoli, 1971; R. De Luca Tamajo, R. Imperiali D'Afflitto, C. Pisani, R. Romei, *Nuove tecnologie e tutela della riservatezza del lavoratore*, Franco Angeli, 1988; A. Bellavista, *Il controllo sui lavoratori*, Giappichelli, 1995.

18 A. Maresca, *Controlli tecnologici e tutele del lavoratore nel nuovo art. 4 St. lav.*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, pag. 3 ss., parla di "malfunzionamento" dell'originario art. 4 St. lav. e di "declino" della tecnica di tutela della riservatezza del lavoratore affidata all'accordo sindacale; per una trattazione *ex professo* dei profili *privacy* nella gestione del rapporto di lavoro cfr. M.P. Aimo, *Privacy, libertà di espressione e rapporto di lavoro*, Jovene, 2003; P. Chieco, *Privacy e lavoro*, Cacucci, 2000.

19 Per A. Maresca, *op. cit.*, pag. 2, le modalità di realizzazione della tutela statutaria finivano per trascurare l'interesse della generalità dei dipendenti alla loro riservatezza in sé stessa considerata.

sembrava assoggettare al regime vincolistico esclusivamente l'uso di apparecchiature estranee al rapporto di lavoro e, quindi, non quelle indispensabili a rendere la prestazione[20]. È fuori di dubbio che gli strumenti informatici e i servizi di comunicazione elettronica siano ormai diffusi nei più disparati contesti lavorativi e adoperati per il corretto svolgimento della prestazione di lavoro. Sono strumenti che, oltre ad assolvere alla loro funzione in vista del corretto adempimento della prestazione, rendono anche possibile il monitoraggio costante delle attività lavorative nonché l'immagazzinamento di grandi quantità di dati sugli utilizzatori, accentuando di gran misura il rischio per il lavoratore di essere sottoposto a controlli occulti ed "invasivi"[21].

Tali criticità non hanno reso ulteriormente differibile un intervento di *restyling* normativo, giunto a distanza di quarantacinque anni dall'introduzione della norma statutaria in materia di controlli a distanza, con una completa riformulazione del testo legale in occasione dell'ampio disegno riformatore, avviato con la legge delega n. 183/2014 e attuato da una pluralità di successivi decreti legislativi (c.d. "Jobs Act")[22].

Nello specifico, la completa riscrittura dell'art. 4 della legge n. 300 del 1970 è stata operata dall'art. 23, co.1, del d. lgs. n. 151/2015, che ha realizzato un nuovo bilanciamento tra l'interesse tecnico produttivo del datore di lavoro a controllare il puntuale adempimento della prestazione lavorativa e l'interesse alla dignità ed alla riservatezza del lavoratore sancito dalla nostra Carta costituzionale (art. 2 ed art. 41, comma 2, Cost.), dalla Convenzione europea per la salvaguardia dei diritti dell'uomo e delle libertà fondamentali (art. 8 CEDU) e dal Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (c.d. "GDPR")[23].

---

20 I. Alvino, *op. cit.*, pag. 5.

21 Per L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *RIDL*, 2016, I, 345, nei contesti lavorativi si assiste alla diffusione di meccanismi di vigilanza fisicamente meno invadenti, ma complessivamente più invasivi; per un approfondimento sui nuovi strumenti di controllo elettronici cfr. C. Carta, *I limiti al potere di controllo sui lavoratori nell'uso di internet e dei servizi di comunicazione elettronica: per un diritto alla moderazione*, in *Labor*, 2, 2018, 175.

22 Per la loro compiuta disamina cfr. Balletti E., Garofalo D. (a cura di), *La riforma della cassa integrazione guadagni nel Jobs act 2*, Cacucci, Bari, 2016; Ghera E., Garofalo D. (a cura di), *Organizzazione e disciplina del mercato del lavoro nel Jobs act 2*, Cacucci, Bari, 2016; Ghera E., Garofalo D. (a cura di), *Semplificazioni–sanzioni–ispezioni nel Jobs act 2*, Cacucci, Bari, 2016; Ghera E. – Garofalo D. (a cura di), *Le tutele per i licenziamenti e per la disoccupazione involontaria nel Jobs act 2*, Cacucci, Bari, 2015.

23 Invero, il diritto alla riservatezza non ha una formulazione espressa nella Carta costituzionale italiana e la sua classificazione fra i diritti fondamentali si ricava dall'interpretazione sistematica dei principi costituzionali inerenti i diritti dell'uomo. Per un approfondimento v. L. Califano, *Tecnologie di controllo del lavoro, diritto alla riservatezza*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, pag. 166 ss.

2.1. L'art. 4 St. lav. riformato: limiti interni/esterni, semplificazione del regime autorizzatorio e utilizzabilità dei dati

Il nuovo articolo 4, St. Lav., consta di due nuclei regolativi, il primo attinente all'utilizzo degli strumenti di controllo, tradotto nei commi 1 e 2, ed il secondo al trattamento dei dati raccolti, tradotto nel comma 3[24]. Il legislatore ha innovato sensibilmente la disciplina in una prospettiva di semplificazione, orientando la propria azione riformatrice anche sulla base degli approdi giurisprudenziali consolidatisi in materia.

Nella disciplina statutaria riformata non si rinviene più un divieto espresso, a carattere generale e assoluto, di uso di strumentazione tecnologica per finalità di controllo a distanza dell'attività dei lavoratori[25]. La sua riformulazione impone una riflessione su una serie di questioni interpretative sulla persistenza di un divieto assoluto di controllo dell'attività del lavoratore, con particolare riguardo all'adempimento della prestazione di lavoro, e sulla valenza delle categorie dottrinali del controllo "diretto" e "indiretto", elaborate in vigenza della norma storica.

Sotto il primo profilo, non sembra dubitabile che il legislatore abbia inteso affermare, seppure implicitamente, l'esistenza di un generale divieto di controllo a distanza del lavoratore attraverso la prescrizione di uno specifico limite esterno alla installazione di apparecchiature finalizzate esclusivamente al controllo del personale dipendente[26]. Ai sensi del comma 1, dell'art. 4, St. Lav., infatti, l'impiego di impianti audiovisivi e altri strumenti dai quali derivi – come effetto collaterale – la possibilità di controllo a distanza dell'attività dei lavoratori è ammesso soltanto in presenza di esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale e la loro installazione può avvenire soltanto previo positivo esperimento della procedura sindacale codeterminativa o dietro autorizzazione amministrativa dell'Ispettorato nazionale del lavoro.

---

24 Per un primo commento all'art. 4 novellato, cfr. anche E. Balletti, *I controlli a distanza dei lavoratori dopo il jobs act*, in F. Santoni, M. Ricci, R. Santucci (a cura di), *Il diritto del lavoro all'epoca del jobs act*, Edizioni Scientifiche Italiane, 2016, pag. 37 ss.; A. Bellavista, *Il nuovo art. 4 dello Statuto dei lavoratori*, in G. Zilio Grandi, M. Biasi, *Commentario breve alla riforma del "Jobs Act"*, 2016, pag. 717 ss.; R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro (art. 23 d.lgs. n. 151/2015)*, in *Riv. It. Dir. Lav.*, 2016, 1, I, pag. 77 ss.; V. Maio, *La nuova disciplina dei controlli a distanza sull'attività dei lavoratori e la modernità post panottica*, in *Arg. Dir. Lav.*, 2015, 6, pag. 1186 ss.; M. T. Salimbeni, *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, in *Riv. It. Dir. Lav.*, 2015, 4, I, pag. 589 ss.

25 M. T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in P. Tullini, *op. cit.*, pag. 46, 47, ricorda come, secondo l'originaria formula statutaria, la generalità del divieto implicasse l'impossibilità dell'attività di controllo, in senso ampio, sia dell'attività di adempimento della prestazione sia del comportamento complessivamente tenuto dal lavoratore.

26 L'esistenza di un divieto generale dell'attività di controllo a distanza dei lavoratori è affermata da R. Del Punta, *op. cit.*, pag. 96; I. Alvino, *op. cit.*, pag. 16; V. Maio, *op. cit.*, pag. 1190; M. T. Salimbeni, *op. cit.*, pag. 602.

La regola di carattere generale, però, non trova applicazione con riferimento alla introduzione degli "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e agli strumenti di registrazione degli accessi e delle presenze", ai sensi dell'art.4, co.2, St. Lav. Se ci si limitasse al tenore letterale della norma, la deroga sembrerebbe mettere in discussione il carattere di "assolutezza" del divieto di controllo "diretto" sull'esatto adempimento della prestazione del lavoratore, circostanza che, ai sensi dell'originaria formula dell'art. 4, St. Lav., è sempre stata respinta dalla dottrina maggioritaria[27].

Così ragionando, le possibilità di controllo del lavoratore sarebbero differenziate a seconda della tipologia di strumenti tecnologici adoperati. Infatti, nel caso degli strumenti di cui al co.1, art. 4, St. Lav., sarebbe ammissibile il controllo a distanza delle attività espletate dal lavoratore in adempimento della obbligazione di lavoro soltanto qualora questo avvenga in modo "indiretto" o "preterintenzionale", in considerazione dello specifico regime vincolistico che impone una ineliminabile connessione funzionale tra la strumentazione tecnologica e le qualificate esigenze aziendali che consentono l'installazione degli impianti[28].

Diversamente, il controllo di tipo diretto del corretto espletamento delle mansioni lavorative sarebbe ammissibile qualora operato mediante gli strumenti tecnologici affidati al lavoratore e necessari per l'esecuzione della prestazione lavorativa, richiamati dal co.2, art. 4, St. Lav., grazie alla utilizzabilità delle informazioni raccolte a tutti i fini connessi al rapporto di lavoro, sancita dall'art.4, comma 3, St. Lav[29]. I dispositivi tecnologici, dunque, per il sol fatto di essere adoperati come strumenti di lavoro amplierebbero a dismisura le possibilità di controllo del datore di lavoro, consentendo un controllo impersonale continuativo in grado di esporre i lavoratori a indebite "esasperazioni di tipo stacanovistico"[30]. Invero, la tesi appena esposta appare troppo legata al tenore letterale della norma e non tiene in debito conto il mutato scenario giuridico in materia di riservatezza e trattamento dei dati personali.

---

27 V. M.T. Carinci, *ibidem*, e la dottrina ivi richiamata.

28 La definizione di controllo "preterintenzionale" è da attribuire a U. Romagnoli, Art. 4, in G. Ghezzi, F. Mancini, L. Montuschi, U. Romagnoli, *Statuto dei lavoratori*, 1979, pagg. 28, 29; il concetto di controllo "preterintenzionale" deve essere oggetto di opportuno discernimento, in considerazione del fatto che la legittimità del controllo tecnologico non dipende da un'indagine sull'elemento soggettivo del datore di lavoro che lo realizza, sul punto v. R. Del Punta, *La nuova disciplina dei controlli a distanza sul lavoro*, in *Riv. It. Dir. Lav.*, 2016, n. 1, pag. 81.

29 La tesi è sostenuta da M. T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in P. Tullini, *op. cit.*, pag. 55; non esclude la legittimità di controlli di tipo diretto A. Maresca, *op. cit.*, pag. 6, 7; per M. Marazza, *op. cit.*, pag. 16, ipotizza in estremo la possibilità di controllo diretto della prestazione lavorativa per finalità di tutela del patrimonio aziendale.

30 In questi termini G. Pera, Art. 4, (*Impianti audiovisivi*), in C. Assanti, G. Pera (a cura di), *Commento allo Statuto dei diritti dei lavoratori*, Cedam, 1972, pag. 25, sulla ratio del divieto di cui all'art. 4, St. Lav.

La permanenza nell'ordinamento di un divieto di controllo diretto di carattere generale ed assoluto è stata sostenuta in modo convincente, ponendo in evidenza la necessità di una interpretazione sistematica e adeguatrice della disposizione statutaria, conforme alla disciplina europea in materia *privacy* e ai principi costituzionali[31]. Il regolamento UE n. 2016/679 ha fissato i principi generali del trattamento dei dati personali, prescrivendo che la raccolta delle informazioni avvenga per finalità determinate, esplicite e legittime, chiarendo al contempo che i dati debbano essere trattati in modo non incompatibile con tali finalità. È bene ricordare che la norma regolamentare è direttamente applicabile nell'ordinamento interno e l'affermazione del principio di "finalità", con tutta evidenza, incrocia la disposizione di cui al comma 3, art. 4, St. Lav., che dichiara l'utilizzabilità "a tutti i fini connessi al rapporto di lavoro" delle informazioni raccolte dal datore di lavoro. Seppure sia possibile ipotizzare che il legislatore nazionale, con la formula di cui al comma 3, art. 4, St. lav., abbia mirato alla liberalizzazione di determinate categorie di strumentazioni tecnologiche in ambito lavorativo, l'intervenuto regolamento UE ed i principi generali da esso sanciti non possono essere derogati da una norma di diritto interno[32].
A favore dell'impossibilità di effettuazione di controlli diretti sulla prestazione lavorativa milita la lettura combinata del divieto di controlli "personali" occulti sancito dall'art. 3 con il divieto di controlli "impersonali", quandanche palesi, sancito dall'art. 4, comma 1, St. Lav. Dalla lettura unitaria delle disposizioni normative si deve arguire che al datore di lavoro sia concesso unicamente di effettuare controlli diretti sulla prestazione di lavoro attraverso personale addetto ad attività di vigilanza[33].
Affermata la permanenza del divieto di controllo di tipo "diretto" anche in relazione agli strumenti di cui al comma 2, art. 4, St. Lav., occorre altresì prendere atto della persistente legittimità dei controlli effettuati in modo "preterintenzionale". In proposito, non sembra dubbio che il datore di lavoro abbia diritto di monitorare il corretto utilizzo degli strumenti lavorativi affidati al personale dipendente, per il soddisfacimento del proprio interesse organizzativo e di tutela del patrimonio aziendale. Dall'attività di controllo potrebbero essere rilevate accidentalmente informazioni circa inadempimenti o comportamenti negligenti che, pur sempre nel rispetto dei principi *privacy* e del diritto del lavo-

---

31 Cfr. V. Pinto, *La flessibilità funzionale e i poteri del datore di lavoro. Prime considerazioni sui decreti attuativi del c.d. Jobs act e sul lavoro agile*, in *Riv. Giur. Lav.*, 2016, I, pag. 348; propende per una interpretazione sistematica e adeguatrice anche V. Nuzzo, *op. cit.*, pag. 104 ss.

32 In tal senso V. Pinto, *I controlli "difensivi" del datore di lavoro sule attività informatiche e telematiche del lavoratore*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, pag. 183; dello stesso avviso anche V. Nuzzo, *op. cit.*, pag. 106, 107, che argomenta in modo ampio e circostanziato sulla incidenza dei principi generali in materia di trattamento dati radicati nel diritto sovranazionale.

33 V. Nuzzo, *op. ult. cit.*, pag. 107, che altresì richiama a sostegno la Raccomandazione del Consiglio di Europa CM/Rec(2015)5.

ratore all'autodeterminazione informativa, potranno essere utilizzate a fini connessi al rapporto di lavoro (ad es. sul piano disciplinare). Sotto questo punto di vista, non si può tacere che la possibilità di monitorare il corretto uso degli strumenti di lavoro implica, in un certo senso, l'esercizio di una forma di controllo sulle modalità di adempimento della prestazione lavorativa. Infatti, a differenza degli strumenti di cui al comma 1, art. 4, St. Lav., i dispositivi di cui al comma 2 sono affidati in uso dai lavoratori, cosicché il controllo conseguente all'attività di monitoraggio degli strumenti sarà un controllo "soggettivizzato". In altre parole, il controllo sulla organizzazione di lavoro operato attraverso il monitoraggio degli strumenti affidati al personale per l'esecuzione della prestazione potrebbe implicare un contestuale accertamento sul corretto/scorretto adempimento dell'obbligazione lavorativa di cui può sostenersi la legittimità. È di tutta evidenza, però, che simili forme di controllo datoriale sull'adempimento della prestazione non potranno travalicare la limitata verifica delle modalità di impiego dello strumento di lavoro.

2.1.1. I vincoli procedurali

La legittimità del controllo sull'attività del lavoratore, ammessa dal primo nucleo regolativo del novellato art. 4, St. Lav., è condizionata al rispetto di precisi limiti interni al potere organizzativo e di controllo del datore di lavoro. Ai sensi del primo comma dell'art. 4, tali limiti sono espressi dalla sussistenza delle menzionate specifiche esigenze aziendali che ammettono l'installazione e l'impiego della strumentazione dalla quale possa derivare il controllo (indiretto) del lavoratore. Il secondo comma dell'art. 4, invece, ammette il controllo "collaterale" del lavoratore attraverso strumenti di lavoro che, in quanto tali, sono soggetti a limite di scopo comprovabile dalla loro oggettiva funzionalizzazione alla esecuzione delle mansioni assegnate e affrancati dalla procedura del comma 1[34].
Nei soli casi di controllo indiretto previsti dal comma 1, art. 4, la sussistenza delle ragioni aziendali è verificata in via preliminare attraverso il rispetto di vincoli procedurali nell'ambito dei quali le esigenze qualificate dovranno essere formalmente specificate[35].

---

34 Per M. T. Carinci, *Il controllo a distanza sull'adempimento della prestazione di lavoro*, in P. Tullini, *op. cit.*, pag. 54, 55, il controllo diretto del lavoratore è adesso pienamente conforme alla legge quanto effettuato tramite strumenti di lavoro.

35 Con circolare n. 302 del 18 giugno 2018, l'Ispettorato nazionale del lavoro ha chiarito che "nel caso di richieste di autorizzazione legate ad esigenze di "sicurezza del lavoro", vadano puntualmente evidenziate le motivazioni di natura prevenzionistica che sono alla base dell'installazione di impianti audiovisivi e altri strumenti di potenziale controllo a distanza dei lavoratori corredate da una apposita documentazione di supporto. Più specificatamente appare necessario che le affermate necessità legate alla sicurezza del lavoro trovino adeguato riscontro nell'attività di valutazione dei rischi effettuata dal datore di lavoro e formalizzata nell'apposito documento (DVR)". In precedenza l'INL, con nota n.299 del 28 novembre 2017, in ipotesi di richiesta di autorizzazione all'installazione di impianti per ragioni inerenti alla tutela del patrimonio, ha precisato che "questi ultimi, essendo

Il potere di controllo del datore di lavoro, così, viene procedimentalizzato attraverso un meccanismo giuridico in grado di contemperare le esigenze aziendali con i bisogni di protezione del lavoratore[36]. Sotto questo profilo il nuovo art. 4, St. Lav., ripropone con qualche semplificazione il regime autorizzatorio preesistente[37]. L'installazione degli strumenti di controllo, infatti, continua ad essere subordinata alla preventiva stipula di un accordo collettivo tra datore di lavoro e rappresentanze sindacali unitarie (r.s.u.) o aziendali (r.s.a.). In mancanza di accordo, dovuto all'impossibile raggiungimento di una intesa oppure all'assenza di rappresentanze sindacali in azienda, gli impianti e gli strumenti possono essere installati previa autorizzazione della sede territoriale dell'Ispettorato nazionale del lavoro[38]. La semplificazione legale è prevista per le imprese multilocalizzate, ovvero con unità produttive ubicate in più province o regioni, per le quali è adesso prevista la possibilità di sottoscrivere l'accordo autorizzatorio con le associazioni sindacali comparativamente più rappresentative sul piano nazionale. La possibilità di attivare livelli superiori di contrattazione non era compendiata dalla previgente normativa e, secondo la giurisprudenza, non era sostenibile neppure in via interpretativa mancando un espresso richiamo legale ad un accordo autorizzatorio unico. Alla luce della novella, le imprese multilocalizzate non sono più costrette al raggiungimento di intese preventive con le rappresentanze sindacali aziendali di ciascuna unità produttiva dislocata sul territorio nazionale. L'attuale formula dell'art. 4, St. Lav., innova in chiave

---

evidentemente finalizzati alla tutela del patrimonio aziendale, trovano la loro legittimazione nella previsione di cui al primo comma del citato art. 4. Quanto alle modalità operative va tenuto presente che, qualora le videocamere o fotocamere si attivino esclusivamente con l'impianto di allarme inserito, non sussiste alcuna possibilità di controllo "preterintenzionale" sul personale e pertanto non vi sono motivi ostativi al rilascio del provvedimento. Conseguentemente, in relazione alla evidente esigenza di celerità nell'attivazione dei predetti impianti, si invitano codesti Uffici a rilasciare il provvedimento autorizzativo in tempi assolutamente rapidi stante l'inesistenza di qualunque valutazione istruttoria".

36 V. Alvino, *op. cit.*, pag. 17.

37 L'Ispettorato nazionale del lavoro, con lettera circolare n. 1881 del 25 febbraio 2019, in materia di modifica degli assetti proprietari e di titolarità dell'impresa, ha precisato che "il mero "subentro" di un'impresa in locali già dotati degli impianti/strumenti in premessa non integra di per sé profili di illegittimità qualora gli impianti/strumenti stessi siano stati installati osservando le procedure (accordo collettivo o autorizzazione) previste dall'art. 4 della L. n. 300/1970 e non siano intervenuti mutamenti: - dei presupposti legittimanti (esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale); - delle modalità di funzionamento. Anche al fine di consentire un efficace svolgimento di eventuali iniziative ispettive, si ritiene pertanto opportuno che, nei casi in esame, il titolare subentrante: - comunichi all'Ufficio che l'ha rilasciato gli estremi del provvedimento di autorizzazione alla installazione degli impianti; - renda dichiarazione con la quale attesti che, con il cambio di titolarità, non sono mutati né i presupposti legittimanti il suo rilascio, né le modalità di uso dell'impianto audiovisivo o dello strumento autorizzato".

38 In alternativa, nel caso di imprese con unità produttive dislocate negli ambiti di competenza di più sedi territoriali, l'autorizzazione può essere rilasciata dalla sede centrale dell'Ispettorato nazionale del lavoro.

semplificatoria il procedimento autorizzativo anche delle imprese con unità produttive nelle quali manchino rappresentanze sindacali aziendali e che siano dislocate negli ambiti di competenza di più sedi territoriali dell'Ispettorato nazionale del lavoro. In tal caso i datori di lavoro potranno avanzare istanza di autorizzazione alla sede centrale dell'Ispettorato nazionale del lavoro[39].

Come si diceva, però, la disciplina riformata opera una inedita differenziazione dei regimi vincolistici in base alla diversa tipologia di strumento dalla cui utilizzazione si possano realizzare forme di controllo sui lavoratori. In particolare, il comma 2 dell'art. 4, St. Lav., esclude l'applicabilità delle prescrizioni in materia di autorizzazione preventiva all'installazione di tutti gli strumenti "utilizzati dal lavoratore per rendere la prestazione lavorativa" e degli "strumenti di registrazione degli accessi e delle presenze".

Alla luce della suddetta disposizione, è possibile individuare una sotto-categoria di strumenti attraverso cui è possibile esercitare forme di controllo sui lavoratori, ricavabile come *species* da quella degli "strumenti di controllo" (*ex* co. 1, art. 4, St. Lav.), alla quale afferiscono gli "strumenti di lavoro" che al tempo stesso consentono un controllo a distanza (*ex* co.2, art. 4, St. Lav.)[40]. La differente previsione normativa per le due categorie trova fondamento nella diversità dei poteri che ne consentono la predisposizione, oltre che nella diversa funzione a cui assolvono gli strumenti tecnologici[41]. Infatti, l'introduzione degli "strumenti di lavoro" è espressione dell'esercizio del potere di "organizzazione del lavoro" che il datore di lavoro acquisisce con la sottoscrizione del contratto e che, come altra faccia della medaglia, implica l'assunzione di precisi doveri per il lavoratore, tra cui l'obbligo di osservanza. Differentemente, l'installazione di "strumenti di controllo" (ai sensi dell'art. 4, co. 1, St. Lav.) trova radicamento nel diritto reale dell'imprenditore all'organizzazione della propria attività e, dunque, prescinde dal contratto di lavoro. L'autorità del datore di lavoro, infatti, si riverbera in ogni "frazione dell'organizzazione complessiva nella quale il prestatore di lavoro si trova inserito"[42].

---

39 L'Ispettorato nazionale del lavoro, con risposta ad interpello n.3/2019, ha chiarito che il silenzio dell'organo amministrativo adito non si configura come "silenzio assenso" poiché la disciplina legale statutaria, in mancanza di accordo con le rappresentanze sindacali aziendali, condiziona inderogabilmente l'installazione degli impianti di controllo ad un provvedimento autorizzativo espresso.

40 La distinzione è operata da M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, in WP CSDLE "Massimo D'Antona".IT – 300/2016, pag. 9, 10.

41 La distinzione giuridica tra potere di organizzazione dell'attività e potere di organizzazione del lavoro è ben tratteggiata da M. Marazza, *Limiti e tecniche di controllo sui poteri di organizzazione del datore di lavoro*, in *Contratto di lavoro e organizzazione*, Volume quarto, Tomo secondo, *Trattato di diritto del lavoro*, diretto da Mattia Persiani e Franco Carinci, 2012, pag. 1272.

42 La tesi è teorizzata in modo convincente da F. Liso, *La mobilità del lavoratore in azienda: il quadro legale*, Giuffrè, 1982, pag. 59, poi ripresa e sostenuta da R. Voza, *op. cit.*, pag. 16.

Se ne deduce che l'esercizio dei poteri sia stato oggetto di un diverso apprezzamento da parte del legislatore che, condivisibilmente, ha ritenuto di assoggettare ad una disciplina limitativa meno stringente l'impiego degli strumenti che sono espressione "di una funzionalità intrinseca ed ineliminabile dell'organizzazione del lavoro", quandanche questi consentano forme di controllo sull'utilizzatore[43].

2.1.2. Gli strumenti di lavoro, registrazione delle presenze e controllo degli accessi

Il *punctum dolens* della semplificazione legale dei vincoli procedurali alla installazione degli strumenti tecnologici di lavoro è l'assenza nel dettato normativo di criteri univoci volti alla individuazione degli strumenti esenti dal controllo sindacale e amministrativo. A causa della formula "lasca" dell'art. 4, comma 2, St. Lav., che si riferisce genericamente agli strumenti "utilizzati dal lavoratore per rendere la prestazione lavorativa" e agli "strumenti di registrazione degli accessi e delle presenze", infatti, la loro classificazione è affidata ai datori di lavoro che dovranno operare una prudente valutazione degli strumenti tecnologici affidati ai propri dipendenti. Infatti, qualora la strumentazione consenta forme di controllo sull'attività del lavoratore, soltanto la verifica di una stretta correlazione tra questa e le mansioni da svolgere potrà legittimarne l'impiego libero[44]. Poiché, però, appare fuori di dubbio che il procedimento valutativo possa, in caso di contestazioni, divenire oggetto di accertamento giudiziale, è necessario che i datori di lavoro adottino un comportamento prudente in considerazione delle conseguenze derivanti dall'errata valutazione delle condizioni di esenzione dal regime concertativo-autorizzativo. In tale ipotesi, infatti, la illiceità dell'impiego degli strumenti tecnologici esporrebbe il datore di lavoro alla sanzione di carattere penale prevista dall'art. 38 St. Lav., e, contestualmente, renderebbe illegittimo il trattamento dei dati personali operato per loro tramite.
Tra i mezzi che ciascun imprenditore reputa più idonei alla esecuzione della prestazione di lavoro e che ha ampia facoltà di assegnare in uso al proprio personale, soltanto quelli strettamente funzionali all'espletamento delle mansioni di ciascun lavoratore potranno beneficiare del regime di impiego semplificato. In questa prospettiva, nell'ampia gamma di mezzi tecnologici affidati in uso ai lavoratori sarà possibile distinguere gli strumenti

---

43 Cit. M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, *op. cit.*, pag. 12; v. anche A. Maresca, *op. cit.*, pag. 7, secondo cui "i controlli dell'attività lavorativa riconducibili al co. 2 dell'art. 4 sono effettuati da strumenti che (...) non possono per la loro stessa natura e funzione essere assoggettati ad una causale o motivazione che ne giustifica l'utilizzo"; A. Maresca, *op. cit.*, pag. 15, evidenzia come non vi sia una differenziazione ontologica tra le due categorie di strumenti, ovvero la loro distinzione si coglie guardando la loro funzione e non le loro caratteristiche oggettive.

44 Così R. Del Punta, *op. cit.*, pag. 100; M. Russo, *op. cit.*, pag. 15.

di lavoro utilizzati per il soddisfacimento di esigenze organizzative aziendali, la cui introduzione resta assoggettata al rispetto dei vincoli procedurali, dagli strumenti utilizzati esclusivamente per rendere la prestazione lavorativa riconducibili all'art. 4, comma 2, St. Lav. Tale distinzione assume rilevanza in particolar modo con riferimento agli strumenti informatici (si pensi ai personal computer) dotati di un complesso sistema di software. Tutte le funzionalità software, infatti, dovranno essere oggetto di specifico procedimento di valutazione in ordine alla stretta correlazione con le mansioni svolte dal dipendente che se ne avvale. Qualora il software (o una sua parte) non risulti esclusivamente preordinato allo svolgimento della prestazione lavorativa, il datore di lavoro sarà tenuto, oltre alla disciplina di protezione dei dati, al rispetto delle procedure di cui all'art. 4, comma 1, St. Lav. La circostanza dovrà ritenersi verificata ogniqualvolta il sistema risponda esclusivamente a specifiche esigenze organizzative e produttive della società, si pensi alla necessità di migliorare la qualità del servizio alla clientela o alla necessità di migliorare le performance del lavoratore, anche attraverso la prevenzione di errori[45].

Nel circoscrivere l'ambito della semplificazione degli obblighi procedurali, il legislatore vi ha ricompreso, oltre agli strumenti di lavoro, anche i dispositivi "di registrazione degli accessi e delle presenze". L'estensione positiva del regime semplificato anche agli strumenti volti a verificare il rispetto dell'orario di lavoro supera definitivamente la querelle ermeneutica, sorta sulla precedente formulazione legale, tra quanti ne sostenevano l'assoggettamento alla procedura autorizzatoria statutaria e quanti reputavano il loro impiego estraneo all'applicazione dell'art. 4 St. Lav. in base alla circostanza che il divieto di controllare a distanza le attività fosse esclusivamente riferito allo svolgimento delle mansioni e non anche alla rilevazione del quantum della prestazione[46]. A causa della laconica formulazione della disposizione di legge, però, non è chiaro se il comma 2, art. 4, St. Lav., debba ritenersi limitato ai soli dispositivi di rilevazione dell'ingresso e dell'uscita del lavoratore all'inizio e al termine del suo turno lavorativo, oppure riferito anche ad altri strumenti di rilevazione degli accessi e della presenza fisica durante l'orario di lavoro[47]. Invero, la disposizione legale sembra consentire una interpretazione maggior-

45 Offre interessanti spunti di riflessione l'argomentazione elaborata dal Garante per la protezione dei dati personali nel provvedimento n. 139 dell'8 marzo 2019, *Trattamento dei dati personali dei dipendenti di un call center*, nel quale si opera un'analisi delle funzionalità software in uso ai telefonisti, accertandone l'assoggettamento ai vincoli procedurali statutari in considerazione della loro predisposizione per soddisfare esclusivamente un'esigenza organizzativa del datore di lavoro.

46 V. Cass. 17 luglio 2007, n. 15892, in Riv. It. Dir. Lav., II, 2008, pag. 726, con nota di M. Vallauri, *È davvero incontenibile la forza espansiva dell'art. 4 dello statuto dei lavoratori?*

47 È favorevole ad una interpretazione restrittiva M. T. Salimbeni, *La riforma dell'articolo 4 dello Statuto dei lavoratori: l'ambigua risolutezza del legislatore*, *op. cit.*, pag. 609, 610; in senso conforme anche E. Raimondi, *op. cit.*, pag. 81

mente estensiva purché rispettosa del principio di istantaneità del controllo. Così, se dalla fattispecie legale è palese debbano escludersi tutti i dispositivi che consentono il tracciamento continuativo degli spostamenti fisici dei lavoratori, diversamente, potranno ad essa essere ricondotti gli strumenti di registrazione degli accessi in aree aziendali riservate in cui l'ingresso è ammesso soltanto al personale autorizzato[48]. L'introduzione in azienda di questi dispositivi, però, nonostante la disapplicazione del comma 1, art. 4, St. Lav., non può ritenersi affidata al mero arbitrio del datore di lavoro, visto il necessario rispetto dei principi di finalità e minimizzazione del trattamento dei dati personali che richiede la sussistenza di uno specifico interesse organizzativo alla rilevazione degli accessi e delle presenze durante l'orario di lavoro. Il tenore letterale della norma, inoltre, non sembra ostare alla possibilità di ricondurre alla fattispecie tipica anche le registrazioni di accesso in ambienti "virtuali" attraverso computer o sistemi informatici, ferma restando l'istantaneità del controllo e il rispetto dei principi privacy.

2.2. Ammissibilità dei controlli difensivi

Con l'ampliamento formale delle ragioni legittimanti l'installazione e l'impiego degli strumenti di controllo anche alle esigenze di tutela del patrimonio aziendale, il legislatore ha determinato un ampliamento delle possibilità d'uso degli strumenti tecnologici rispetto al passato con importanti ripercussioni sulle condizioni di legittimità dei cosiddetti "controlli difensivi" diretti ad accertare comportamenti illeciti dei lavoratori.

Invero, nel vigore della precedente disposizione, si era già sostenuta in via interpretativa la legittimità dei controlli finalizzati alla protezione del patrimonio aziendale, benché mancasse una esplicita previsione legale in tal senso, a condizione che la loro esecuzione fosse rispettosa delle prescrizioni limitative dell'art. 4, St. Lav[49].

Nella giurisprudenza di legittimità però, si è andata ulteriormente affermando l'esistenza di una terza categoria di controlli rappresentata dai controlli difensivi "diretti ad accer-

---

48 M. Marazza, *op. cit.*, pag. 23, 24, sostiene fermamente la legittimità di un'interpretazione estensiva del dettato normativo.

49 In dottrina, cfr. R. Imperiali, *Controlli sul lavoratore e tecnologie*, Giuffrè, 2012, 173 ss.; P. Tullini, *Videosorveglianza a scopi difensivi e utilizzo delle prove di reato commesso dal dipendente*, *Riv. It. Dir. Lav.*, 2, I, 2011, 86 ss.; M.T. Salimbeni, *Il controllo a distanza sull'attività dei lavoratori: la sopravvivenza dell'art. 4 sugli impianti audiovisivi*, Dir. Lav. Merc., 2010, 3, pag. 587 ss.; C. Zoli, *Il controllo a distanza del datore di lavoro: l'art. 4, l. n. 300/1970 tra attualità ed esigenze di riforma*, *Riv. It. Dir. Lav.*, 4, I, 2009, 49; P. Tullini, *Comunicazione elettronica, potere di controllo e tutela del lavoratore*, *Riv. It. Dir. Lav.*, 3, I, 2009, 330 ss.; P. Ichino, *Il contratto di lavoro*, in *Trattato di diritto civile e commerciale*, 2003, III, 233 ss.; in giurisprudenza cfr. Cass. 17 luglio 2007, n. 15892, in *Riv. it. dir. lav.* 2008, 3, II, pag. 714 ss., con nota di Vallauri; Cass. 23 febbraio 2010, n. 4375, in Giust. civ. 2011, 4, pag. 1049 ss., con nota di Buffa; Cass. 18 aprile 2012, n. 16622, in *Guida al diritto 2012*, 49-50, 41; Cass. 27 marzo 2015, n. 10955, in *Rivista Italiana di Diritto del Lavoro 2016, 1, II, 120 ss.*, con nota di Puccetti.

tare comportamenti illeciti dei lavoratori idonei a pregiudicare beni estranei al rapporto di lavoro" [50]. Secondo tale orientamento, i controlli avrebbero dovuto ritenersi sottratti all'applicazione della norma statutaria e, pertanto, essere reputati legittimi anche in assenza di preventivo accordo sindacale o autorizzazione amministrativa all'installazione degli strumenti utilizzati per il controllo[51]. È con riferimento a tali categorie di controlli "eccezionali", dunque, che sembra palesarsi la portata innovativa dell'ampliamento positivo delle finalità legittimanti l'impiego di strumenti di controllo anche alle esigenze di tutela del patrimonio aziendale. Con esso, infatti, il legislatore potrebbe aver posto fine ad ogni ambiguità in materia di controlli difensivi, prescrivendo quale condizione di legittimità l'espletamento della procedura autorizzativa (sindacale o amministrativa) anche qualora il controllo sia operato per l'accertamento delle condotte illecite idonee a pregiudicare beni estranei al rapporto di lavoro[52].

A dire il vero, non sembra potersi escludere la sopravvivenza di controlli difensivi in "senso stretto", tuttora al di fuori del campo di applicazione dell'art. 4, St. Lav., in quanto mirati ad accertare selettivamente condotte illecite del lavoratore, non aventi ad oggetto l'attività del lavoratore[53]. Si tratta di quei comportamenti rilevanti penalmente, giuridi-

50 Cit. I. Alvino, *op. cit.*, pag. 18; *ex pluris* sulla legittimità dei controlli difensivi volti alla tutela di beni estranei al rapporto di lavoro, cfr. Cass. 23 febbraio 2012, n. 2722 e Cass. 4 aprile 2012, n. 5371 in *Riv. It. Dir. Lav.*, 2013, 1, II, pag. 113 ss., con nota di Spinelli; Cass. 17 luglio 2007, n. 15892, in *Riv. It. Dir. Lav.*, 2008, II, 714, con nota di Vallauri; Cass. 28 gennaio 2011, n. 2117, ADL, 2012, 136, con nota di Erboli, e Cass. 23 febbraio 2010, n. 4375, in *Riv. It. Dir. Lav.*, 2010, II, 564, con nota di Galardi; per una sintetica rassegna della giurisprudenza di legittimità, cfr. D. Conte, *Riflessioni sull'articolo 4 dello statuto dei lavoratori alla luce della consistenza trifasica del controllo*, in *Lavoro e previdenza oggi*, n. 1-2, 2017, pag. 8 e ss.

51 La prima, controversa, sentenza di legittimità in materia di controlli difensivi estranei all'applicazione dell'art. 4, St. Lav., è Cass. 3 aprile 2002, n. 4746, in Notiz. giur. lav., 2002, pag. 644, a partire dalla quale si è sviluppata l'elaborazione sull'ammissibilità dei controlli occulti, finanche diretti a verificare eventuali inadempimenti del lavoratore. Il rischio di un'eccessiva e ingiustificata dilatazione delle possibilità di controllo affrancate dalla disciplina limitativa statutaria è stato contenuto negli anni successivi dagli arresti della Suprema Corte volti a limitare la nozione di controllo difensivo, v. Cass. 17 luglio 2007, n. 15892, in *Riv. giur. lav.*, 2008, II, pag. 358 ss., con nota di A. Bellavista, *Controlli a distanza e necessità del rispetto della procedura di cui al comma 2 dell'art. 4 St. lav.*

52 A favore della tesi, P. Lambertucci, *Potere di controllo del datore di lavoro e tutela della riservatezza del lavoratore: i controlli a "distanza" tra attualità della disciplina statutaria, promozione della contrattazione di prossimità e legge delega del 2014 (c.d. Jobs act)*, in WP C.S.D.L.E. "Massimo D'Antona" .IT – 255/2015; Salimbeni, *op. cit.*, pag. 589; L. Tebano, *La nuova disciplina dei controlli a distanza: quali ricadute sui controlli conoscitivi?*, in *Riv. It. Dir. Lav.*, n. 3, I, pag. 353; Alvino, *op. cit.*, pag. 17; M. Russo, *Quis custodiet ipsos custodes? I "nuovi" limiti all'esrcizio del potere di controllo a distanza*, in *Labour&Law Issues*, 2016, vol.2, n.2, pag. 23; G. A. Recchia, *Controlli datoriali difensivi: note su una categoria in via di estinzione*, in *Il lavoro nella giurisprudenza*, 2017, n. 4, pag. 353.

53 In questi termini A. Maresca, *op. cit.*, pag. 10; la tesi è sostenuta anche da M. Marazza, *op. cit.*, pag. 18, il quale nonostante riconosca che il tenore letterale della norma giustifichi la riconduzione di tutti i controlli difensivi alle disposizioni di cui al comma 1, art. 4, St. Lav., residuerebbero margini per una interpretazione difforme volta a so-

camente autonomi rispetto alla obbligazione di lavoro, la cui qualificazione prescinde dalla possibilità che la condotta possa al contempo configurare anche un inesatto adempimento dell'obbligazione di lavoro[54]. Qualora avvalorata, la tesi tenderebbe anche ad eludere le difficoltà, riscontrate in passato, di individuazione delle condotte estranee all'attività lavorativa sulle quali poter operare controlli difensivi occulti[55]. Dirimente in ordine alla legittimità del controllo difensivo in senso stretto sarebbe l'esistenza di un pericolo attuale, connesso alla commissione di un illecito già commesso, di cui non si conosce l'autore e di cui si teme la reiterazione, purché l'attività di controllo sia strettamente correlata e limitata alla sua prevenzione[56]. Dalla specificità della condotta, inoltre, dovrebbe desumersi che il controllo difensivo attraverso strumentazione tecnologica deroghi non soltanto le prescrizioni in materia di autorizzazione, all'installazione ma anche quelle relative all'obbligo di informazione adeguata a trasparente.

2.3. Il rispetto della normativa privacy

L'allargamento della facoltà dell'imprenditore di introdurre strumenti di lavoro tecnologici non configura, però, una liberalizzazione dell'attività di controllo. Stante il nuovo impianto normativo, infatti, il trattamento e l'utilizzabilità delle informazioni raccolte attraverso l'uso della tecnologia, riferibile indifferentemente ai primi due commi dell'art. 4 St. Lav., sono assoggettati alle restrizioni prescritte nel nuovo comma 3. Con quest'ultima disposizione il legislatore ha finalmente aggiornato la disciplina del potere di controllo, regolamentando tutte le fasi della relativa attività di controllo in vista del soddisfacimento del bisogno di protezione della dignità e della riservatezza del lavoratore. Infatti, l'attuale formula dell'art. 4, St. Lav. non si limita più, come in passato, a dettare le con-

---

stenere le legittimità dei controlli difensivi, pur in mancanza di autorizzazione preventiva, qualora questi fossero volti ad accertare comportamenti del lavoratore di rilevanza penale.

54 V. M. Marazza, *I controlli a distanza di natura "difensiva"*, in P. Tullini (a cura di), *Controlli a distanza e tutela dei dati personali del lavoratore*, Giappichelli, 2017, pag. 40, 41, il quale sottolinea che per poter valutare le legittimità di un controllo difensivo occorrerà verificare l'esistenza degli elementi di attualità del pericolo.

55 Sulla possibilità di una tale distinzione fortemente critico A. Bellavista, *La Cassazione e i controlli a distanza sui lavoratori*, in *Riv. giur. lav.*, 2010, II, pag. 465, secondo cui "la Cassazione pensa di separare con l'accetta due aree: da un lato, l'attività lavorativa, che rientrerebbe nel campo di applicazione della disposizione, dall'altro, le condotte illecite del medesimo lavoratore, le quali invece sarebbero al di fuori del suddetto campo di applicazione e sulle quali pertanto il controllo tecnologico potrebbe svolgersi senza alcun limite. Ma nella realtà effettuale le cose non stanno proprio così. Ciò perché i controlli diretti ad accertare condotte illecite del lavoratore molto spesso sono anche controlli sull'attività lavorativa Eppure, "l'accertamento della condotta "illecita" del dipendente spesso può essere rilevata solo controllando l'esecuzione della prestazione lavorativa".

56 M. Marazza, *op. cit.*, pag. 41, ipotizza in via esemplificativa l'installazione di telecamere per l'individuazione dell'autore di un furto, esclusivamente nell'area dove quest'ultimo possa ripetersi, non anche nel resto dei locali aziendali.

dizioni di legittimità per la "predisposizione del controllo", ma regolamenta anche il momento della "rilevazione e acquisizione" dell'informazione e del "trattamento" del dato registrato da parte del datore di lavoro[57].

Il comma 3, art. 4, St. Lav., prevede due condizioni di legittimità per l'utilizzabilità delle informazioni raccolte: il lavoratore deve essere adeguatamente informato delle modalità d'uso degli strumenti e di effettuazione dei controlli; il trattamento deve avvenire nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n. 196[58].

Sull'adeguata informazione al lavoratore ci si soffermerà più avanti (v. par. 3.2), limitandoci al momento a rilevare come la sua prescrizione rappresenti un rafforzamento della procedimentalizzazione del potere del datore di lavoro[59]. Per quanto, invece, concerne il rispetto della disciplina del codice *privacy*, la sua introduzione nella disciplina statutaria comporta che i limiti in esso prescritti assumano "una diretta incidenza sul legittimo esercizio dei poteri datoriali", al pari dei vincoli prescritti nei commi 1 e 2, art. 4 St. Lav., con riferimento a tutte le attività di controllo impersonali a prescindere dalla tipologia di strumento tecnologico impiegato per realizzarle[60].

Poiché il rispetto degli adempimenti e delle prescrizioni *privacy*, alla luce della novella, assurge a condizione imprescindibile per l'utilizzabilità delle informazioni raccolte tramite strumenti tecnologici, la comprensione dell'esatta portata del rinvio legale alla normativa inerente alla protezione dei dati personali non rappresenta un problema di poco momento, considerato il nuovo assetto della disciplina limitativa del potere di controllo a distanza. La regola affermata ha come effetto immediato la neutralizzazione di ogni azione sul piano individuale che il datore di lavoro dovesse intraprendere nei confronti del lavoratore sulla base delle informazioni raccolte illegittimamente. A differenza del passato, dunque, per dimostrare il legittimo utilizzo dei dati raccolti al datore di lavoro

57 Secondo D. Conte, *Riflessioni sull'articolo 4 dello statuto dei lavoratori alla luce della consistenza trifasica del controllo*, in *Lavoro e previdenza oggi*, 1-2, 2017, pag. 2, "l'attività di controllo passibile di essere ritenuta regolata dall'art. 4, ha una consistenza che si articola in almeno tre "fasi" o "momenti" tra loro distinti (c.d. consistenza "trifasica" del controllo): quella di predisposizione del controllo, che consiste nell'attività di ideazione, progettazione, installazione e programmazione dello strumento destinato al controllo; quella della rilevazione acquisizione in tempo reale dell'informazione da parte dello strumento; quella del trattamento da parte del datore di lavoro o di suoi incaricati del dato registrato".

58 Per una analisi dei limiti all'esercizio del potere di controllo ricavabili dal nuovo art. 4, St. Lav., v. M. Russo, *Quis custodiet ipsos custodes? I "nuovi" limiti all'esercizio del potere di controllo a distanza*, in *Labour&Law Issues*, vol. 2, n.2, 2016.

59 Per G. A. Recchia, *Controlli datoriali difensivi: note su una categoria in via di estinzione*, *op. cit.*, pag. 353, pone in evidenza come il potere di controllo del datore di lavoro esca fortemente procedimentalizzato dalla novella post Jobs Act dell'art. 4, St. Lav.

60 Cit. I. Alvino, *op. cit.*, pag. 30.

non sarà sufficiente dimostrare di aver operato nel rispetto dei limiti "finalistici" e "procedurali", previsti dai primi due commi della norma statutaria, ma anche che l'attività di vigilanza sia stata eseguita nel rispetto dei limiti "sostanziali" che vanno ricercati nella disciplina *privacy*.

Non può tacersi, però, che in assenza di specifiche disposizioni normative disciplinanti il trattamento dei dati nell'esercizio dell'attività di controllo e, oltretutto, in assenza di formante giurisprudenziale, la compiuta armonizzazione della disciplina lavoristica con quella in materia di riservatezza e trattamento dei dati personali sarà di fatto demandata ai datori di lavoro e agli operatori del diritto chiamati ad un arduo compito esegetico.

Per i fini che qui interessano e data l'economia del presente contributo, si cercherà di fare maggiore chiarezza in ordine agli adempimenti dei datori di lavoro previsti nella fase applicativa dell'attività di controllo, tenuto conto degli orientamenti e della prassi dell'Autorità Garante per la protezione dei dati personali a cui, il d.lgs. n. 196/2003 attribuisce funzioni non soltanto di controllo, interdittive, promozionali, consultive e propositive, ma anche di carattere para giurisdizionale.

3. Le condizioni di liceità del trattamento dei dati personali nell'esercizio del potere di controllo a distanza

3.1. La base giuridica del trattamento dati

Il Regolamento Europeo sulla protezione dei dati n. 679/2016 (in inglese, *General Data Protection Regulation*, d'ora in poi anche GDPR) non prevede norme specifiche per il trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro, rinviando agli Stati membri o alla contrattazione collettiva la possibilità di una loro introduzione (cfr. considerando 155).

In particolare, ai sensi dell'art. 88 GDPR, possono essere adottate norme di diritto interno al fine di assicurare una maggiore protezione al lavoratore sia in relazione al trattamento finalizzato all'instaurazione e cessazione del rapporto di lavoro, sia per quello relativo alla esecuzione del contratto di lavoro e all'adempimento degli obblighi stabiliti dalla legge o da contratti collettivi[61]. Norme specifiche possono anche essere previste

61 Il trattamento dei dati dei lavoratori con la finalità di assunzione esula dall'oggetto del presente lavoro. Tuttavia, tale genere di operazioni di trattamento dei dati da parte dei datori di lavoro è molto frequente, in particolare grazie all'utilizzo di social network, professionali (come *Linkedin*) o generici (come *Facebook*, *Instagram*, *Twitter*). Per un'analisi di tipo statistico sull'utilizzo del *social recruiting* da parte delle imprese italiane, dettagliata e divisa per settore merceologico, cfr. il Report dell'Osservatorio sulle competenze digitali 2018, realizzato da Aica,

per finalità di pianificazione e organizzazione del lavoro nonché per quelle relative alla parità sul posto di lavoro ed alla prevenzione dei rischi in materia di salute o alla protezione della proprietà del datore di lavoro o del cliente.
In ciascuno dei casi previsti dall'art. 88 GDPR, le discipline legali interne dovranno includere misure a tutela della *privacy*, con riferimento alla trasparenza del trattamento, nonché al trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune. Infine, particolare attenzione viene posta dal legislatore europeo alle modalità di utilizzo dei dispositivi, hardware e software attraverso i quali sia possibile il monitoraggio del personale dipendente.
Il legislatore italiano ha proceduto all'armonizzazione del Codice *Privacy* con il regolamento dell'Unione europea attraverso l'emanazione del d.lgs. n. 101/2018 che ha modificato, e in gran parte abrogato, le disposizioni del d.lgs. n. 196/2003[62]. Nel nuovo testo del Codice *Privacy* non si rinvengono disposizioni di particolare rilievo in materia di controllo a distanza, bensì un laconico rinvio all'art. 4 Statuto dei Lavoratori[63]. Per il resto, il titolo VIII, del d.lgs. n. 196/2003, dedicato ai "trattamenti nell'ambito del rapporto di lavoro", contiene una scarna disciplina, essenzialmente di rinvio ad altre disposizioni. Rispetto alla tematica trattata, alcuni ulteriori profili di interesse possono rinvenirsi soltanto nell'art. 111, titolo VIII d.lgs. n. 196/2003, che attribuisce al Garante il compito di promuovere l'adozione di regole deontologiche per i soggetti pubblici e privati interessati al trattamento dei dati personali effettuato nell'ambito del rapporto di lavoro per le finalità di cui all'articolo 88 del Regolamento, prevedendo anche specifiche modalità per le informazioni da rendere all'interessato. La nuova formulazione abbandona l'idea del "codice di deontologia e buona condotta", individuando una libertà delle forme per la raccolta e la formulazione delle stesse, e ribadisce la necessità di un'informazione adeguata al lavoratore[64].
Nelle more di una specifica disciplina di diritto interno, dunque, la liceità del trattamento dei dati dei lavoratori andrà verificata alla luce delle regole generali e delle condizioni dettate dalla norma regolamentare. Secondo l'art. 6, GDPR, dunque, ogni titolare del

---

Anitec-Assinform, Assintel, Assinter, con il supporto di CFMT, Confcommercio, Confindustria e in collaborazione con AgID - Agenzia per l'Italia Digitale e Ministero dell'Istruzione dell'Università e della Ricerca, reperibile su https://www.lispa.it.

62 Il vigente art. 1, d.lgs. n. 196/2003, prescrive che il trattamento dei dati personali avvenga secondo le norme del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e nel rispetto della dignità umana, dei diritti e delle libertà fondamentali della persona.

63 *Ex* art. 114, Codice privacy, "resta fermo quanto disposto dall'articolo 4 della legge 20 maggio 1970, n.300".

64 Cfr. G.M. Riccio, G. Scorza, E. Belisario (a cura di), *GDPR e normativa privacy. Commentario*, Ipsoa, 2018, pag. 652.

trattamento dovrà *in primis* accertarsi che le relative operazioni abbiano base giuridica in una delle seguenti ipotesi:

a) il consenso del lavoratore;
b) la necessità del trattamento ai fini dell'esecuzione del rapporto contrattuale di cui l'interessato è parte;
c) l'adempimento di un obbligo legale al quale è soggetto il datore di lavoro;
d) la necessità del trattamento ai fini della salvaguardia di un interesse vitale del lavoratore;
e) l'esecuzione di un compito di interesse pubblico;
f) il perseguimento del proprio legittimo interesse, a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali del lavoratore.

Il rispetto degli adempimenti e delle prescrizioni *privacy* quale condizione imprescindibile per l'utilizzabilità delle informazioni raccolte nei luoghi di lavoro tramite strumenti tecnologici, previsto dal comma 3, art. 4, St. Lav., impone innanzitutto l'individuazione delle condizioni di liceità del trattamento dati implicato nell'esercizio del potere di controllo. Tale attività interpretativa, però, presenta profili problematici di non poco momento.
In primo luogo, la circostanza per la quale il rapporto di lavoro abbia fonte negoziale non pare sufficiente a legittimare il trattamento occasionato dall'attività di controllo a distanza, in quanto tra le esigenze che a questo sottendono e l'esecuzione del rapporto contrattuale di lavoro non è sempre rinvenibile l'esistenza di un nesso di causalità tale per cui la mancanza del trattamento dati comporterebbe l'impossibilità di esecuzione del contratto. Confortano l'assunto, peraltro, le indicazioni già fornite dal WP29[65], per il quale la base giuridica "non si applica a tutte le ulteriori azioni avviate a seguito di inosservanza o a tutti gli altri incidenti intervenuti nell'esecuzione di un contratto"[66]. Diversamente, la necessità del trattamento ai fini dell'esecuzione di un rapporto contrattuale di lavoro potrà dirsi senz'altro verificata in relazione alle informazioni riguardanti la determinazione e la liquidazione degli stipendi.

---

65 Sulla funzione del WP29, cfr. nota 6.

66 Cfr. WP217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, pag. 20, 21. Secondo il gruppo di lavoro "il monitoraggio elettronico dell'utilizzo di Internet, della posta elettronica o del telefono da parte dei dipendenti o la videosorveglianza dei lavoratori costituiscono più chiaramente trattamenti che con ogni probabilità vanno oltre quanto necessario all'esecuzione di un contratto di lavoro, sebbene anche in questo caso ciò possa dipendere dalla natura dell'attività lavorativa".

Anche l'ulteriore fondamento giuridico rinvenibile nell'adempimento di obblighi legali si adatta difficilmente alla fattispecie che qui si analizza. Infatti, configurandosi per lo più come esercizio facoltativo di potere, soltanto in ipotesi circoscritte l'attività di controllo trova la propria base giuridica in un obbligo legale al quale è soggetto il titolare del trattamento[67], come accade, ad esempio, con gli apparecchi di controllo nel settore del trasporto su strada (dispositivi cronotachigrafi), in ossequio al regolamento 561/2006/CE, come modificato dal regolamento europeo 165/2014/CE, o come accade con i sistemi di localizzazione GPS dei veicoli portavalori, ai sensi dell'allegato D, art. 257 T.U.L.P.S. (Testo unico delle leggi di pubblica sicurezza)[68].

Uno specifico presupposto legale è anche necessario con riguardo alla base giuridica per il trattamento di dati personali effettuato per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri che l'art. 2-*ter*, d.lgs. n. 196/2003, precisa essere costituita esclusivamente da una norma di legge o di regolamento. Si pensi alle previsioni della legge n. 56 del 19 giugno 2019, recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", volte alla introduzione per le amministrazioni pubbliche specificamente indicate dell'obbligo legale di introdurre sistemi di riconoscimento attraverso dati biometrici e di videosorveglianza in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso, ai fini della verifica dell'osservanza dell'orario di lavoro (sul trattamento dei dati biometrici v. par. 4.5 e 4.5.1)[69].

---

67 Si condivide quanto affermato da M. Marazza, *I controlli a distanza del lavoratore di natura "difensiva"*, *op. cit.*, pag. 43, in ordine alla limitata utilizzabilità dei dati così raccolti per le sole finalità prescritte dalla legge.

68 L'Ispettorato nazionale del lavoro ha fornito chiarimenti in merito all'installazione di apparecchiature di localizzazione satellitare GPS con la circ. 2/2016.

69 Ai sensi dell'art. 2, co. 1, l. n. 56/2019, "Ai fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione dei dipendenti di cui all'articolo 3 del medesimo decreto e fuori dei casi di cui all'articolo 18 della legge 22 maggio 2017, n. 81, introducono, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente e della dotazione del fondo di cui al comma 5, sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso, nel rispetto dei principi di proporzionalità, non eccedenza e gradualità sanciti dall'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro per la pubblica amministrazione, da adottare ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, previa intesa in sede di Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e previo parere del Garante per la protezione dei dati personali ai sensi dell'articolo 154 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sulle modalità di trattamento dei dati biometrici, sono individuate le modalità attuative del presente comma, nel rispetto dell'articolo 9 del regolamento (UE) 2016/679 del Parlamento europeo

Il trattamento di dati personali dovrebbe essere altresì considerato lecito quando è necessario per proteggere un interesse essenziale per la vita dell'interessato o di un'altra persona fisica. Come precisato dal considerando 46 GDPR, però, il trattamento di dati personali fondato sull'interesse vitale di un'altra persona fisica dovrebbe avere luogo in principio unicamente quando il trattamento non può essere manifestamente fondato su un'altra base giuridica. Rispetto ai circoscritti fini dell'analisi, la base di legittimità non sembra facilmente compatibile con le finalità sottese al trattamento dati in caso di controllo a distanza. Tuttalpiù, in casi piuttosto peculiari, l'interesse vitale potrebbe essere invocato quale condizione di liceità dal datore di lavoro che intenda porre in essere attività di controllo motivate da esigenze di sicurezza del lavoro in chiave prevenzionistica per la riduzione dei rischi di salute a cui sono esposti i lavoratori, qualora queste non risultino in qualche modo riconducibili ad un obbligo legale a cui è assoggettato il titolare del trattamento. D'altronde, l'art. 4, comma 1, St. Lav., nel declinare le esigenze legittimanti l'installazione di impianti dai quali potrebbe derivare un controllo indiretto dei lavoratori, individua, fra le altre, quelle relative alla sicurezza del lavoro[70].
Invero, rispetto ai profili di cui si tratta, il ricorso alle esigenze vitali in funzione di base giuridica del trattamento, appare piuttosto residuale, in considerazione dell'esistenza di un legittimo interesse in capo al datore di lavoro, che si ritiene palesato in forza delle prerogative legali attribuitegli in materia di poteri e controlli.

3.1.1. Il legittimo interesse come base del trattamento dei dati in ambito lavorativo

In proposito sembra potersi affermare che la comprovata esistenza di esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale, ovvero la necessità di adottare strumenti tecnologici per rendere la prestazione lavorativa, secondo quanto previsto proprio dall'art. 4 St. Lav., non sia altro che una specificazione legale del legittimo interesse richiamato dal GDPR.
Tale approccio interpretativo, peraltro, è avvalorato dal Considerando n. 47, GDPR, secondo il quale i legittimi interessi di un titolare del trattamento "possono costituire una base giuridica del trattamento", sussistendo "quando esista una relazione pertinente e

---

e del Consiglio, del 27 aprile 2016, e delle misure di garanzia definite dal predetto Garante, ai sensi dell'articolo 2-*septies* del citato codice di cui al decreto legislativo n. 196 del 2003".

70 In proposito cfr. circolare Ispettorato Nazionale del lavoro prot. N. 302 del 18 giugno 2018, nella quale si afferma che "nel caso di richieste di autorizzazione legate ad esigenze di "sicurezza del lavoro", vadano puntualmente evidenziate le motivazioni di natura prevenzionistica che sono alla base dell'installazione di impianti audiovisivi e altri strumenti di potenziale controllo a distanza dei lavoratori corredate da una apposita documentazione di supporto". Inoltre, le necessità legate alla sicurezza del lavoro devono trovare "adeguato riscontro nell'attività di valutazione dei rischi effettuata dal datore di lavoro e formalizzata nell'apposito documento (DVR)".

appropriata tra l'interessato e il titolare del trattamento, ad esempio quando l'interessato è [...] alle dipendenze del titolare del trattamento" ma "a condizione che i legittimi interessi del titolare non prevalgano [su] gli interessi o i diritti e le libertà fondamentali dell'interessato, tenuto conto delle ragionevoli aspettative nutrite dall'interessato in base alla sua relazione con il titolare del trattamento".

La presenza dell'inciso "a condizione che non prevalgano gli interessi o i diritti e le libertà fondamentali" dell'interessato impone al datore di lavoro, che intenda porre il proprio legittimo interesse a fondamento del trattamento, di valutarne attentamente l'incidenza sulla sfera di riservatezza del lavoratore[71]. In particolare, il metodo scelto o la tecnologia specifica con cui verrà effettuato il trattamento devono essere necessari per il perseguimento del legittimo interesse del datore di lavoro e il trattamento deve essere proporzionato alle esigenze aziendali, in ossequio ai principi di minimizzazione e di limitazione della finalità, previsti dall'art. 5 GDPR[72].

D'altronde, nonostante l'abrogazione dell'art. 24, Codice Privacy, le valutazioni già espresse dal Garante in ordine al bilanciamento di interessi sono perfettamente mutuabili al nuovo contesto normativo[73]. Così, in forza del legittimo interesse all'esercizio del potere di controllo, nei modi e attraverso gli strumenti di cui all'art. 4, St. Lav., i datori di lavoro privati possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili purché gli interessi o i diritti e le libertà fondamentali di questo non siano prevalsi da quelli datoriali, anche in assenza del consenso del lavoratore che, come si preciserà appresso, non sembra una base giuridica di cui ci si possa generalmente avvalere nell'ambito del rapporto di lavoro.

---

71 Nel Considerando 47, si legge: "in ogni caso, l'esistenza di legittimi interessi richiede un'attenta valutazione anche in merito all'eventualità che l'interessato, al momento e nell'ambito della raccolta dei dati personali, possa ragionevolmente attendersi che abbia luogo un trattamento a tal fine. Gli interessi e i diritti fondamentali dell'interessato potrebbero in particolare prevalere sugli interessi del titolare del trattamento qualora i dati personali siano trattati in circostanze in cui gli interessati non possano ragionevolmente attendersi un ulteriore trattamento dei dati personali". Tale previsione appare espressione del più generale principio di "Accountability" o "responsabilizzazione" del titolare del trattamento, esplicitato all'art. 5, par. 2 GDPR, ai sensi del quale gli viene demandata la capacità di comprovare il rispetto della normativa. A tal fine si rende necessario, per ogni titolare del trattamento, un'attività di audit di processi interni che, partendo da un'analisi del rischio, metta in atto politiche adeguate di protezione dei dati. Spunti operativi sul tema in A. Carnabuci, P. Ceccoli, B. De Rosa, I. Mariani, C. Minieri, P. Radaelli, A. Zappia, A. Zucchetti, *Privacy e dati personali: problemi e casi pratici*, Key Editore, 2018.

72 Sulle specificità del trattamento basato sul legittimo interesse del datore di lavoro, cfr. Gruppo di lavoro Articolo 29, *Parere 2/2017 sul trattamento dei dati sul posto di lavoro*, 8 giugno 2017 e Gruppo di lavoro Articolo 29, *Parere 6/2014 sul concetto di interesse legittimo del titolare del trattamento ai sensi dell'art. 7 della Direttiva 95/46/CE*, 9 aprile 2014.

73 Cfr. Garante italiano per la protezione dei dati personali, deliberazione n. 13/2007, *Lavoro: le Linee Guida del Garante per posta elettronica e internet.*

Il rispetto delle garanzie apprestate dallo Statuto dei lavoratori nelle ipotesi di controllo a distanza continua ad essere sinonimo di un bilanciamento di interessi che può dirsi correttamente operato a seguito del positivo esperimento della fase di controllo sindacale o, in difetto, dell'ottenimento dell'autorizzazione dell'Ispettorato nazionale del lavoro. Lo stesso può dirsi anche in caso di controlli effettuati attraverso gli strumenti di lavoro di cui al nuovo comma 2, art. 4 St. lav., in quanto l'assenza di una procedura autorizzatoria all'installazione di tali strumenti è giustificata dal rilievo legale del relativo interesse datoriale che è frutto di un bilanciamento operato *in nuce* dallo stesso legislatore.

3.1.2. Il consenso del lavoratore

Il consenso dell'interessato assurge a base "generale" di legittimità per il trattamento dei dati personali, superabile in presenza di uno degli ulteriori cinque diversi presupposti di liceità individuati dall'art. 6, GDPR. Il regolamento ne prescrive gli elementi di validità senza circoscrivere *a priori* gli ambiti specifici rispetto ai quali debba o possa essere ammesso il consenso quale presupposto del trattamento dei dati. In tal senso, la base giuridica si palesa quale condizione di legittimità di tipo generale in grado di operare sia in "sovrapposizione" agli altri presupposti legittimanti sia in via residuale ad essi. La generalità della base giuridica, però, non è mutuabile rispetto alle finalità della raccolta dei dati, in quanto il consenso dell'interessato non può legittimare genericamente il trattamento dei dati che dovrà sempre essere giustificato dall'esistenza di una finalità specifica. In proposito e in termini più ampi, il gruppo WP29 ha opportunamente chiarito che "l'ottenimento del consenso non fa venir meno né diminuisce in alcun modo l'obbligo del titolare del trattamento di rispettare i principi applicabili al trattamento sanciti nel regolamento generale sulla protezione dei dati, in particolare all'articolo 5, per quanto concerne la correttezza, la necessità e la proporzionalità, nonché la qualità dei dati" [74].
Il "consenso" è definito dal regolamento come "qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con la quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento" (*ex* art. 4, n. 11, GDPR)[75].
Perché possa essere posto a base giuridica del trattamento, dunque, il consenso deve presentarsi come genuina manifestazione del diritto all'autodeterminazione informativa

---

74 Cit. Gruppo di lavoro Articolo 29, *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, del 28 novembre 2017, come modificate e adottate da ultimo il 10 aprile 2018, doc. WP 259 rev.01, pag. 3.

75 Un'analisi approfondita della nozione di consenso è fornita dal Gruppo di lavoro Articolo 29, nelle richiamate *Linee guida sul consenso ai sensi del regolamento (UE) 2016/679*, doc. WP 259 rev.01.

in forza del quale l'interessato dichiara la propria scelta in condizione di effettiva libertà, mantenendo il controllo dei propri dati durante il trattamento[76].

Il requisito di validità andrà in particolar modo valutato rispetto alla presenza/assenza di condizionamenti derivanti dall'accettazione di clausole che determinano un significativo squilibrio dei diritti e degli obblighi derivanti dal contratto, nonché dalla circostanza che il consenso sia "parte non negoziabile delle condizioni generali di contratto/servizio"[77]. Sotto quest'ultimo profilo, l'art. 7, par. 4, GDPR, richiede un'analisi rispetto alla possibilità che nell'esecuzione di un contratto, compresa la prestazione di un servizio, sia richiesto un consenso al trattamento di dati personali non necessario all'esecuzione di tale contratto. Come chiarito dal considerando 43 GDPR, "si presume che il consenso non sia stato liberamente espresso (...) se l'esecuzione di un contratto, compresa la prestazione di un servizio, è subordinata al consenso sebbene esso non sia necessario per tale esecuzione".

Allo stesso modo, il soggetto interessato non disporrà di effettiva libertà di scelta ogniqualvolta sussista un evidente squilibrio di potere nella relazione con il titolare del trattamento, come accade tipicamente nel contesto dell'occupazione. Lo svolgimento del rapporto di lavoro nella impresa organizzata gerarchicamente, infatti, collide con la possibilità che il consenso, quale manifestazione di volontà dei lavoratori, possa presentare i caratteri di libertà e assenza di condizionamento richiesti dalla legge, in considerazione dell'evidente squilibrio di potere esistente tra il lavoratore interessato e il datore di lavoro titolare del trattamento[78]. L'evidenza di tale asimmetria porta ad escludere che il consenso nell'ambiente di lavoro possa costituire una condizione di liceità, sollecitando gli operatori alla individuazione di una diversa e idonea base giuridica del trattamento che, come sopra argomentato con riguardo all'esercizio del potere di controllo, sembra poter risiedere prevalentemente nel legittimo interesse del datore di lavoro ad espletare l'attività di controllo per le finalità previste dalla legge.

In una diversa prospettiva e sempre con specifico riferimento al potere di controllo del datore di lavoro, appare convincente la tesi che esclude la necessità del consenso per

76 Cfr. il parere 15/2011 sulla definizione di consenso (WP 187), pagine 6-8, richiamato dalle linee guida sul consenso, nonché quanto già espresso dal Garante italiano per la protezione dei dati, 28 maggio 1997, in Bollettino, 1, pag.17, alla luce della direttiva 95/46/CE.

77 Indicazioni esemplificative sono offerte dal WP29 nelle linee guida: "Un'applicazione mobile per il fotoritocco chiede agli utenti di attivare la localizzazione GPS per l'utilizzo dei suoi servizi. L'applicazione comunica agli utenti che utilizzerà i dati raccolti per finalità di pubblicità comportamentale. Né la geolocalizzazione né la pubblicità comportamentale online sono necessarie per la prestazione del servizio di fotoritocco e vanno oltre la fornitura del servizio principale. Poiché gli utenti non possono utilizzare l'applicazione senza acconsentire a tali finalità, il consenso non può essere considerato liberamente espresso".

78 Cfr. Considerando 43 GDPR. Lo squilibrio di potere è chiaramente riconosciuto nelle linee guida WP259.

il trattamento dati conseguente all'attività di controllo a distanza motivandola rispetto alla natura speciale della norma statutaria, cosicché il codice *privacy* dovrebbe trovare applicazione solo nella misura in cui non sia derogato dall'art. 4, St. Lav., con la prima rilevante conseguenza che l'acquisizione e l'utilizzabilità delle informazioni non sarebbe subordinata al rilascio di alcun consenso da parte del lavoratore[79]. Tale consenso sarebbe, di fatto, sostituito dall'obbligo di adeguata informazione in favore del lavoratore che, fermo restando il rispetto degli ulteriori vincoli previsti per la predisposizione degli strumenti di controllo, abilita di per sé il datore di lavoro alla raccolta ed al trattamento dei dati personali. D'altronde, ritenere il consenso del lavoratore necessario ai fini dell'esercizio del potere di controllo del datore di lavoro striderebbe con la *ratio* di quest'ultimo che non tollera di essere subordinato al consenso del soggetto passibile di controllo. In definitiva, sembra potersi affermare che il consenso nell'ambito del rapporto di lavoro costituisca una condizione di liceità solo in ipotesi residuali, comunque estranee all'esercizio del potere di controllo del datore di lavoro. Si pensi, ad esempio, al caso delle riprese audiovisive nei luoghi aziendali (per finalità di divulgazione, di promozione o di comunicazione delle attività aziendali). Solo in simili circostanze, il lavoratore sembra libero di decidere se autorizzare o meno la ripresa della propria immagine, non configurandosi conseguenze negative in caso di rifiuto[80]. L'individuazione di specifiche e ulteriori ipotesi, come si evince dal considerando 155 GDPR, sono rimesse alle previsioni di diritto interno e di contratto collettivo, a cui la norma regolamentare rimanda per la definizione delle condizioni alle quali i dati personali nei rapporti di lavoro possono essere trattati sulla base del consenso del dipendente, 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, 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".

Sempre in tema di consenso, inoltre, è opportuno sgomberare il campo da equivoci circa la possibilità di *bypassare* la procedura autorizzatoria sindacale o amministrativa di cui all'art. 4, comma 1, St. Lav., in forza del consenso prestato da parte di tutti i lavoratori

---

79 Per M. Marazza, *Dei poteri (del datore di lavoro), dei controlli (a distanza) e del trattamento dei dati (del lavoratore)*, *op. cit.*, pag. 27, il rispetto dei commi 1 e 2 nonché dell'obbligo di informativa supera ogni diversa previsione del Codice *Privacy* in materia di consenso al trattamento e/o finalità dello stesso; contra M. Barbieri, *op. cit.*, pag. 194, con particolare riguardo alle finalità del trattamento; E. Raimondi, *Potere di controllo, tutela della riservatezza e «lavoro agile»*, in *Riv. giur. Lav.*, 2019, n. 1, pag. 85.

80 Secondo il parere 15/2011 sulla definizione di consenso (WP 187), pagg. 14-19, stante la specialità del rapporto di lavoro subordinato, la dipendenza tra il soggetto interessato rispetto al titolare del trattamento dei dati implica l'esistenza di una marcata presunzione che la libera manifestazione del consenso sia limitata.

alla installazione di impianti tecnologici idonei a consentire il controllo a distanza dei dipendenti. La tesi (improbabile) dell'equipollenza tra consenso individuale dei lavoratori e accordo sindacale è stata sostenuta da un'isolata pronuncia della Cassazione penale che, oltre ad essere in contrasto con la consolidata giurisprudenza lavoristica in materia, è stata ben presto contraddetta dalla stessa Sezione penale[81]. Come affermato dalla più autorevole dottrina, l'indicazione dei soggetti collettivi legittimati a concludere l'accordo sindacale, infatti, deve considerarsi tassativa e, in considerazione della garanzia degli interessi collettivi e superindividuali a cui è preordinato, soltanto l'accordo con le rappresentanze sindacali richiamate dalla legge sarà idoneo al soddisfacimento degli obblighi procedurali, senza possibilità di letture estensive del dettato normativo[82].

3.2. L'informazione adeguata e trasparente

Il datore di lavoro, al pari di ogni titolare del trattamento, è tenuto a fornire al lavoratore interessato una informativa conforme alle prescrizioni dell'art. 13 GDPR, declinata con riferimento a tutte le operazioni di trattamento dei dati poste in essere. Questa rappresenta un adempimento irrinunciabile, al quale il titolare del trattamento deve sempre attenersi e il cui contenuto minimo comprende:

- identità e dati di contatto del Titolare e, ove vi sia, del suo Rappresentante[83];
- i dati di contatto del Responsabile della protezione dei dati[84];
- le finalità del trattamento;

---

81 La tesi dell'equipollenza sostenuta in Cass. pen. 11 giugno 2012, n. 22611, in *Not. giur. lav.*, 2012, 465 ss. è stata apertamente contraddetta dalle successive pronunce di Cass. 10 ottobre 2012, n. 16622, in *Not. giur. lav.*, 2012, pag. 462, e, in sede penale, di Cass. Pen. 31 gennaio 2017, n.22148, in *GiustiziaCivile.com*, fasc. 7 febbraio 2018, con nota di T. Frigerio, quest'ultima ha evidenziato come la norma penale di cui all'art. 4 St. lav. non si limiti a tutelare la posizione giuridica dei singoli lavoratori bensì è posta a garanzia di "interessi di carattere collettivo e superindividuale", di cui "le rappresentanze sindacali sono portatrici".

82 *Ex pluris* v. A. Bellavista, *Gli accordi sindacali in materia di controlli a distanza sui lavoratori*, in *Lav. nella giur.*, 2014, 8-9, pag. 738, il quale cataloga la sentenza di Cassazione penale 11 giugno 2012, n. 22611, alla stregua di un vero e proprio "strafalcione".

83 Il Rappresentante del Titolare è, ai sensi dell'art. 4 punto 17 del GDPR, "la persona fisica o giuridica stabilita nell'Unione che, designata dal titolare o dal responsabile del trattamento per iscritto ai sensi dell'art. 27, li rappresenta per quanto riguarda gli obblighi rispettivi a norma del presente regolamento". In altre parole, è una figura che riguarda i titolari del trattamento che hanno sede legale al di fuori dell'UE, ma che sono soggetti al GDPR e, per tale ragione, devono nominare un loro rappresentante stabilito nell'UE.

84 Il Responsabile della protezione dei dati (RPD) o *Data Protection Officer* (DPO) è una nuova figura prevista dal GDPR, auspicata dal legislatore comunitario in tutte le realtà, ma obbligatoria solo nei seguenti casi:
a) il trattamento è effettuato da un'autorità pubblica o da un organismo pubblico, eccettuate le autorità giurisdizionali quando esercitano le loro funzioni giurisdizionali;

- la base giuridica del trattamento;
- l'indicazione dei legittimi interessi del titolare, qualora il trattamento trovi fondamento nei medesimi;
- gli eventuali destinatari dei dati personali;
- l'intenzione, ove applicabile, di trasferire i dati in un Paese terzo rispetto alla UE.

L'informativa costituisce espressione del generale principio di trasparenza del trattamento, il quale impone che le informazioni e le comunicazioni relative al trattamento di tali dati personali siano facilmente accessibili e comprensibili e che sia utilizzato un linguaggio semplice e chiaro (cfr. considerando n. 39, GDPR)[85].
In relazione alle attività connesse all'esercizio del proprio potere di controllo, le finalità del trattamento che dovranno essere oggetto dell'informativa saranno necessariamente riferite ad esigenze organizzative e produttive, per la sicurezza del lavoro o per la tutela del patrimonio aziendale, per gli strumenti di cui al comma 1, art. 4 St. Lav., oppure ad esigenze lavorative per i controlli sugli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa e per la registrazione degli accessi e delle presenze.
La nuova norma statutaria, però, prevede un rafforzamento dei diritti conoscitivi del lavoratore soggetto ad attività di controllo tecnologico, in una prospettiva di una nuova espansione del diritto alla c.d. "autodeterminazione informativa", per certi versi, compresso dal superamento della necessità di consenso. Così, il comma 3 dell'art. 4 St. Lav. richiede al datore di lavoro intenzionato ad utilizzare "a tutti i fini connessi al rapporto di lavoro" le informazioni raccolte (ai sensi dei commi 1 e 2) l'obbligo di fornire al lavoratore un'adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli.
È opinione condivisa che la "adeguata informazione" prevista dallo norma statutaria presenti un contenuto diverso dall'informativa *ex* art. 13 GDPR, in quanto la prima deve illustrare le consentite modalità di utilizzo degli strumenti aziendali e dei possibili controlli, anche a fini disciplinari, e dunque è legata ai regolamenti aziendali o ai codici disciplinari interni; mentre la seconda deve esplicitare tutti i punti richiesti dalla norma-

---

b) le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che, per loro natura, ambito di applicazione e/o finalità, richiedono il monitoraggio regolare e sistematico degli interessati su larga scala;
c) le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento, su larga scala, di categorie particolari di dati personali.

85 Appare preferibile un'informativa concisa rispetto ad una prolissa, per far sì che gli interessati ne prendano visione e ne comprendano i contenuti, in coerenza con quanto espresso dal WP29 nel parere n. 2 dell'8 giugno 2017 in materia di trattamento dei dati sul posto di lavoro.

tiva privacy, allo scopo di rendere edotto il lavoratore circa le operazioni di trattamento dei suoi dati personali poste in essere, anche, nell'ambito del potere di controllo del datore di lavoro.

L'adeguatezza dell'informazione da fornire al lavoratore dovrà valutarsi caso per caso "considerando l'idoneità della stessa di mettere a conoscenza il lavoratore, in maniera dettagliata, almeno: a) di quali sono gli strumenti, presenti in azienda o utilizzati direttamente o indirettamente dal lavoratore, dai quali può derivare una possibilità di controllo a distanza dell'attività lavorativa; b) di quali sono le modalità con le quali è possibile utilizzare gli strumenti forniti dal datore di lavoro, soprattutto con riferimento alla eventuale possibilità di utilizzare quegli stessi strumenti per finalità personali; c) delle modalità con cui potranno essere eseguiti dei controlli sui dati registrati dallo strumento installato in azienda e/o messo a disposizione del lavoratore" (quando, come e perché)[86].

Dal necessario rispetto dell'obbligo di informazione trasparente, si evince chiaramente come uno dei capisaldi dell'impianto di tutela in materia di controllo a distanza sia la "verificabilità del corretto procedimento di trattamento dei dati" da parte del lavoratore che, da un lato, preclude la legittimità di controlli occulti e, dall'altro, deve consentirgli la piena consapevolezza dell'intero *iter* di trattamento dei dati personali ai fini della sua migliore possibilità di difesa in caso di manipolazione o utilizzo dei dati non consentito[87]. Dal dettato normativo non si ricava alcuna prescrizione in ordine alle modalità e alla forma dell'informazione adeguata, ma in considerazione delle sue finalità, sembra senz'altro preferibile la redazione di una informativa a carattere individuale che dia conto in modo mirato delle attività di controllo a cui è soggetto il singolo lavoratore anziché di tipo collettivo. Ciascun lavoratore dovrà comprendere attraverso quali strumenti si concreta l'attività di controllo nei suoi confronti e, nel caso questi fossero a lui affidati per l'espletamento delle sue mansioni, come il loro uso si raccordi con l'attività di controllo, quale tipologia di dati saranno trattati e quali i margini di utilizzabilità.

Premessa la diversità, sul piano finalistico e dei contenuti, tra informazione statutaria e informativa *privacy*, non è esclusa la possibilità di adempiere agli obblighi di legge attraverso la redazione e la notifica al lavoratore di un unico documento che contenga tutte le informazioni prescritte dalle due discipline legali. La soluzione è prospettabile in chiave di semplificazione degli adempimenti (limitati ad un'unica comunicazione) e sembra suggeribile in considerazione della stretta correlazione delle informazioni da trasmettere ai lavoratori, nonché in vista della necessaria gestione globale dell'attività di controllo e di trattamento dei dati.

86 Cit. Alvino, *op. cit.*, pag. 28.

87 Cit. A. Maresca, *op. cit.*, pag. 22.

Qualora non si opti per la trasmissione al lavoratore di un documento informativo unico, i titolari del trattamento dovranno trasmettere ai lavoratori *in primis* l'informativa *privacy*, avendo cura in un secondo momento di rendere l'eventuale ulteriore informazione statutaria. La normativa, infatti, non richiede che i predetti adempimenti debbano essere contestuali, ma ne detta implicitamente una "cronologia" desumibile dalle finalità e dalle conseguenze della loro mancata realizzazione. Infatti, mentre la mancanza della informazione statutaria rende inutilizzabili i dati raccolti ai fini del rapporto di lavoro, l'assenza della informativa *privacy* rende illegittimo il trattamento stesso dei dati. Il titolare del trattamento, dunque, dovrà fornire l'informativa ai lavoratori preliminarmente alla attivazione dei sistemi tecnologici di controllo, o tuttalpiù contestualmente ad essa, potendo semmai decidere di procrastinare l'ulteriore informazione statutaria nella consapevolezza, però, che i dati raccolti non saranno utilizzabili. In ogni caso, a fronte della notifica dell'informativa non è richiesta alcuna accettazione da parte del lavoratore, il quale dovrà limitarsi a prendere conoscenza dei suoi contenuti. In proposito, poiché il titolare del trattamento è onerato della prova aver efficacemente informato i lavoratori, è opportuno che notifichi in forma scritta l'informativa così da poter conservare una ricevuta di avvenuta comunicazione, sia essa cartacea o elettronica.

L'utilizzabilità dei dati a tutti fini del rapporto di lavoro prevista dal nuovo art. 4, comma 3, St. Lav., peraltro, impone una riflessione in ordine all'adeguatezza della richiamata informazione rispetto agli specifici fini disciplinari perseguibili dal datore di lavoro. Dalla norma non si ricava alcuna indicazione circa la necessità di integrare l'informazione da rendere al lavoratore con l'indicazione delle conseguenze sanzionatorie previste per l'eventuale uso scorretto della strumentazione tecnologica affidatagli. Al contrario, appare pressoché superfluo constatare che nulla vieta al datore di lavoro di darne comunque evidenza nell'ambito della adeguata informazione. Si badi, però, questa circostanza non assume alcun rilievo rispetto alla successiva sanzionabilità del comportamento censurato al lavoratore, poiché le disposizioni legali di procedimentalizzazione del potere disciplinare impongono al datore di lavoro tali specificazioni esclusivamente nel codice disciplinare affisso in luogo accessibile a tutti i lavoratori, come previsto dall'art. 7 St. Lav., ai fini della loro valida contestazione.

In ultima analisi, la salvaguardia dei diritti conoscitivi del lavoratore nell'ambito dell'attività di controllo impone al datore di lavoro titolare del trattamento tre livelli di informazione, la cui graduale ottemperanza si rende rispettivamente necessaria per la raccolta, il trattamento e la successiva utilizzabilità dei dati personali.

3.3. La valutazione d'impatto sulla protezione dei dati

In conformità con il principio di responsabilizzazione (*accountability*), il nuovo sistema *privacy* richiede al datore di lavoro, in qualità di titolare del trattamento dati, che il controllo a distanza dei lavoratori effettuato tramite strumenti tecnologici debba essere preceduto dalla valutazione d'impatto sulla protezione dei dati (in inglese *Data Protection Impact Assessment*, d'ora in poi anche DPIA), ogniqualvolta il controllo tecnologico operato presenti rischi potenziali elevati per i diritti e le libertà del lavoratore. La DPIA si sostanzia in un processo di autovalutazione dal quale deve emergere dettagliatamente l'origine, la natura, la particolarità e la gravità dei rischi implicati nell'attività di controllo, nonché le misure apprestate per il loro contrasto.

L'istituto è introdotto e disciplinato dall'art. 35 del regolamento europeo n. 679/2016, il quale prescrive l'obbligo di preventiva valutazione di impatto sulla protezione dei dati in considerazione della natura, l'oggetto, il contesto e le finalità del trattamento (v. considerando 84 GDPR).

Il contenuto minimo della DPIA è specificato dall'articolo 35, paragrafo 7, come segue:

a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;
b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;
c) una valutazione dei rischi per i diritti e le libertà degli interessati;
d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione.

Come chiarito nel considerando 84 GDPR, l'esito della valutazione deve essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali sia conforme al regolamento generale. Quest'ultimo, non individua in concreto i casi di insorgenza dell'obbligo di valutazione lasciando all'interprete il compito di qualificare la fattispecie concreta[88]. In particolare il comma 3, art. 35, GDPR, prevede che la DPIA sia obbligatoria in tre ipotesi:

88 Si tenga conto che la questione non è di scarsa rilevanza, anche perché il GDPR, in caso di violazione della disciplina in materia di DPIA, prevede l'applicabilità di una sanzione amministrativa pecuniaria fino a 10.000.000 di euro o, per le imprese, fino al 2% del fatturato mondiale totale annuo dell'esercizio precedente, se superiore.

a) quando il titolare del trattamento intenda effettuare una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche;
b) quando il trattamento, operato su larga scala, interessi i dati personali sensibili classificati dal legislatore comunitario come "categorie particolari di dati personali", elencati all'art. 9, par. 1, GDPR[89]; nonché interessi i dati personali relativi alle condanne penali e ai reati di cui all'articolo 10, GDPR[90];
c) quando il trattamento implichi la sorveglianza sistematica su larga scala di una zona accessibile al pubblico.

Le modalità tipiche con le quali è generalmente esercitato il potere di controllo a distanza dei lavoratori portano ad escludere che il presupposto applicativo della DPIA sia rinvenibile nella lettera b) o c), comma 3, art. 35 del GDPR, poiché, con specifico riguardo al contesto lavorativo, è improbabile che il trattamento sia configurato su "larga scala", almeno secondo il significato che a tale locuzione è possibile attribuire in via interpretativa[91].
Diversamente, non è infrequente che il controllo nei luoghi di lavoro sia operato attraverso il monitoraggio regolare e sistematico delle attività del prestatore di lavoro, anche ai fini di una valutazione quali-quantitativa dell'attività svolta[92].

---

89 I dati personali annoverati dall'art. 9, par. 1, GDPR sono quelli che rivelano "l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale", nonché quelli inerenti i "dati genetici, dati biometrici intesi a identificare in modo univoco una persona fisica, dati relativi alla salute o alla vita sessuale o all'orientamento sessuale della persona".

90 Ai sensi dell'art. 10, GDPR, "il trattamento dei dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza sulla base dell'articolo 6, paragrafo 1, deve avvenire soltanto sotto il controllo dell'autorità pubblica o se il trattamento è autorizzato dal diritto dell'Unione o degli Stati membri che preveda garanzie appropriate per i diritti e le libertà degli interessati. Un eventuale registro completo delle condanne penali deve essere tenuto soltanto sotto il controllo dell'autorità pubblica".

91 Il regolamento non definisce cosa rappresenti un trattamento "su larga scala". Una soluzione interpretativa è stata elaborata dal Gruppo di lavoro articolo 29 per la protezione dei dati nelle "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243. Secondo il Gruppo di lavoro per stabilire se un trattamento sia effettuato su larga scala occorre prendere in considerazione: il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento; il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento; la durata, ovvero la persistenza, dell'attività di trattamento; la portata geografica dell'attività di trattamento.

92 Anche per quanto attiene alla nozione di "monitoraggio regolare e sistematico", cfr. le "Linee guida sui responsabili della protezione dei dati" del 5 aprile 2017, WP 243. Secondo il Gruppo di lavoro, il carattere della

A titolo esemplificativo, i controlli datoriali effettuati sui terminali elettronici e informativi dei dipendenti, il monitoraggio della navigazione Internet e degli account di posta elettronica aziendali, la videosorveglianza e la geolocalizzazione sono tutte attività che, se realizzate con sistematicità o metodicità, richiederanno l'adempimento della DPIA. Altresì, la valutazione preventiva di impatto è obbligatoria quando il trattamento è finalizzato alla profilazione dei lavoratori, nonché allo svolgimento di attività predittive riguardanti il loro rendimento professionale, l'affidabilità o il comportamento, l'ubicazione o i loro spostamenti[93].

L'esistenza di presupposti giuridici di applicazione della DPIA di tipo "aperto" suggerisce un'interpretazione estensiva della disposizione normativa volta all'allargamento della casistica soggetta a valutazione di impatto del trattamento dati, anche sulla scorta dell'impostazione prudenziale assunta in merito dal Garante della privacy italiano con la pubblicazione dell'elenco delle tipologie di trattamenti soggetti al requisito di valutazione (allegato al provvedimento n. 467, 11 ottobre 2018)[94].

Non è rilevante ai fini della determinazione dell'insorgenza dell'obbligo di DPIA che il controllo avvenga attraverso gli strumenti tecnologici di cui all'art. 4, co.1, St. Lav., oppure attraverso strumenti esentati dalla procedura di autorizzazione preventiva all'installazione ai sensi del comma 2 dell'art. 4, St. Lav. (strumenti di lavoro o per la registrazione degli accessi e delle presenze). Qualora, però, il trattamento dei dati personali avvenga tramite strumentazione la cui installazione è subordinata al positivo esperimento della procedura autorizzatoria statutaria e, al contempo, sia soggetto a DPIA, si rende necessario comprendere quale rapporto vi sia tra gli adempimenti preventivi. Mancando, nelle rispettive disposizioni normative, alcuna espressa connessione tra le due procedure, deve concludersi che l'autonomo esperimento di ciascuna possa essere condotto legittimamente. D'altronde, finalisticamente, gli adempimenti sono preordinati all'accertamento di condizioni di legittimità diverse. Nel primo caso, l'autorizzazione preventiva all'installazione degli strumenti di derivazione statutaria è necessaria per la verifica

---

sistematicità è riscontrabile, alternativamente, quando il trattamento avviene per sistema; è predeterminato, organizzato o metodico; ha luogo nell'ambito di un progetto complessivo di raccolta di dati; è svolto nell'ambito di una strategia.

93 Il Garante per la privacy italiano è intervenuto in merito redigendo un *Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati*, cfr. Allegato 1, al Provvedimento n. 467, 11 ottobre 2018, del Garante per la protezione dei dati personali.

94 Le prime indicazioni utili sono state fornite dal WP29 nelle *Linee-guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del regolamento 2016/679 del 2017* (la prima versione è del 4 aprile 2017, successivamente emendata il 4 ottobre 2017), ove si sostiene l'obbligatorietà della DPIA nel caso in cui "un'Azienda controlli sistematicamente le attività dei dipendenti, compreso l'utilizzo dei terminali informatici, la navigazione su Internet, ecc.".

della sussistenza delle esigenze legittimanti, esclusivamente, di tipo organizzativo, produttivo, per la sicurezza del lavoro e per la tutela del patrimonio aziendale. Nel secondo caso, l'autovalutazione *privacy* è finalizzata alla individuazione dei rischi del trattamento dati e delle misure da adottare per la loro minimizzazione.

In considerazione, però, della stretta correlazione tra gli adempimenti, talché l'inadempimento dell'uno o dell'altro impedisce indifferentemente il trattamento dei dati, è opportuno che il datore di lavoro provveda a verificarne complessivamente le condizioni di legittimità. Sul piano pratico-applicativo, la gestione efficace ed efficiente dei processi suggerirebbe di far precedere la DPIA alla richiesta di autorizzazione all'installazione degli impianti atti al controllo del personale, per almeno due ordini di ragioni. In primo luogo perché in fase di DPIA potrebbero emergere elementi preclusivi al trattamento dei dati per il superamento dei quali sia richiesta, a fini prevenzionistici, una modifica della architettura tecnologica atta al controllo dei lavoratori. In secondo luogo, qualora nelle unità produttive interessate agiscano rappresentanze sindacali aziendali (RSA, RSU), il datore di lavoro potrebbe essere da queste sollecitato a rendere conto del positivo esito della DPIA durante la fase di negoziazione sindacale. In proposito, infatti, vista l'ampiezza del raggio di azione sindacale rientra senz'altro tra le prerogative delle RSA o RSU la possibilità di chiedere in sede negoziale rassicurazioni e riscontri in materia *privacy* ai fini della più ampia tutela degli interessi dei lavoratori.

Peraltro, un simile approccio pratico appare in sintonia con la possibilità compendiata dall'art. 35, comma 9, GDPR, ai sensi del quale il titolare del trattamento raccoglie le opinioni degli interessati o dei loro rappresentanti sul trattamento previsto[95].

Nell'ipotesi in cui manchino le rappresentanze sindacali nell'unità produttiva interessata o non sia possibile raggiungere un accordo, il datore di lavoro dovrà avviare la procedura amministrativa inoltrando apposita istanza di autorizzazione alla sede territoriale competente dell'Ispettorato nazionale del lavoro. In assenza di specifiche disposizioni normative, all'Ispettorato non è riconosciuta la facoltà di verificare l'adempimento della DPIA e quale "risultato" in termini di *risk analisys* ne sia scaturito, essendo soltanto tenuto alla verifica di legittimità delle esigenze legittimanti l'installazione degli impianti e delle modalità di controllo. D'altronde, questo appare desumibile dal modulo di istanza di autorizzazione all'installazione degli strumenti di controllo, ai sensi dell'art. 4, St. Lav., adottato dall'Ispettorato nazionale del lavoro (Moduli INL 1, 1.1, 1.2) nel quale, in materia di *privacy*, è richiesto soltanto al datore di lavoro di dichiarare che "sarà rispettata la disciplina dettata dal Regolamento UE 2016/679 in materia di trattamento dei dati personali".

95 Cfr. diagramma Garante *privacy* in appendice.

Nulla vieta al datore di lavoro, pertanto, di poter provvedere in un secondo momento alla valutazione di impatto, nonostante restino anche in questo caso valide le ragioni di opportunità che, al contrario, spingono a preordinare la DPIA alla richiesta di autorizzazione o alla installazione fisica degli impianti di controllo in considerazione della possibilità che dalla autovalutazione sui rischi *privacy* emerga la necessità di interventi correttivi della infrastruttura tecnologica.

A questo si aggiunga, peraltro, che nell'eventualità in cui si dovesse accertare in sede di valutazione di impatto che il trattamento presenti un rischio elevato a fronte del quale il titolare del trattamento non sia in condizione di adottare idonee contromisure, si renderà necessario consultare preventivamente il Garante, che sarà chiamato ad esprimere un parere di conformità del trattamento alla normativa alla quale il titolare del trattamento dovrà attenersi[96].

In ultima analisi, il trattamento dati conseguente alla attività di controllo a distanza, disciplinata dall'art. 4, St. Lav., difficilmente potrà prescindere dall'adempimento della DPIA, fatta eccezione per quei casi residuali in cui il trattamento dovesse rivelarsi privo di sistematicità, non organizzato, né predeterminato e metodico. Così circoscritta, la casistica parrebbe risolversi alle ipotesi di controllo sulle strumentazioni di lavoro qualora lo stesso sia effettuato soltanto al ricorrere di eventi eccezionali. Si pensi all'attività di controllo e trattamento dati operata dal datore di lavoro su un computer messo a disposizione del lavoratore per l'adempimento della propria prestazione lavorativa solo nel caso di intrusione da parte di hacker informatici, senza che questa sia predeterminata o organizzata.

3.4. Il rispetto dei principi regolatori sanciti dalla normativa privacy

In conseguenza della centralità assunta dalla disciplina privacy nel nuovo testo dell'art. 4 St. Lav., l'esercizio del potere di controllo del datore di lavoro è assoggettato al rispetto delle regole e dei principi generali attualmente enunciati dall'art. 5 GDPR[97]. L'ampiezza

96 L'art. 36, par. 2, GDPR, prevede che: "Se ritiene che il trattamento previsto di cui al paragrafo 1 violi il presente regolamento, in particolare qualora il titolare del trattamento non abbia identificato o attenuato sufficientemente il rischio, l'autorità di controllo fornisce, entro un termine di otto settimane dal ricevimento della richiesta di consultazione, un parere scritto al titolare del trattamento e, ove applicabile, al responsabile del trattamento e può avvalersi dei poteri di cui all'articolo 58. Tale periodo può essere prorogato di sei settimane, tenendo conto della complessità del trattamento previsto. L'autorità di controllo informa il titolare del trattamento e, ove applicabile, il responsabile del trattamento di tale proroga, unitamente ai motivi del ritardo, entro un mese dal ricevimento della richiesta di consultazione. La decorrenza dei termini può essere sospesa fino all'ottenimento da parte dell'autorità di controllo delle informazioni richieste ai fini della consultazione.

97 Ai sensi dell'art. 5 GDPR, i dati personali sono: a) trattati in modo lecito, corretto e trasparente nei confronti dell'interessato («liceità, correttezza e trasparenza»); b) raccolti per finalità determinate, esplicite e legittime, e

e le modalità di controllo, in particolare, sono condizionate dai principi di finalità e minimizzazione del trattamento che impongono al titolare di garantire che i dati personali siano "raccolti per finalità determinate, esplicite e legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità". Il trattamento, al contempo, deve presentarsi adeguato, pertinente e limitato a quanto necessario rispetto alle finalità per le quali si è inteso operarlo.

Prima dell'emanazione del regolamento UE, simili principi erano già presenti nell'ordinamento interno. Con il d.lgs. n. 196/2003 (codice *privacy*), infatti, il legislatore aveva già sancito il "principio di necessità nel trattamento dei dati" (*ex* art. 3) e prescritto specifiche modalità di raccolta e utilizzazione la cui violazione comportava l'impossibilità di utilizzazione dei dati (*ex* art. 11)[98]. I principi hanno trovato conferma e ampliamento nel GDPR, tanto che con il d.lgs. n. 101 del 10 agosto 2018, in una prospettiva di adeguamento della norma interna con quella sovraordinata di tipo regolamentare, gli articoli 3 e 11 del codice *privacy* sono stati abrogati in quanto ormai ricompresi nella portata dell'art. 5 GDPR.

In buona sostanza, il principio di necessità impone che ogni trattamento di dati personali sia operato in modo da evitare che gli interessati siano identificati quando le finalità

---

successivamente trattati in modo che non sia incompatibile con tali finalità; un ulteriore trattamento dei dati personali a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici non è, conformemente all'articolo 89, paragrafo 1, considerato incompatibile con le finalità iniziali («limitazione della finalità»); c) adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati («minimizzazione dei dati»); d) esatti e, se necessario, aggiornati; devono essere adottate tutte le misure ragionevoli per cancellare o rettificare tempestivamente i dati inesatti rispetto alle finalità per le quali sono trattati («esattezza»); e) conservati in una forma che consenta l'identificazione degli interessati per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati; i dati personali possono essere conservati per periodi più lunghi a condizione che siano trattati esclusivamente a fini di archiviazione nel pubblico interesse, di ricerca scientifica o storica o a fini statistici, conformemente all'articolo 89, paragrafo 1, fatta salva l'attuazione di misure tecniche e organizzative adeguate richieste dal presente regolamento a tutela dei diritti e delle libertà dell'interessato («limitazione della conservazione»); f) trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»).

98 Ai sensi degli abrogati artt.3 e 11, d.lgs. n. 196/2003, i sistemi informativi e i programmi informatici avrebbero dovuto essere configurati riducendo al minimo l'utilizzazione di dati personali e di dati identificativi, "in modo da escluderne il trattamento quando le finalità perseguite nei singoli casi possono essere realizzate mediante, rispettivamente, dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità". Inoltre, I dati personali oggetto di trattamento erano : a) trattati in modo lecito e secondo correttezza; b) raccolti e registrati per scopi determinati, espliciti e legittimi, ed utilizzati in altre operazioni del trattamento in termini compatibili con tali scopi; c) esatti e, se necessario, aggiornati; d) pertinenti, completi e non eccedenti rispetto alle finalità per le quali sono raccolti o successivamente trattati; e) conservati in una forma che consenta l'identificazione dell'interessato per un periodo di tempo non superiore a quello necessario agli scopi per i quali essi sono stati raccolti o successivamente trattati.

perseguite non lo richiedano né lo impongano. Le restrizioni sulla identificabilità degli interessati possono dirsi oggi riassunte nelle regole di non eccedenza e pertinenza, logico corollario del principio di minimizzazione sancito dal GDPR.
Con specifico riferimento al rapporto di lavoro, sia pubblico che privato, è opportuno evidenziare che i provvedimento dell'Autorità italiana garante della *privacy* hanno declinato a livello operativo i principi generali del GDPR. In proposito, con il provvedimento 13 dicembre 2018, n. 497 (doc. web n. 9068972), il Garante, nelle more dell'adozione delle regole deontologiche previste dal d.lgs. n. 101/2018, ha individuato le prescrizioni contenute nell'autorizzazione generale n. 1/2016 in materia di lavoro ritenute compatibili con la norma regolamentare europea e il Codice *privacy* ultimamente adeguato.

4. Forme di controllo a distanza e tecnologie a disposizione del datore di lavoro

La peculiarità e la pervasività delle strumentazioni tecnologiche che consentono al datore di lavoro di trattare dati personali dei propri dipendenti e collaboratori costituiscono un fattore di rischio per la riservatezza di questi ultimi che l'ordinamento intende tutelare attraverso la prescrizione di limitazioni e accorgimenti. Di seguito, si analizzeranno sinteticamente le condizioni di liceità del trattamento dei dati connesso all'esercizio delle più comuni forme di controllo a distanza dei lavoratori, alla luce delle linee guida emanate dalle Autorità Europee in materia di protezione dei dati, nonché i pareri, le *best practices* e i provvedimenti del Garante italiano di particolare importanza per l'argomento in esame.

4.1. Videosorveglianza

Il controllo operato attraverso sistemi di videosorveglianza è una pratica molto diffusa negli ambienti di lavoro. Negli ultimi anni i sistemi di monitoraggio video sono notevolmente cambiati, principalmente con riferimento alla riduzione delle dimensioni delle telecamere, associata ad un aumento della capacità di definizione delle immagini, alla possibilità di accedere facilmente a distanza ai dati raccolti tramite smartphone, all'implementazione di tecniche di analisi delle immagini e della c.d. videosorveglianza intelligente.
Sono in commercio numerose soluzioni di analisi video che permettono, ad esempio, l'attivazione di funzioni di *motion detection* e *motion tracking*[99] o il rilevamento auto-

99 Sistemi software in grado di rilevare e registrare il movimento di una persona o di un oggetto nello spazio.

matizzato delle espressioni facciali, al fine di individuare deviazioni da modelli di movimento predefiniti.

L'utilizzo delle descritte tecnologie sul posto di lavoro complica, rispetto ai sistemi "classici" di videosorveglianza, il quadro di valutazione della *compliance* allo Statuto dei lavoratori (stante il divieto di installazione di apparecchiature preordinate al controllo, ai sensi dell'art. 4, co. 1, St. Lav.), nonché alla normativa *privacy*, considerata l'incisiva pervasività di tali sistemi nella sfera di riservatezza del lavoratore. Il trattamento delle immagini dei lavoratori basato su sistema di monitoraggio video potrebbe essere realizzato per il soddisfacimento di esigenze organizzative o produttive, ovvero di sicurezza del lavoro seppure nel rigoroso rispetto delle garanzie poste a presidio dei diritti e delle libertà del lavoratore.

Indicazioni circa la conformità del trattamento delle immagini alla normativa in materia di protezione dei dati personali si rinvengono da ultimo nelle linee guida 3/2019 sul trattamento dei dati personali attraverso dispositivi video, elaborate dal Comitato europeo per la protezione dei dati (Edpb). Sul piano pratico, inoltre, il provvedimento in materia di videosorveglianza adottato dal Garante privacy in data 8 aprile 2010 continua a offrire spunti utili nonostante gli anni trascorsi dall'adozione del documento abbiano visto l'evolversi della tecnologia in maniera molto incisiva[100].

Perché l'attività di videosorveglianza sia conforme alla disciplina privacy, gli scopi perseguiti attraverso l'attività di controllo è necessario che siano documentati per iscritto e messi a conoscenza dei lavoratori interessati dal trattamento, ai sensi dell'art. 13 GDPR, non essendo sufficiente che gli stessi siano specificati nella sola istanza preventiva di autorizzazione alla installazione di impianti presentata all'Ispettorato nazionale del lavoro.

Come confermato dalle succitate linee guida Edpb, in linea di principio, seppure ogni base giuridica di cui all'art. 6, par. 1, possa fornire una base giuridica utile per l'elaborazione dei dati di videosorveglianza, nella pratica i presupposti di legittimità del trattamento si rinvengono, per lo più, nel legittimo interesse (*ex* art. 6, par. 1, lett. f) o nella necessità di procedere al trattamento di dati da parte di autorità pubbliche nell'esecuzione dei loro compiti (*ex* art. 6, par. 1, lett. e).

Qualora il lavoratore interessato si opponga alla videosorveglianza, il titolare del trattamento potrà effettuarla soltanto qualora l'interesse legittimo sia prevalente rispetto agli interessi, i diritti e le libertà dell'interessato o per l'istituzione, l'esercizio o la difesa di rivendicazioni legali. L'esistenza dell'interesse legittimo deve essere verificata rispetto

100 Garante italiano per la protezione dei dati personali, Provvedimento in materia di videosorveglianza - 8 aprile 2010.

alla attualità e l'entità della problematica che rende necessario avviare la videosorveglianza nei luoghi di lavoro[101].

I principi di legittimità e determinatezza del fine perseguito, nonché di proporzionalità, correttezza e non eccedenza del trattamento, impongono una gradualità nell'ampiezza e tipologia di monitoraggio che rende residuali i controlli più invasivi, legittimandoli solo a fronte della rilevazione di specifiche anomalie e comunque all'esito dell'esperimento di misure preventive meno limitative dei diritti dei lavoratori[102]. Ciò rileva in particolare per l'utilizzo delle nuove tecnologie di videosorveglianza, di cui si sono accennate le principali evoluzioni.

Secondo il principio di necessità, i dati personali trattati devono essere adeguati, pertinenti e limitati a quanto necessario in relazione alle finalità per i quali vengono elaborati ("minimizzazione dei dati"). Pertanto, l'installazione di un sistema di videosorveglianza deve sempre essere preceduta da un esame critico atto a verificare che le misure di controllo adottate sono adatte al raggiungimento dell'obiettivo desiderato nonché adeguate e necessarie ai suoi scopi. Inoltre, il controllo a distanza tramite videosorveglianza dovrebbe essere scelto solo qualora lo scopo del trattamento non possa ragionevolmente essere raggiunto da altri mezzi meno invasivi dei diritti e delle libertà fondamentali dell'interessato[103].

La prassi decisoria del Garante italiano e i principali documenti del WP29 hanno confermato un'interpretazione restrittiva della legittimità delle tecnologie più invasive, esprimendo un orientamento fortemente garantista per il lavoratore. In particolare, il Garante ha autorizzato, in un caso di verifica preliminare, l'installazione sul posto di lavoro di un sistema di analisi video in grado di rilevare e registrare i movimenti delle persone nello spazio, poiché il titolare era stato in grado di dimostrare la sussistenza di oggettive esi-

101 Nelle linee guida 3/2019, il Comitato europeo per la protezione dei dati (Edpb) ribadisce che il legittimo interesse deve esistere realmente e deve rappresentare un problema attuale (cioè non deve essere immaginario o speculativo). In via esemplificativa, riferendosi a situazioni reali di pericolo, di protezione della proprietà da furto o vandalismo, l'Edpb precisa che prima di iniziare la sorveglianza, alla luce del principio di responsabilità, i titolari del trattamento sarebbero invitati a documentare gli incidenti rilevanti (data, modalità, perdita finanziaria). Tali incidenti documentati possono essere una prova evidente dell'esistenza di un interesse legittimo. L'imminenza della situazione di pericolo può essere presunta e, dunque, costituire un interesse legittimo nel caso di negozi preposti alla vendita di beni preziosi (ad es. gioiellieri) o attività tipicamente esposte al rischio di crimini contro proprietà (ad es. stazioni di benzina).

102 Principio esplicitato dal Garante nel provvedimento sopra citato e condiviso anche dall'Ispettorato Nazionale del Lavoro nella circolare n. 5 del 19 febbraio 2018.

103 Cfr. linee guida Edpb n.3/2019, pag. 8.

genze di sicurezza e, in ogni caso, le telecamere potevano essere attivate esclusivamente durante l'orario extra-lavorativo[104].

Considerazioni diverse, invece, valgono per quelle tecnologie in grado di rilevare le espressioni facciali al fine di individuare deviazioni da modelli standard: l'utilizzo da parte del datore di lavoro appare sproporzionato rispetto alla finalità da perseguire[105]. In applicazione del principio di proporzionalità, nei casi in cui sia stato scelto un sistema che preveda la conservazione delle immagini, questa deve essere temporanea e commisurata al tempo necessario (e predeterminato) a raggiungere la finalità perseguita. In particolare "la conservazione deve essere limitata a poche ore o, al massimo, alle ventiquattro ore successive alla rilevazione", fatte salve speciali esigenze di ulteriore conservazione in forza delle quali tale periodo potrebbe essere esteso a non oltre sette giorni[106].

Il sistema impiegato dovrebbe essere programmato in modo da operare, allo scadere del termine previsto, l'integrale cancellazione automatica da ogni supporto delle informazioni, anche mediante sovra-registrazione, con modalità tali da rendere non riutilizzabili i dati cancellati[107]. Al ricorrere di specifiche esigenze, non è da escludere la possibilità di un monitoraggio in tempo reale, qualora questa modalità di controllo sia necessaria rispetto allo scopo perseguito. Poiché il monitoraggio in tempo reale potrebbe presenta-

---

104 V. Garante italiano per la protezione dei dati, provvedimento n. 276 /2018, *Verifica preliminare. Installazione di sistemi di videosorveglianza c.d. intelligenti - 9 maggio 2018*.

105 Impostazione condivisa dal Gruppo di lavoro articolo 29, Parere n.2/2017 dell'8 giugno 2017 in materia di trattamento dei dati sul posto di lavoro.

106 Cfr. Garante italiano per la protezione dei dati, *Provvedimento in materia di videosorveglianza* del 8 aprile 2010. Secondo l'Autorità, estensioni del periodo di conservazione sarebbero possibili in relazione a festività o chiusura di uffici o esercizi, nonché nel caso in cui si aderisse ad una specifica richiesta investigativa dell'autorità giudiziaria o di polizia giudiziaria. Solo in alcuni casi, per peculiari esigenze tecniche (mezzi di trasporto) o per la particolare rischiosità dell´attività svolta dal titolare del trattamento (ad esempio, per alcuni luoghi come le banche può risultare giustificata l´esigenza di identificare gli autori di un sopralluogo nei giorni precedenti una rapina), può ritenersi ammesso un tempo più ampio di conservazione dei dati che, sulla scorta anche del tempo massimo legislativamente posto per altri trattamenti, si ritiene non debba comunque superare la settimana. Nella vigenza della procedura di verifica preliminare, ora sostituita, per alcuni aspetti, dalla consultazione preventiva ex art. 36 GDPR , in tutti i casi in cui il titolare del trattamento avesse inteso procedere a un allungamento dei tempi di conservazione per un periodo superiore alla settimana, avrebbe dovuto sottoporre una richiesta in tal senso alla verifica preliminare del Garante, sostenuta da adeguata motivazione con riferimento ad una specifica esigenza di sicurezza perseguita, in relazione a concrete situazioni di rischio riguardanti eventi realmente incombenti e per il periodo di tempo in cui venga confermata tale eccezionale necessità.

107 A proposito di tempi di conservazione delle immagini in materia di videosorveglianza dei locali aziendali, v. Garante italiano per la protezione dei dati personali, provvedimento n. 21/2019, con il quale l'Autorità sanziona un datore di lavoro esercente attività commerciale a causa delle conservazione delle immagini registrate per un periodo di 15 giorni, in assenza di particolari esigenze; v. altresì provvedimento n.39/2019, un datore di lavoro viene sanzionato per allungamento dei tempi di conservazione delle immagini a 12 giorni

re dei profili di maggiore rischio rispetto alla memorizzazione e successiva eliminazione automatica del materiale dopo un periodo limitato di tempo, il titolare del trattamento dovrà conformare l'attività di controllo al principio di minimizzazione.
Per quel che concerne l'aspetto relativo alla sicurezza del trattamento, come noto, il GDPR ha eliminato il riferimento alle misure di sicurezza "minime", sostituendolo con quello alle misure tecniche e organizzative "adeguate" al rischio, ovvero oggetto di valutazione caso per caso da parte del titolare del trattamento (ex art. 32, par.1).
L'elenco delle misure minime di sicurezza in materia di videosorveglianza, messo a punto dal Garante, rimane, quindi, un paradigma di riferimento nell'individuazione di specifici accorgimenti da adottare nel rispetto dei principi di liceità, minimizzazione, esattezza, limitazione della conservazione, di cui all'art. 5 GDPR, ovvero: previsione di diversi livelli di visibilità delle immagini, in base alle differenti competenze dei singoli operatori; predisposizione di misure per la cancellazione, anche in forma automatica, delle registrazioni; accesso limitato ai soggetti dotati di credenziali di autenticazione abilitanti alla visione delle immagini e, nel caso di interventi derivanti da esigenze di manutenzione, accesso ai dati consentito ai soggetti terzi preposti a tali operazioni solo se ciò si renda indispensabile al fine di effettuare eventuali verifiche tecniche, comunque in presenza di soggetti dotati di credenziali di autenticazione abilitanti; applicazione di tecniche crittografiche nel caso in cui le immagini vengano trasmesse su una rete pubblica (internet)[108].
Inoltre, a tutela della dignità e della riservatezza del lavoratore, non è mai ammesso l'uso di telecamere in spazi riservati al personale, quali bagni, spogliatoi, docce, armadietti e luoghi ricreativi[109].
Per garantire un'adeguata informazione agli interessati, in aggiunta all'informativa completa di cui al paragrafo 2.2 del presente lavoro, per prassi consolidata in linea con le indicazioni del Comitato europeo per la protezione dei dati e del Garante privacy italiano viene prescritto l'utilizzo di apposita segnaletica conforme al modello di informativa "minima" riportante l'indicazione del titolare del trattamento e la finalità perseguita. Tutti i soggetti interessati devono essere consapevoli della esistenza e del raggio di azione dell'attività di videosorveglianza nei luoghi di lavoro monitorati, nel rispetto degli obblighi generali in materia di trasparenza e informazione stabiliti dall'art. 12 GDPR[110].
In proposito, il Comitato europeo per la protezione dei dati (Ebdp) ha precisato che, alla luce del volume di informazioni che è necessario fornire all'interessato, i titolari del trat-

108 Già citato, provvedimento in materia di videosorveglianza del 8 aprile 2010, punto 3.3.1

109 V. Garante italiano per la protezione dei dati, "Depliant Videosorveglianza".

110 Le linee guida del gruppo di lavoro "Articolo 29" sulla trasparenza ai sensi del regolamento 2016/679 (WP260)", che sono stati approvati dall'EDPB il 25 maggio 2018, forniscono ulteriori indicazioni su contenuti e modalità della informativa dovuta ai soggetti interessati.

tamento dei dati possono seguire un approccio a più livelli in cui scelgono di utilizzare una combinazione di metodi per garantire la trasparenza (WP260, par. 35; WP89, p. 22). Per quanto riguarda la videosorveglianza, le informazioni più importanti dovrebbero essere visualizzate sul segnale di avvertimento (primo livello) mentre gli ulteriori dettagli obbligatori possono essere forniti con altri mezzi (secondo livello)[111].

Per quello che concerne il primo livello di informazione, nelle linee guida Ebdp 3/2019 viene fornito un esempio di segnaletica che, in combinazione con un'icona grafica, è considerato idoneo a fornire in modo facilmente visibile e intelligibile una panoramica del trattamento previsto come richiesto dall'art. 12, par. 7, GDPR (l'esempio è riportato in appendice, fig. 2)[112]. Per la tutela degli interessati, i cartelli segnaletici devono essere collocati prima del raggio d'azione delle telecamere e devono essere chiaramente visibili in ogni condizione di illuminazione ambientale. La segnaletica non deve necessariamente specificare l'esatta ubicazione delle videocamere, ferma restando la chiarezza circa le aree soggette a monitoraggio e il contesto della sorveglianza[113].

Le informazioni del secondo livello devono essere rese facilmente accessibile all'interessato. Seppure non sia prescritta, a tal fine, una specifica modalità informativa, rendere le informazioni disponibili in modo digitale potrebbe rendere più facile la consultazione da parte degli interessati.

4.2. Posta elettronica e internet

Posta elettronica e navigazione sul web rappresentano oggi degli strumenti di lavoro pressoché imprescindibili e sui quali il datore di lavoro ha spesso interesse a svolgere attività di controllo a diverso titolo.

Secondo autorevole giurisprudenza la posta elettronica aziendale di tipo nominativo rappresenta il domicilio informatico del dipendente, ovvero uno spazio a sua disposizione in via esclusiva[114].

---

111 Cfr. Linee guida Ebdp n.3/2019, pagg. 21, 22.

112 V. Linee guida Ebdp n. 3/2019, pag. 23. Nel documento si precisa che il formato delle informazioni deve essere adattato alla posizione individuale (WP89 p. 22).

113 Il Comitato europeo per la protezione attraverso le linee guida (cfr. pag. 22) ha fornito indicazione esemplificativa del contenuto minimo informativo di "primo livello". La segnaletica di avvertimento deve annoverare i dettagli delle finalità del trattamento, l'identità del responsabile del trattamento e l'esistenza dei diritti di l'interessato, unitamente alle informazioni sui maggiori impatti del trattamento; gli interessi legittimi perseguiti dal responsabile del trattamento (o da una terza parte); i contatti del responsabile della protezione dei dati.

114 Cass. Pen. Sez. IV, sentenza 31 marzo 2016, n. 13057, ove la Corte ha evidenziato che "qualora siano attivate caselle di posta elettronica a nome di uno specifico dipendente, quelle caselle rappresentano il domicilio informatico proprio del dipendente [...]. La casella rappresenta uno spazio a disposizione in via esclusiva della persona, sicché la sua invasione costituisce lesione della riservatezza."

Anche su tali strumenti, naturalmente, si applica il generale divieto di controllo a distanza del lavoratore, che nel caso specifico si sostanzia nel divieto di utilizzo di software al solo scopo di ricostruire minuziosamente le attività svolte dallo stesso.
É il caso, ad esempio, di programmi in grado di leggere e registrare sistematicamente i messaggi di posta elettronica (o dei relativi dati esteriori), al di là di quanto tecnicamente necessario per svolgere il servizio e-mail; o di software in grado di memorizzare sistematicamente le pagine web visualizzate dal lavoratore[115].
Con riferimento invece ai programmi che consentono controlli "indiretti", questi devono, come si è detto in precedenza, conformarsi ad una logica di graduazione e, sulla base dei principi di trasparenza e correttezza del trattamento dei dati, essere tarati sulla prevenzione di comportamenti non diligenti o contrari alle policy aziendali.
Proprio sulla prevenzione, piuttosto che sulla repressione, il Garante, nei documenti di orientamento e nella prassi decisoria, ha sempre posto l'accento, evidenziando che l'adozione di *policy* chiare e trasparenti consente di trattare correttamente i dati ricavabili dalla posta elettronica e internet in uso al dipendente.
In altre parole, il datore di lavoro può scegliere strumenti e modalità che riducano al minimo la capacità intrusiva delle tecnologie nella sfera di riservatezza del lavoratore.
Tra le *best practice* si segnalano: l'adozione di policy aziendali volte a disciplinare l'uso di posta elettronica e internet; l'individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa; la configurazione di sistemi o l'utilizzo di filtri che prevengano determinate operazioni reputate inconferenti con l´attività lavorativa, quali l'upload o l'accesso a determinati siti (inseriti in una sorta di *black list*) e/o il download di file o software aventi particolari caratteristiche (dimensionali o di tipologia di dato). Ad esempio, un sistema di *black list* basato su parole chiave impedirebbe *ex ante* al lavoratore di accedere ai siti web considerati non correlati con la prestazione lavorativa o illegali.
Particolarmente consigliato uno strumento informatico di prevenzione della perdita dei dati in grado di rilevare una mail in uscita come possibile violazione di dati (in ipotesi perché trasferisce un database di clienti), e che invii al mittente, prima della trasmissione del messaggio, un avviso che gli permetta di annullare l'invio[116].

115 Garante italiano per la protezione dei dati personali, deliberazione n. 13/2007 *Lavoro: le Linee Guida del Garante per posta elettronica e internet.*

116 Sistemi di *Data Loss Prevention* (DLP), ovvero tecniche e sistemi che identificano, monitorano e proteggono i dati in uso (ad esempio azioni degli endpoint), i dati in movimento (ad esempio azioni di rete), e dati a riposo (ad esempio la memorizzazione dei dati) all'interno o all'esterno dell'azienda, con il fine di individuare e prevenire l'uso non autorizzato e la trasmissione di informazioni riservate.

Preferibile inoltre una modalità che permetta il trattamento di dati in forma anonima o tale da precludere l'immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai file di *log* riferiti al traffico web, su base collettiva o per gruppi sufficientemente ampi di lavoratori).

Alla luce delle suesposte considerazioni, si evidenziano alcune misure idonee a tutelare la riservatezza del lavoratore: rendere disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it) eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it); invio automatico in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), di messaggi di risposta contenenti le "coordinate" di un altro soggetto o altre utili modalità di contatto della struttura, allo scopo di prevenire l'apertura della posta elettronica; avvertimento, nei messaggi di posta elettronica, ai destinatari nel quale sia dichiarata l´eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell´organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

In applicazione del principio di proporzionalità, la conservazione dei dati relativi agli account aziendali non può svolgersi per tutta la durata del rapporto di lavoro e anche successivamente all'interruzione dello stesso; inoltre gli account nominativi devono essere disattivati dopo la cessazione del rapporto di lavoro[117].

Sono attività vietate, si ripete, quelle deputate esclusivamente al controllo a distanza del lavoratore, quali, ad esempio, l'installazione di software in grado di leggere e registrare i caratteri inseriti tramite la tastiera o i movimenti effettuati col mouse, ovvero l'attivazione di telecamere web e la raccolta di filmati registrati[118].

4.3. La geolocalizzazione

I dispositivi di localizzazione geografica, installati su mezzi o strumenti aziendali o ad uso promiscuo, sono in grado di fornire al datore di lavoro informazioni di tipo statico (la posizione nello spazio) e di tipo dinamico (gli spostamenti nello spazio).

Le informazioni si riferiscono sempre al mezzo (*smartphone*, *tablet*, veicolo o altro strumento mobile in dotazione), ma nel momento in cui rendono identificabile o rintraccia-

---

117 Garante italiano per la protezione dei dati personali, provvedimento n. 53/2018, *Trattamento di dati personali effettuato sugli account di posta elettronica aziendale*. Il Garante vieta ad un'azienda di trattare ulteriormente i dati personali dei lavoratori ricavati dai loro account di posta elettronica in quanto erano raccolte sistematicamente tutte le comunicazioni elettroniche dei dipendenti e la conservazione dei dati veniva prevista per tutta la durata del rapporto di lavoro e anche successivamente all'interruzione dello stesso, in violazione dei principi di necessità, pertinenza e non eccedenza.

118 Garante italiano per la protezione dei dati personali, deliberazione n. 13/2007 *Lavoro: le Linee Guida del Garante per posta elettronica e internet.*

bile il lavoratore, anche indirettamente, costituiscono un trattamento dei dati ai sensi della normativa europea, per cui il datore di lavoro è tenuto ad osservare tutte le prescrizioni generali e specifiche previste dalla legge[119]. Alla luce dell'analisi sistematica precedentemente sviluppata in ordine ai presupposti di legittimità dell'attività di controllo impersonale, il fondamento giuridico del trattamento dei dati connesso all'impiego di dispositivi di geolocalizzazione dei veicoli aziendali è generalmente rinvenibile nel soddisfacimento di esigenze aziendali qualificate ai sensi dell'art. 4, comma 1, St. Lav., a loro volta rilevanti quale declinazione del legittimo interesse del datore di lavoro titolare del trattamento[120]. Come osservato dall'Ispettorato nazionale del lavoro, infatti, si può ritenere che i sistemi di geolocalizzazione rappresentino, in linea di massima e in termini generali, "un elemento "aggiunto" agli strumenti di lavoro, non utilizzati in via primaria ed essenziale per l'esecuzione dell'attività lavorativa, ma per rispondere ad esigenze ulteriori di carattere assicurativo, organizzativo, produttivo o per garantire la sicurezza del lavoro"[121]. In proposito, però, con riferimento alle possibili basi giuridiche del trattamento, si è già detto della possibilità che l'installazione sia prescritta eccezionalmente dalla legge, in questi casi i sistemi di geolocalizzazione sarebbero classificabili alla stregua di strumenti di lavoro e pertanto, impiegabili liberamente, senza il rispetto di vincoli procedurali. Il connesso trattamento dei dati, parimenti, troverebbe legittimazione nell'obbligo legale imposto al datore di lavoro.

In tema di localizzazione dei veicoli aziendali è intervenuto anche il Garante *privacy*, che ha offerto indicazioni su alcune finalità legittimanti un siffatto trattamento quali: esigenze di tipo logistico (al fine di impartire tempestive istruzioni al conducente del veicolo); elaborazione di rapporti di guida (allo scopo di commisurare il tempo di lavoro del conducente, con la conseguente determinazione della retribuzione dovuta, anche in vista dell´assolvimento degli obblighi legali connessi alla tenuta del libro unico del lavoro); calcolo dei costi da imputare alla clientela; efficiente gestione e manutenzione del parco veicoli, con effetti vantaggiosi anche sulla sicurezza sul lavoro e per la sicurezza della collettività; utilizzazione dei dati raccolti in caso di furto del veicolo[122].

---

119 Garante italiano per la protezione dei dati personali, provvedimento n. 427/2018: in tema di geolocalizzazione di veicoli aziendali, il Garante evidenzia che l'identificabilità del lavoratore è resa possibile dall'abbinamento con i turni di lavoro: "sebbene i veicoli non siano assegnati sempre al medesimo dipendente, tuttavia [...] l'identità degli autisti è sempre ricavabile dal programma di lavoro giornaliero".

120 Gruppo di lavoro articolo 29, Parere n. 13/2011 *Servizi di geolocalizzazione su dispositivi mobili intelligenti.*

121 V. circ. INL n.2/2016. L'Ispettorato chiarisce la necessità che, in tali casi, le relative apparecchiature siano installate solo previo accordo stipulato con la rappresentanza sindacale ovvero, in assenza di tale accordo, previa autorizzazione da parte dell'Ispettorato nazionale del lavoro.

122 Garante italiano per la protezione dei dati personali, provvedimento n. 370/2011 *Sistemi di localizzazione dei veicoli nell'ambito del rapporto di lavoro.*

In ossequio ai principi di minimizzazione del trattamento e della c.d. *privacy by default*[123], si deve provvedere a configurare il sistema tecnologico in modo che siano trattati, per impostazione predefinita, solo i dati personali strettamente necessari rispetto alla finalità del trattamento (ad esempio prevedendo la possibilità per il lavoratore di disattivare la localizzazione durante le pause) e non dati ulteriori (quali l'invio di segnali d'allarme in relazione alla velocità del veicolo, o la velocità media del veicolo). I sistemi di localizzazione sui veicoli utilizzati per l'esecuzione di prestazioni lavorative dovranno anche collocare all'interno degli stessi delle vetrofanie recanti la dizione "veicolo sottoposto a localizzazione" o comunque avvisi ben visibili che segnalino la circostanza della geolocalizzazione del veicolo. Nel caso di dispositivi mobili, il sistema dovrà essere configurato in modo che sia visibile un'icona indicante l'attivazione della funzionalità di localizzazione[124]. Sotto il profilo delle concrete modalità operative del sistema tecnologico, occorre sempre rispettare il principio di proporzionalità, in riferimento alla periodicità della rilevazione (la quale non può essere troppo ravvicinata, permettendo la ricostruzione particolareggiata del percorso) e ai tempi di conservazione delle informazioni raccolte (i quali devono essere proporzionati rispetto agli scopi, anche in considerazione della specifica attività lavorativa svolta)[125].

Rispetto alla tendenziale frequenza alla installazione di dispositivi di geolocalizzazione sui veicoli aziendali affidati in uso al personale, è ormai in larga diffusione l'utilizzo di sistemi di localizzazione incorporati in strumenti elettronici portatili sia aziendali sia di proprietà dei lavoratori, adoperati principalmente con finalità di rilevazione delle presenze anche con funzione combinata di registrazione delle entrate e delle uscite da lavoro ad inizio e fine turno. La rilevazione delle presenze può costituire, in determinati casi, una finalità legittima della localizzazione, ad esempio nel caso di dipendenti in

123 Il principio della *data protection by-default* è diretta implicazione del principio di responsabilizzazione del titolare del trattamento e si sostanzia nell'adozione di misure tecniche e organizzative già nella fase di progettazione del sistema di raccolta e trattamento dei dati. Per questi si richiede "protezione per impostazione predefinita", come evidenziato dal considerando 78 GDPR che menziona la pseudonimizzazione e la minimizzazione tra gli accorgimenti funzionali a garantire che vengano trattati solo i dati personali necessari alle finalità perseguite. *Amplius* cfr. L. Bolognini, E. Pelino, C. Bistolfi, *Il regolamento privacy europeo. Commentario alla nuova disciplina sulla protezione dei dati personali*, Giuffrè Editore, pag. 324 ss.

124 Garante italiano per la protezione dei dati personali, provvedimento n. 232/2018, *Verifica preliminare. Trattamento di dati personali mediante un sistema di localizzazione geografica dei dispositivi aziendali.*

125 Garante italiano per la protezione dei dati personali, provvedimento n. 396/2018 *Localizzazione di veicoli aziendali.*

somministrazione dislocati in varie sedi, attraverso l'utilizzo di una applicazione *software* installata sui *device* personali dei lavoratori[126].

La nuova frontiera dei dispositivi di localizzazione dei lavoratori, invece, è rappresentata dagli strumenti c.d. "cyberfisici", ovvero tecnologie in grado di interagire in modo continuo con il sistema fisico in cui operano. Tra questi rientrano i "dispositivi *wearable*, apparecchiature di comunicazione tra operatore/operatori e sistema produttivo [...] interfacce uomo-macchina intelligenti che coadiuvano l'operatore a fini di sicurezza ed efficienza delle operazioni di lavorazione, manutenzione, logistica", che sono stati peraltro inclusi nel Piano nazionale Industria 4.0, a dimostrazione che il legislatore ne ha ipotizzato l'utilizzo anche in ambito lavorativo[127].

Sul punto, è stata molto discussa la scelta di Amazon di brevettare un braccialetto elettronico che, indossato dagli addetti al magazzino, sarebbe in grado di seguirne i movimenti, vibrando nel caso in cui siano scorretti, allo scopo di velocizzare il processo di ricerca del prodotto attraverso una triangolazione dei dati relativi al posizionamento del lavoratore e dei pacchi da ritirare[128]. Il dispositivo non è mai stato né è attualmente in uso nei magazzini Amazon situati in Italia, tuttavia l'ipotesi di una sua possibile introduzione ha suscitato critiche, da parte dei sindacati e del Presidente dell'Autorità Garante per la protezione dei dati, in ordine alla compatibilità con la disciplina privacy e alla possibile violazione dei diritti di libertà e dignità dei lavoratori che ne fossero costretti all'uso[129].

---

126 Garante italiano per la protezione dei dati personali, provvedimento n. 350/2016, *Verifica preliminare. Trattamento di dati personali dei dipendenti effettuato attraverso la localizzazione di dispositivi smartphone per finalità di rilevazione delle presenze.* Il Garante ha stabilito la liceità del trattamento a condizione che fossero rilevati i soli dati relativi alla sede di lavoro, alla data e all'orario della timbratura virtuale. Non consentito invece il trattamento di dati ultronei quali dati relativi al traffico telefonico, sms, posta elettronica e navigazione web.

127 Il Piano prevede misure concrete in base a tre principali linee guida: operare in una logica di neutralità tecnologica; intervenire con azioni orizzontali e non verticali o settoriali; agire su fattori abilitanti. Tra le principali azioni, è previsto l'iper e il super ammortamento per supportare e incentivare le imprese che investono in beni strumentali nuovi, in beni materiali e immateriali (software e sistemi IT) funzionali alla trasformazione tecnologica e digitale dei processi produttivi. Tra i beni compresi nel descritto incentivo figurano quelli appena citati c.d. "cyberfisici".

128 V. E. Dagnino, *Il braccialetto di Amazon, facciamo chiarezza*, in *Bollettino Adapt* del 5 febbraio 2018, n. 5; anche Corriere della sera, 6 febbraio 2018.

129 In relazione alla normativa nazionale ed europea, il trattamento dei dati derivante dal dispositivo brevettato da Amazon non pare rispondere ai principi di proporzionalità, di trasparenza e di salvaguardia della dignità dell'uomo. Sul punto v. A. Soro, *Persone in rete. I dati tra poteri e diritti*, Fazi Editore, 2018, ove il Presidente del Garante italiano per la protezione dei dati personali invita a riflettere, in senso più ampio, "in che misura è ammissibile imporre al lavoratore la sudditanza a una macchina, che ne guidi i comportamenti sin quasi ad annientarne le capacità di discernimento e di libera valutazione".

Al di là delle polemiche suscitate dal caso Amazon, il Garante italiano per la protezione dei dati personali si è di recente pronunciato con proprio provvedimento sulla ammissibilità dell'impiego di dispositivi RFID (*Radio Frequency Identification*) con tecnologia GPS associata ad un braccialetto indossabile dai dipendenti, senza escluderne aprioristicamente la legittimità. Nello specifico, all'esame del Collegio del Garante è stato sottoposto il caso di un'azienda operante servizi di spazzamento su strada che ha implementato un sistema tecnologico in grado di tracciare la collocazione territoriale dei cestini dei rifiuti e, in via indiretta, di identificare i lavoratori addetti al loro svuotamento, attraverso un incrocio tra le informazioni ricavate tramite dispositivo GPS con quelle dei dati dei turni di lavoro[130]. Per la ditta appaltatrice in questione, peraltro, la localizzazione degli strumenti collegati alla prestazione lavorativa si sarebbe resa necessaria per il rispetto di specifiche obbligazioni assunte contrattualmente con l'impresa appaltante, che prevedevano il controllo della qualità del servizio erogato.

Secondo il Garante, la circostanza per la quale l'attività di controllo sia assunta dall'imprenditore in forza di un obbligo contrattuale non influisce sul necessario rispetto delle disposizioni in materia di protezione dei dati personali cosicché dovranno sempre garantiti i principi di liceità, correttezza, trasparenza, finalità, minimizzazione dei dati, sanciti dall'art. 5 GDPR. Inoltre, nel provvedimento si rinvengono alcune indicazioni circa gli accorgimenti da adottare per il trattamento lecito dei dati acquisiti attraverso simili strumenti di localizzazione[131]. Fondamentalmente, la tipologia di misure di carattere generale per il trattamento dei dati raccolti tramite gli strumenti *cyberfisici* non differisce da quelle prescritte per il trattamento dei dati di geolocalizzazione dei mezzi aziendali. Semmai, in considerazione del rischio di maggiore pervasività di un controllo operato attraverso strumenti tecnologici indossabili, la salvaguardia della libertà e dignità del lavoratore richiederà uno *standard* di protezione maggiormente stringente. Così, il principio di finalità e proporzionalità necessita l'individuazione dei tempi di conservazione dei dati strettamente necessari rispetto agli scopi perseguiti, nel caso di specie anche avendo riguardo ad eventuali tempistiche relative alle contestazioni di inadempimento, da parte dell'impresa appaltante, di obblighi contrattuali assunti con il conferimento del servizio. Inoltre, dovranno essere indicati preventivamente e tassativamente i casi

130 Secondo il Garante italiano per la protezione dei dati personali, provvedimento 28 febbraio 2019, *Trattamento di dati personali dei dipendenti mediante dispositivi indossabili*, "sebbene i dispositivi indossabili (e il relativo numero identificativo univoco) saranno collegati alle zone di spazzamento e non ai singoli dipendenti, attraverso i registri contenenti il turno di lavoro, la zona di spazzamento e l'identità del lavoratore, sarà possibile individuare il dipendente che ha effettuato le rilevazioni dei tag [...] in particolare qualora il turno in una determinata zona di spazzamento sia effettuato da un solo dipendente o da un numero esiguo di dipendenti".

131 Cfr. Garante italiano per la protezione dei dati personali, provvedimento 28 febbraio 2019, *Trattamento di dati personali dei dipendenti mediante dispositivi indossabili.*

specifici (descritti nel dettaglio) nei quali si renderà necessario interconnettere le informazioni ottenute per il tramite dei dispositivi di localizzazione con quelli amministrativi (ad es. registri turni) allo scopo di poter ricostruire fatti oggetto di contestazione. In proposito, si rende necessario adottare misure organizzative e tecnologiche per mantenere distinte (segregate) le basi di dati (in particolare quelli trattati attraverso i menzionati registri) qualora non sia più necessaria l'eventuale interconnessione in vista dell'eventuale ricostruzione di fatti rilevanti disciplinarmente, ma sia comunque necessaria per fini amministrativi l'ulteriore conservazione dei registri dei turni.
In altri termini, il principio di minimizzazione dei dati, di cui all'art. 3 d.lgs. n. 196/2003, richiede come regola generale di evitare il trattamento quando le finalità perseguite dal datore di lavoro possano essere realizzate mediante dati anonimi od opportune modalità che permettano di identificare l'interessato solo in caso di necessità. Inoltre l'attività di monitoraggio non potrà essere continua e la conservazione del dato dovrà essere limitata allo stretto necessario[132].
Come evidenziato analizzando le condizioni generali di legittimità del trattamento, in tutti i casi in cui vengano installati dispositivi di geolocalizzazione in grado di rendere identificabili i lavoratori, sarà necessario procedere alla valutazione d'impatto DPIA, ai sensi dell'art. 35 GDPR[133].

4.4. Dispositivi BYOD (Bring Your Own Device)

Nei contesti aziendali tecnologicamente evoluti sono diffuse scelte organizzative che implicano l'utilizzo di dispositivi portatili personali del lavoratore quali strumenti necessari per l'esecuzione dell'attività lavorativa (telefoni, personal computer, *tablet*, ...). Il dispositivo, generalmente, viene dotato di *software* che consente di "isolare" le funzionalità necessarie in ambito lavorativo da quelle utilizzate dal lavoratore durante la sua vita privata nel tentativo di prevenire i rischi di commistione tra le diverse categorie di dati memorizzati.
Per quanto i dispositivi BYOD offrano al datore di lavoro vantaggi consistenti, in termini di abbattimento dei costi aziendali per l'acquisto di strumentazione tecnologica e per la realizzazione di attività di formazione e istruzione, la valutazione sulla opportunità della loro adozione è resa difficile dall'implementazione dei profili di sicurezza e protezione dei dati, sia personali che aziendali. Infatti, l'utilizzo "promiscuo" della strumentazione, da un lato, amplifica i rischi di *data breach*, dall'altro, rende complessa l'attività di con-

132 In tal senso la Raccomandazione CM/Rec(2015)5 del Consiglio d'Europa; v. anche Garante italiano per la protezione dei dati personali, provvedimento 28 febbraio 2019 e prima ancora nel provvedimento n. 247/2017.

133 La DPIA viene prescritta dal Garante nel provvedimento n.232/2018 e nel già citato provvedimento del 28 febbraio 2019.

trollo del datore di lavoro sui dati e le attività registrate dal dispositivo in considerazione della quantità di dati sensibili relativi in esso memorizzati e in nessun modo pertinenti all'attività di lavoro.

L'attualità della problematica è resa evidente dalle possibilità che l'ordinamento vigente offre agli imprenditori e ai lavoratori di optare per forme di adempimento della prestazione al di fuori del perimetro "fisico" aziendale. Si pensi al telelavoro e al lavoro agile (o *smart working*) che rappresentano delle modalità di esecuzione della prestazione vantaggiose sia per il lavoratore, in termini di risparmio di tempo e denaro necessari per raggiungere fisicamente il posto di lavoro e di maggiore possibilità di conciliazione del tempo dedicato alla professione con quello dedicato alla vita familiare o personale; sia per il datore di lavoro, relativamente alla riduzione della spesa di gestione ordinaria di una sede di lavoro, alla organizzazione degli spazi aziendali o alla programmazione delle pause dal lavoro.

Per telelavoro si intende "una forma di organizzazione e/o di lavoro che si avvale delle tecnologie dell'informazione nell'ambito di un contratto o di un accordo di lavoro, in cui l'attività lavorativa, che potrebbe anche essere svolta nei locali dell'impresa, viene regolarmente svolta al di fuori", mentre il lavoro agile rappresenta una modalità di esecuzione della prestazione di lavoro subordinato senza vincoli di luogo o di orario, in parte all'interno e in parte all'esterno dei locali aziendali con possibile utilizzo di strumenti tecnologici[134].

Allo *smart working* vengono associati aspetti positivi quali una maggiore efficienza e flessibilità nell'esecuzione delle mansioni, nonché una maggiore soddisfazione generale nel lavoro[135].

Generalmente, la possibilità di lavorare da remoto implica che il datore di lavoro metta a disposizione tecnologie, quali sistemi *cloud* o software installati sui dispositivi, che il lavoratore custodisce a casa o in viaggio o comunque in un luogo diverso dalla sede

---

134 La definizione di telelavoro è stata elaborata in occasione dell'European Framework Agreement del 16 luglio 2002, recepito in Italia da accordi collettivi di settore. La definizione di lavoro agile si trova nella L. n. 81/2017 recante "Misure per la tutela del lavoro autonomo non imprenditoriale e misure volte a favorire l'articolazione flessibile nei tempi e nei luoghi del lavoro subordinato". Per un'analisi delle analogie e differenze tra lavoro agile e telelavoro, *ex pluris* v. G. Santoro Passarelli, *Lavoro eterorganizzato, coordinato, agile e il telelavoro: un puzzle non facile da comporre in un'impresa in via di trasformazione*, WP C.S.D.L.E. "Massimo D'Antona".IT – 327/2017.

135 Secondo un'indagine dell'Osservatorio sullo smart working del Politecnico di Milano, "lo *smart working* continua a diffondersi in Italia e ad oggi il 58% delle grandi imprese, il 24% delle PMI e il 9% delle PA lavora in questo modo. Inoltre, a un anno dall'approvazione della legge sul Lavoro Agile, è possibile valutare i primi impatti delle nuove regole e procedure: per il 60% delle PA è risultata di stimolo, mentre ha avuto un impatto negativo per il 45% delle grandi imprese. Il numero degli smart worker cresce, arrivando a 480.000, e gli *smart worker* si sentono più motivati e soddisfatti rispetto agli altri lavoratori". Indagine completa reperibile su https://www.osservatori.net/it_it/osservatori/smart-working.

aziendale, al fine di rendere la prestazione lavorativa. Non è infrequente che gli strumenti siano concessi ad uso "promiscuo", anche come *benefit* individuali, per scopi personali del lavoratore o della sua famiglia, circostanza che ripropone inalterate le considerazioni operate sui dispositivi BYOD.

Per quanto riguarda il bilanciamento tra il legittimo esercizio del potere datoriale e la privacy dei lavoratori, nell'ambito di queste modalità di lavoro, si rimanda a quanto detto, con particolare riferimento a posta elettronica, internet e geolocalizzazione, non essendovi peculiarità rispetto alle modalità di esecuzione "tipiche" della prestazione lavorativa.

4.4.1. Lavoro "agile", telelavoro e tutela della riservatezza

Lo sviluppo delle nuove tecnologie digitali ha consentito la "smaterializzazione" del posto di lavoro e la diffusione di nuove modalità di esecuzione della prestazione lavorativa, accompagnando un processo di modernizzazione dell'organizzazione di lavoro. Grazie ad esso, le imprese sono state incentivate a concedere ai lavoratori ampi margini di flessibilità spaziale e temporale, nei casi in cui le esigenze organizzative aziendali e la tipologia di obbligazione lavorativa non implicassero la necessaria presenza nell'unità produttiva. Il fenomeno, che ha trovato iniziale manifestazione nelle sperimentazioni avviate dalle imprese, ha trovato sponda regolativa con il telelavoro, disciplinato dall'accordo quadro europeo del 16 luglio 2002 e dall'accordo interconfederale del 9 giugno 2004[136], e con la recente riforma del lavoro autonomo che ha promosso il lavoro agile (c.d. *smart working*) quale "modalità di esecuzione del rapporto di lavoro subordinato stabilita mediante accordo tra le parti, anche con forme di organizzazione per fasi, cicli e obiettivi e senza precisi vincoli di orario o di luogo di lavoro, con il possibile utilizzo di strumenti tecnologici per lo svolgimento dell'attività lavorativa" (*ex* art. 18, comma 1, l. n. 81/2017)[137].

---

136 La disciplina del telelavoro nella pubblica amministrazione è disciplinata dalla legge 16 giugno 1998, n. 191 e dal D.P.R. n. 70/1999.

137 Per una trattazione *ex professo* della disciplina del lavoro agile introdotta con gli artt. 18 – 24, l. n. 81/2017, v. i contributi di F. Chietera, *Il lavoro agile*, in D. Garofalo (a cura di), *La nuova frontiera del lavoro: autonomo – agile – occasionale*, Adapt University Press, 2018, pag. 365 ss.; A. Zilli, *Il lavoro agile nella pubblica amministrazione "4.0"*, *ivi*, pag. 356 ss.; G. A. Recchia, *Lavoro agile e autonomia collettiva*, ivi, pag. 380 ss.; C. Garofalo, *Produttività, efficienza e lavoro agile*, *ivi*, pag. 399 ss.; P. Mastrorilli, *Forma scritta, obblighi di comunicazione e recesso nel lavoro agile*, *ivi*, pag. 410 ss.; M. G. Deceglie, *Il trattamento del lavoratore agile*, *ivi*, pag. 427 ss.; V. Lamonaca, *Il diritto (eventuale) all'apprendimento continuo e la (complessa) certificazione delle competenze nel lavoro agile: un rebus di difficile soluzione*, *ivi*, pag. 446 ss.; A. Arbore, *Potere di controllo e potere disciplinare nel lavoro agile*, *ivi*, pag. 456 ss.; G. Leone, *La tutela della salute e della sicurezza dei lavoratori agili*, *ivi*, pag. 469 ss.; S. Caffio, *Lavoro agile e tutela assicurativa contro gli infortuni e le malattie professionali*, *ivi*, pag. 90 ss.; nonché C. Spinelli, *Tecnologie digitali e lavoro agile*, Cacucci, 2018.

La condizione del "telelavoratore" e del lavoratore agile che esegue la propria prestazione distante dalla organizzazione produttiva richiede al datore di lavoro l'implementazione di un diverso sistema di controllo da remoto, finalizzato non soltanto alla verifica dei risultati ottenuti, ma anche all'accertamento del corretto utilizzo degli strumenti di lavoro affidati con una accentuazione del rischio di indebita compressione della riservatezza del lavoratore[138]. Le modalità di esecuzione della prestazione di lavoro a distanza, infatti, condizionano all'utilizzo di supporti informatici (c.d. "esecuzione digitale dell'obbligazione lavorativa). In molti casi, "l'utilizzo del computer è incorporato nella prestazione lavorativa stessa, per cui diventa difficile, se non impossibile, attuare il controllo su questa se non attraverso lo strumento informatico". Sulla base di questi presupposti, non vi sarebbe alcuna distinzione tra 'strumenti di lavoro' e 'strumenti di controllo'.

Nel tentativo di ovviare alla problematica, il legislatore ha rinviato le modalità attuative del lavoro agile alla contrattazione individuale[139]. Nello specifico, l'art. 21, co.1, della legge n. 81/2017, precisa che nell'accordo relativo alla modalità di lavoro agile deve anche essere disciplinato l'esercizio del potere di controllo del datore di lavoro sulla prestazione resa dal lavoratore all'esterno dei locali aziendali nel rispetto di quanto disposto dall'articolo 4 della legge 20 maggio 1970, n. 300, e successive modificazioni. Tale disposizione deve essere letta in combinato con l'art. 115, co. 1, d. lgs. n. 196/2003 il quale stabilisce che "nell'ambito del rapporto di lavoro domestico del telelavoro e del lavoro agile il datore di lavoro è tenuto a garantire al lavoratore il rispetto della sua personalità e della sua libertà morale".

Infine, un cenno merita, il c.d. diritto alla disconnessione, previsto in materia di lavoro agile dalla l. n.81/2017, consistente nell'individuazione di un arco temporale durante il quale il lavoratore sia completamente libero da incombenze aziendali e non possa essere raggiunto da mail, messaggi o telefonate[140]. Per quanto non strettamente connesso

---

138 E. Sena, *Lavoro agile e diritto alla disconnessione: l'incidenza delle nuove tecnologie sulle modalità di esecuzione della prestazione di lavoro*, in *Il diritto del mercato del lavoro*, pag. 246, 247.

139 Spesso tale compito viene svolto dalla contrattazione collettiva. Si vedano sul punto i contratti nazionali siglati recentemente tra sindacati e datori di lavoro privati riportati da Il Sole24ore nell'articolo "Basta mail e Whatsapp fuori orario, lo dice il contratto" di C. Casadei, 8 aprile 2019, reperibile al link: https://www.ilsole24ore.com/art/norme-e-tributi/2019-04-07/basta-mail-e-whatsapp-fuori-orario-dice-contratto-104901.shtml?uuid=ABCwRHlB.

140 Art. 19 co.1 l. n.81/2017: "L'accordo relativo alla modalità di lavoro agile è stipulato per iscritto ai fini della regolarità amministrativa e della prova, e disciplina l'esecuzione della prestazione lavorativa svolta all'esterno dei locali aziendali, anche ocn riguardo alle forme di esercizio del potere direttivo del datore di lavoro ed agli strumenti utilizzati dal lavoratore. L'accordo individua altresì i tempi di riposo del lavoratore nonché le misure tecniche e organizzative necessarie per assicurare la disconnessione del lavoratore dalle strumentazioni tecnologiche di lavoro".

alla disciplina *privacy,* il diritto alla disconnessione è preordinato non solo e non tanto al recupero delle energie, ma soprattutto alla tutela della vita privata del lavoratore, tanto come singolo quanto all'interno della comunità in cui vive[141].

4.5. Strumenti di registrazione degli accessi e delle presenze attraverso dati biometrici

La tecnologia mette al servizio dei datori di lavoro strumenti sempre più avanzati di controllo degli accessi ad aree aziendali e di registrazione delle presenze del dipendente, in grado di operare l'identificazione o il riconoscimento dei lavoratori attraverso dati biometrici come le impronte digitali, la topografia della mano, la fisionomia dei volti, le caratteristiche vocali o dell'iride[142].
I dati biometrici rientrano tra le "categorie particolari di dati" previste all'art. 9 del GDPR, il quale dispone il divieto generale di trattamento, a meno che non si rientri in uno dei casi espressamente previsti dal comma 2 del medesimo articolo, ovvero quando:

a) l'interessato abbia prestato il proprio consenso esplicito;
b) il trattamento sia necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e della sicurezza sociale e protezione sociale, nella misura in cui sia autorizzato dal diritto dell'Unione o degli Stati membri o da un contratto collettivo ai sensi del diritto degli Stati membri, in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato.

Il decreto di armonizzazione del Codice Privacy al GDPR ha previsto che i dati biometrici debbano inoltre essere trattati in conformità alle misure di garanzia disposte dal Garante con provvedimento a cadenza almeno biennale (art. 2-*septies*, d.lgs. n. 196/2003, come modificato dal d.lgs. n. 101/2018).

---

141 M. Luciani, *Articoli 35-47*, in G. Neppi Modona (a cura di) *Stato nella Costituzione*, Milano 1995, pag. 151. Per un approfondimento recente sul diritto alla disconnessione: E. Sena, *Lavoro agile e diritto alla disconnessione: l'incidenza delle nuove tecnologie sulle modalità di esecuzione della prestazione di lavoro*, ne *Il diritto del mercato del lavoro*, 1/2018, pagg. 245-268.

142 La definizione normativa di dati biometrici è fornita dal GDPR all'art. 4 co. 1 num. 14): i dati personali ottenuti da un trattamento tecnico specifico relativi alle caratteristiche fisiche, fisiologiche o comportamentali di una persona fisica che ne consentono o confermano l'identificazione univoca, quali l'immagine facciale o i dati dattiloscopici. In dottrina v. S. Girotto, *Trattamento dei dati biometrici e dignità della persona*, in *Nuova Giurisprudenza civile*, n. 3, 2012, pag. 248 ss.; M. Pulice, *Sistemi di rilevazione dei dati biometrici e privacy*, in *Il lavoro nella giurisprudenza*, n. 10, 2009, pag. 994 ss.

Tale provvedimento non è ancora stato emanato dall'Autorità italiana, per cui le considerazioni che si faranno in prosieguo terranno conto della normativa europea e degli orientamenti espressi dal Garante in materia, in quanto compatibili con il GDPR.

Occorre premettere che il datore di lavoro è sempre tenuto a cercare i mezzi meno invasivi scegliendo, se possibile, un procedimento non biometrico al fine di verificare la presenza del dipendente, in quanto "i principi generali di tutela dei dati personali impongono che siano preventivamente considerati altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche che possano assicurare parimenti una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro senza fare ricorso al trattamento dei dati biometrici"[143].

Il Garante ha tuttavia ritenuto, fermi gli obblighi di sicurezza e il rispetto di quanto prescritto dalla normativa, "che il datore di lavoro privato possa utilizzare siffatti sistemi per "specifiche esigenze di sicurezza commisurate ai rischi incombenti sui dati o sui sistemi informatici che la procedura di autenticazione è destinata a proteggere" e che, dunque, "il trattamento dei dati biometrici può avvenire senza il consenso degli interessati"[144].

Con riferimento all'accesso fisico a luoghi il cui ingresso è limitato a soggetti abilitati, il Garante ha chiarito che l'adozione di sistemi biometrici basati sull'elaborazione dell´impronta digitale o della topografia della mano può essere consentita per limitare l'accesso ad aree e locali ritenuti "sensibili" in cui è necessario assicurare elevati e specifici livelli di sicurezza, oppure per consentire l'utilizzo di apparati e macchinari pericolosi ai soli soggetti qualificati e specificamente addetti alle attività.

Ad esempio, un datore di lavoro che installasse un siffatto sistema in una sala server in cui sono conservati, in formato elettronico, dati personali e sensibili dei propri dipendenti, sarebbe perfettamente *compliant* con la normativa che prevede l'obbligo di proteggere tali dati dall'accesso non autorizzato. Così, in caso di perdita dei dati, di anomalie o accessi non autorizzati, il datore di lavoro potrà legittimamente recuperare le registrazioni conservate allo scopo di individuare i soggetti entrati nell'area riservata. Diversamente, non sembra lecito il trattamento dei dati biometrici qualora utilizzati per valutare il rendimento dei dipendenti o monitorarne gli spostamenti all'interno dei locali aziendali.

---

143 Garante italiano per la protezione dei dati personali, provvedimento n. 357/2016, *Verifica preliminare. Sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale per la rilevazione della presenza in servizio.*

144 Garante italiano per la protezione dei dati personali, provvedimento n. 513/2014 *Provvedimento generale prescrittivo in tema di biometria.*

Affinchè possa parlarsi di trattamento di dati biometrici, è sempre imprescindibile che il sistema utilizzato permetta, anche indirettamente, l'identificazione dell'interessato[145].

4.5.1. Le novità per i dipendenti pubblici introdotte dalla legge "concretezza"

Nella seduta del 12 giugno 2019, è stato definitivamente approvato al Senato il disegno di legge recante "interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo", c.d. "ddl Concretezza". Il ddl era collegato alla Legge di bilancio 2019, della quale ha seguito l'*iter* di approvazione concluso in terza lettura presso il Senato[146].

Tra le altre disposizioni, la legge n. 56 del 13 giugno 2019, all'art. 2 co. 1, prevede l'applicazione generalizzata di sistemi di rilevazione delle presenze del personale in servizio presso le amministrazioni pubbliche basati sulla registrazione di dati biometrici e sull'installazione di apparati di videosorveglianza, entrambi preordinati alla verifica dell'osservanza dell'orario di lavoro[147].

---

145 Sul concetto di identificazione, cfr. Cass. sez. II civ. 15 ottobre 2018, n. 25686, per la quale *"ciò che rileva [...] è che il sistema, attraverso la conservazione dell'algoritmo, è in grado di risalire al lavoratore, al quale appartiene il dato biometrico"*, identificandolo, seppur indirettamente. Nel caso di specie si discuteva di un sistema di rilevamento delle presenze sulla base dei dati biometrici della mano dei dipendenti successivamente trasformati in un codice numerico memorizzato nel badge personale che, contrariamente a quanto affermato dal datore di lavoro, era però in grado di consentire la identificazione del lavoratore e, dunque, giudicato illegittimo e sanzionato dal Garante. Il Tribunale di Catania, adito dal datore di lavoro in contestazione della sanzione amministrativa comminata dal Garante, accoglieva le doglianze del primo, confermandone l'interpretazione in tema di identificazione. La Suprema Corte abbraccia invece l'orientamento del Garante, in un'ottica sostanziale, per la quale se il sistema consente di risalire all'interessato, trattasi di trattamento di dati biometrici. Rilievi critici sulla sentenza da parte di A. Sitzia e S. Crafa, *Impronte digitali, algoritmo e trattamento di dati personali: questioni di "law and technology"*, in *Il lavoro nella giurisprudenza*, 3/2019, pag. 245 ss.

146 La legge di bilancio 2019 (Legge 30 dicembre 2018 n. 145 Bilancio di previsione dello Stato per l'anno finanziario 2019 e bilancio pluriennale per il triennio 2019-2021) è stata approvata in seguito all'ottenimento della fiducia del Parlamento e pubblicata in Gazzetta Ufficiale Serie Generale n. 302 del 31-12-2018.

147 L'art. 2, della legge "concretezza", rubricato "misure per il contrasto all'assenteismo" recita: "Ai fini della verifica dell'osservanza dell'orario di lavoro, le amministrazioni pubbliche di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, con esclusione dei dipendenti di cui all'articolo 3 del medesimo decreto e fuori dei casi di cui all'articolo 18 della legge 22 maggio 2017, n. 81, introducono, nell'ambito delle risorse umane, finanziarie e strumentali disponibili a legislazione vigente e della dotazione del fondo di cui al comma 5, sistemi di verifica biometrica dell'identità e di videosorveglianza degli accessi, in sostituzione dei diversi sistemi di rilevazione automatica, attualmente in uso, nel rispetto dei principi di proporzionalità, non eccedenza e gradualità sanciti dall'articolo 5, paragrafo 1, lettera c), del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e del principio di proporzionalità previsto dall'articolo 52 della Carta dei diritti fondamentali dell'Unione europea. Con decreto del Presidente del Consiglio dei ministri, su proposta del Ministro per la pubblica amministrazione, da adottare ai sensi dell'articolo 17, comma 3, della legge 23 agosto 1988, n. 400, previa intesa in sede di Conferenza unificata di cui all'articolo 8 del decreto legislativo 28 agosto 1997, n. 281, e previo

Come dichiarato nella relazione illustrativa, lo scopo che si prefigge la norma è quello di ottenere "l'eliminazione o comunque la drastica riduzione delle false attestazioni di presenza in servizio" e, più in generale, di "contrasto dell'assenteismo", attraverso l'impiego simultaneo dei sistemi per il trattamento dei dati biometrici e dell'immagine dei dipendenti pubblici.

Sebbene non già precisamente individuati dalla legge, generalmente i dati biometrici oggetto di sistemi di rilevazione della presenza si basano sull'impronta digitale, sul riconoscimento dell'iride o facciale, sulla topografia della mano o, più raramente, sul riconoscimento vocale.

Le modalità attuative della previsione normativa vengono demandate a regolamenti da adottarsi previo parere del Garante italiano per la protezione dei dati, in particolare sulle modalità di trattamento dei dati biometrici che rientrano nella definizione di "categorie particolari di dati", di cui all'art. 9 del GDPR, e sono sottoposti a misure di protezione rafforzata. Per certo, stando alla lettera della legge, le modalità attuative dovranno essere limitate alla realizzazione di sistemi di riconoscimento basati sulla "verifica biometrica dell'identità e di videosorveglianza degli accessi". La dizione "verifica biometrica dell'identità" è stata inserita a seguito delle osservazioni del Garante, in sostituzione della precedente "identificazione biometrica", modalità di riconoscimento quest'ultima comportante un trattamento eccedente le finalità perseguite dalla norma.

Il Garante per la protezione dei dati personali ha fornito una definizione dei diversi processi di riconoscimento biometrico, evidenziandone le diverse caratteristiche e i profili di rischio. Nel caso dei processi biometrici basati sulla verifica dell'identità dell'interessato il confronto viene effettuato tra un determinato modello biometrico associato all'identità dichiarata dall'utente nella fase assertiva (per esempio, mediante l'inserimento di un codice d'utente o l'utilizzo di un badge a varia tecnologia) e il modello biometrico generato al momento della richiesta di riconoscimento. Questo tipo di riconoscimento viene detto anche "confronto uno-a-uno". Qualora il confronto risulti positivo l'identità potrà dirsi verificata e si otterrà la conseguente abilitazione alla successiva azione tecnica (apertura di un varco, nel caso di accesso fisico, abilitazione all'accesso a un sistema informatico, nel caso dell'accesso logico) la cui corretta esecuzione costituisce la finalità del trattamento biometrico. Laddove il trattamento sia invece volto all'identificazione biometrica dell'interessato, il modello biometrico estratto dovrà essere confrontato o

---

parere del Garante per la protezione dei dati personali ai sensi dell'articolo 154 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sulle modalità di trattamento dei dati biometrici, sono individuate le modalità attuative del presente comma, nel rispetto dell'articolo 9 del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, e delle misure di garanzia definite dal predetto Garante, ai sensi dell'articolo 2-septies del citato codice di cui al decreto legislativo n. 196 del 2003".

utilizzato come indice per la consultazione nella banca dati dei modelli biometrici di riferimento (confronto uno-a-molti). In tale ipotesi, la complessità dell'operazione è certamente superiore, dipendendo dalla dimensione della banca dati in termini di numerosità dei dati in essa presenti e dagli algoritmi di ricerca e confronto utilizzati[148].

La base giuridica che legittima siffatti trattamenti è rinvenibile, ai sensi del GDPR, nella necessità per il titolare, ovvero la P.A., (art. 6, par. 1 lett. e) di eseguire "un compito di interesse pubblico o connesso all'esercizio di pubblici poteri, di cui è investito", identificato dalla legge "concretezza", oltre che dal perseguimento delle finalità istituzionali del titolare del trattamento. Inoltre, in seguito alla autorizzazione del diritto interno, la legittimità dei trattamenti dei dati biometrici sarebbe garantita dalla necessità di assolvimento degli "obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro", purché questi avvengano in presenza di garanzie appropriate per i diritti fondamentali e gli interessi dell'interessato (cfr. art. 6, par. 1, lett. c) ed e), art. 3, art. 9, par. 2, lett. b), GDPR).

Sul disegno di legge si era espresso il Garante, con parere favorevole, ma rilevando come, per assicurare il rispetto dei principi di liceità, proporzionalità e minimizzazione sanciti dalla normativa europea sovraordinata, fosse necessario integrare l'art. 2, comma 1, dello schema di disegno legge affinché[149]:

a) fosse limitata la scelta ad un solo strumento di verifica;
b) fosse previsto in ogni caso l'utilizzo, nel rispetto del principio di gradualità delle misure limitative dei diritti delle persone, ove cioè altri sistemi di rilevazione delle presenze non risultino idonei rispetto agli scopi perseguiti;
c) l'utilizzo fosse ancorato alla sussistenza di specifici fattori di rischio ovvero a particolari presupposti, quali ad esempio le dimensioni dell'ente, il numero dei dipendenti coinvolti, la ricorrenza di situazioni di criticità dipendenti dal contesto ambientale. La declinazione di tali fattori potrebbe essere demandata ai regolamenti di attuazione, sui quali il Garante dovrà esprimere il parere di competenza".

148 Tali definizioni sono esplicitate nel provvedimento n. 513/2014, *Linee-guida in materia di riconoscimento biometrico e firma grafometrica" - Allegato A al Provvedimento del Garante del 12 novembre 2014 in materia di biometria.*

149 V. Garante italiano per la protezione dei dati, provvedimento n. 464/2018 *Parere su uno schema di disegno di legge recante "Interventi per la concretezza delle azioni delle pubbliche amministrazioni e la prevenzione dell'assenteismo"*. L'orientamento è stato confermato successivamente in occasione dell'audizione del presidente dell'Autorità garante per la protezione dei dati personali nell'ambito dell'esame del disegno di legge C. 1433 recante interventi per la concretezza delle azioni nelle pubbliche amministrazioni e la prevenzione dell'assenteismo presso le Commissioni riunite I Affari Costituzionali e XI Lavoro della Camera dei Deputati del 6 febbraio 2019.

In buona sostanza, il Garante ha espresso un parere complessivamente favorevole alla adozione di tali strumenti di rilevazione purché sussistano correttivi volti ad evitare che il trattamento dei dati da parte del datore di lavoro pubblico risulti sproporzionato ed eccedente rispetto alle finalità che lo stesso vuole raggiungere. Il provvedimento normativo, infatti, rimanda la definizione delle concrete modalità di attuazione del disposto dell'articolo 2 a successivi decreti di carattere regolamentare, sui quali dovrà esprimersi nuovamente il Garante, con particolare riferimento all'adozione delle misure, anche tecniche, necessarie per conformare pienamente i trattamenti di dati ai principi e alle garanzie previsti dal Regolamento.

Non si tratta della prima volta che l'Autorità in materia di protezione dei dati si esprime in merito all'utilizzo di siffatte tecnologie, sia in ambito pubblico che privato.

Nel 2014 il Garante aveva emanato un Provvedimento generale in materia di trattamento di dati biometrici, focalizzato principalmente sulla necessaria analisi dei rischi preliminare all'adozione delle soluzioni tecnologiche di riconoscimento basate su tali tipologie di dati, nonché sugli aspetti tecnici di protezione degli stessi[150].

---

150 V. Garante italiano per la protezione dei dati, provvedimento n. 513/2014, Provvedimento generale prescrittivo in tema di biometria. Le prescrizioni emanate in tale occasione dall'Autorità si ritiene si mostrano utili, pure nel mutato contesto giuridico, a misurare la rispondenza del trattamento dei dati biometrici ai principi generali affermati dal GDPR. Nel 2014, il Garante comunicava che "i titolari sono esonerati dall'obbligo di presentare istanza di verifica preliminare se il trattamento è svolto nel rispetto delle seguenti prescrizioni: a) Le caratteristiche biometriche consistono nell'impronta digitale o nell'emissione vocale. b) Nel caso di utilizzo dell'impronta digitale, il dispositivo di acquisizione ha la capacità di rilevare la c.d. vivezza. c) Nel caso di utilizzo dell'emissione vocale, tale caratteristica è utilizzata esclusivamente in combinazione con altri fattori di autenticazione e con accorgimenti che escludano i rischi di utilizzo fraudolento di eventuali registrazioni della voce (prevedendo, per esempio, la ripetizione da parte dell'interessato di parole o frasi proposte nel corso della procedura di riconoscimento). d) La cancellazione dei dati biometrici grezzi ha luogo immediatamente dopo la loro trasformazione in campioni o in modelli biometrici. e) I dispositivi per l'acquisizione iniziale (*enrolment*) e quelli per l'acquisizione nel corso dell'ordinario funzionamento sono direttamente connessi oppure integrati nei sistemi informatici che li utilizzano, siano essi postazioni di *enrolment* ovvero postazioni di lavoro o sistemi server protetti con autenticazione biometrica. f) Le trasmissioni di dati tra i dispositivi di acquisizione e i sistemi informatici sono rese sicure con l'ausilio di tecniche crittografiche caratterizzate dall'utilizzo di chiavi di cifratura di lunghezza adeguata alla dimensione e al ciclo di vita dei dati. g) Nel caso in cui i riferimenti biometrici siano conservati in modalità sicura su supporti portatili (*smart card* o analogo dispositivo sicuro) dotati di adeguate capacità crittografiche e certificati per le funzionalità richieste in conformità alla norma tecnica UNI CEI ISO/IEC 15408 o FIPS 140-2 almeno *level* 3: i. il supporto è rilasciato in un unico esemplare, è nell'esclusiva disponibilità dell'interessato e, in caso di cessazione dei diritti di accesso ai sistemi informatici, è restituito e distrutto con procedura formalizzata; ii. l'area di memoria in cui sono conservati i dati biometrici è resa accessibile ai soli lettori autorizzati e protetta da accessi non autorizzati; iii. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati. h) Nel caso di conservazione del campione o del riferimento biometrico sul sistema informatico protetto con autenticazione biometrica: i. è assicurata, tramite idonei sistemi di raccolta dei log, la registrazione degli accessi da parte degli amministratori di sistema ai sistemi informatici; ii. sono adottate idonee misure e accorgimenti tecnici per contrastare i rischi di installazione di software e di modi-

Con specifico riferimento, poi, al trattamento di dati biometrici da parte delle pubbliche amministrazioni finalizzato alla rilevazione della presenza dei dipendenti, il Garante si era già espresso, sostenendo una posizione contraria ad un suo utilizzo di tipo generalizzato, senza che, quindi, fossero valutati preventivamente altri sistemi, dispositivi e misure di sicurezza fisiche e logicistiche che potessero "assicurare una puntuale e attendibile verifica delle presenze e degli ingressi sul luogo di lavoro", evitando un trattamento sproporzionato[151]. Secondo l'Autorità, il titolare del trattamento, anche nell'ambito della pubblica amministrazione era tenuto ad accertare che la finalità perseguita potesse essere realizzata senza utilizzare dati biometrici, consentendo il loro utilizzo solo in casi eccezionali, giustificati da specifiche esigenze o da particolari situazioni contingenti, in coerenza con quanto affermato dal principio di necessità.
Affermava il Garante che "il titolare del trattamento, per verificare il puntuale rispetto dell'orario di lavoro, impedendo condotte abusive degli interessati, ben può disporre di altri (più "ordinari") sistemi, meno invasivi della sfera personale nonché della libertà individuale del lavoratore, che non ne coinvolgano la dimensione corporale"[152].
In assenza di una norma di legge basata sull'interesse pubblico al trattamento, come quella di recente emanata, il Garante ha ammesso, in passato, il trattamento per finalità

fiche della configurazione dei sistemi informatici, se non esplicitamente autorizzati; iii. i sistemi informatici sono protetti contro l'azione di malware; iv. sono adottate misure e accorgimenti volti a ridurre i rischi di manomissione e accesso fraudolento al dispositivo di acquisizione; v. i campioni o i riferimenti biometrici sono cifrati con tecniche crittografiche con lunghezza delle chiavi adeguata alla dimensione e al ciclo di vita dei dati; vi. i campioni o i riferimenti biometrici sono conservati per il tempo strettamente necessario a realizzare le finalità del sistema biometrico; vii. i campioni o i riferimenti biometrici sono conservati separatamente dai dati identificativi degli interessati; viii. sono previsti meccanismi di cancellazione automatica dei dati, cessati gli scopi per i quali sono stati raccolti e trattati. i) è esclusa la realizzazione di archivi biometrici centralizzati. j) è predisposta una relazione che descrive gli aspetti tecnici e organizzativi delle misure messe in atto dal titolare, fornendo altresì la valutazione della necessità e della proporzionalità del trattamento biometrico. Tale relazione è conservata aggiornata, con verifica di controllo almeno annuale, per tutto il periodo di esercizio del sistema biometrico e mantenuta a disposizione del Garante".

151 Cfr. Garante italiano per la protezione dei dati, deliberazione n. 23/2007, *Linee guida in materia di trattamento di dati personali di lavoratori per finalità di gestione del rapporto di lavoro in ambito pubblico*, punto 7.1; tale orientamento è stato condiviso, altresì, in sede di impugnazione di un'ordinanza-ingiunzione dell'Autorità, dal Trib. Prato, 19 settembre 2011.

152 Garante italiano per la protezione dei dati, provvedimento n. 38/2013, Trattamento di dati biometrici per finalità di rilevazione delle presenze dei dipendenti: verifica preliminare richiesta dal Comune di Boscoreale -.
Sul punto, medesime considerazioni anche in: Rilevazione delle presenze dei dipendenti di un Comune tramite un sistema biometrico basato sul trattamento di impronte digitali - 22 ottobre 2015 (provvedimento/2015).
Con riferimento alla rilevazione delle presenze del personale dipendente di una scuola, tramite l'utilizzo di impronta digitale, posizione nettamente contraria dell'Autorità espressa, tra gli altri, in: Videosorveglianza e biometria all'interno di un istituto scolastico per la rilevazione delle presenze dei dipendenti - 30 maggio 2013 (provvedimento n. 261/2013)

di accertamento della presenza in servizio dei dipendenti solo in ragione delle specificità connesse a quel particolare contesto lavorativo. È il caso, ad esempio, del sistema di rilevazione di dati biometrici dei lavoratori basato sulla lettura della geometria della mano, adottato da una società a partecipazione pubblica, consentito dal Garante, in considerazione della situazione del caso, al fine di "ottemperare agli obblighi di informare l'autorità giudiziaria della effettiva presenza al lavoro di personale sottoposto a regimi alternativi alla detenzione e di non esporsi al rischio di incorrere nel reato di colpa del custode per procurata evasione di cui all'art. 387 c.p." [153]. Il Garante aveva anche ammesso, in via eccezionale, l'utilizzo di un sistema di identificazione del dipendente pubblico mediante l'impronta digitale, giustificato dalla vastità della struttura sanitaria in cui questo era occupato e dal verificarsi sistematico di episodi di assenteismo di gran parte dei dipendenti, anche in considerazione della necessità di garantire il servizio pubblico in maniera continuativa[154].

In conclusione, gli specifici ambiti di applicazione, le misure di sicurezza tecniche e organizzative a protezione dei dati della c.d. legge "concretezza" dovranno necessariamente essere indagati alla luce delle successive norme di attuazione e degli esiti delle attività consultive del Garante italiano per la protezione dei dati, non tralasciando l'analisi del rischio condotta nell'ambito della più volte citata DPIA, valutazione di impatto richiesta, *ex* art. 35 GDPR, quando il trattamento abbia ad oggetto dati biometrici.

---

153 Garante italiano per la protezione dei dati, provvedimento n. 4/2013, *Sistema di rilevazione di dati biometrici dei lavoratori basato sulla lettura della geometria della mano*, nei confronti di Asia Napoli S.p.A. (società esercente attività e servizi di igiene ambientale nella provincia di Napoli). Il. Garante non ritiene il trattamento sproporzionato, considerando: l´elevato numero di lavoratori beneficiari di misure alternative alla detenzione (circa 500 su 2200 unità), il rischio della messa in atto di atti intimidatori nei confronti dei lavoratori "incensurati" (aggravati dal difficile contesto ambientale di riferimento, notoriamente soggetto a infiltrazioni camorristiche) e la notevole estensione del territorio della provincia di Napoli (tale da non consentire un agevole controllo sulla presenza e sull´osservanza dell´orario di lavoro da parte degli interessati, peraltro in un´area caratterizzata da manifeste problematiche sul fronte della rimozione e dello smaltimento dei rifiuti).

154 Si legge in una decisione dell'Autorità nei confronti dell'Azienda ospedaliero-Universitaria "San Giovanni di Dio e Ruggi d´Aragona" di Salerno, (v. Garante italiano per la protezione dei dati, provvedimento n. 357/2016 *Verifica preliminare. Sistema di lettura di dati biometrici mediante parziale identificazione dell'impronta digitale per la rilevazione della presenza in servizio*, che "al fine di garantire la salute pubblica, come fondamentale diritto dell´individuo e interesse della collettività e considerata la assoluta specificità del caso - ha riconosciuto la necessità e la proporzionalità del trattamento [...], in quanto quasi la metà dei dipendenti è risultata essere sotto indagine della magistratura per essersi assentata dopo aver timbrato il cartellino o per aver timbrato per conto di colleghi non presenti; [...] le caratteristiche del luogo non rendono possibile l'istallazione di varchi di accesso o tornelli nei pressi dei marcatempo che consentano il passaggio di una persona alla volta; [...] vastità dell´area e della necessità dei lavoratori di spostarsi per servizio tra padiglioni diversi".

5. Appendice

Figura 1 - Diagramma Valutazione d'impatto sulla protezione dei dati personali
a cura del Garante italiano per la protezione dei dati personali

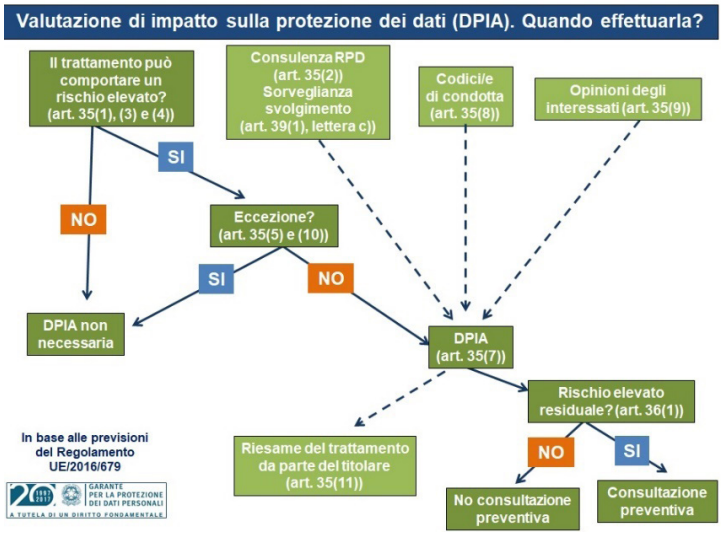


Figura 2 - Modello di informativa "minima" relativa alla videosorveglianza

Video surveillance!

Ulteriori informazioni sono disponibili:

- tramite avviso
- presso la nostra segreteria / ufficio relazioni esterne
- sul sito internet www.....

Identità del titolare e, ove applicabile, del rappresentante del responsabile del trattamento:

Dati di contatto del responsabile della protezione dei dati (ove applicabile):

Finalità del trattamento a cui sono destinati anche i dati personali la base giuridica per il trattamento:

Diritti degli interessati: in quanto soggetto interessato ha diversi diritti nei confronti del titolare/responsabile del trattamento, in particolare il diritto di richiedere l'accesso o la cancellazione dei suoi dati personali.

Per ulteriori dettagli sull'attività di videosorveglianza, inclusi i suoi diritti, può consultare le informazioni complete fornite dal titolare/responsabile del trattamento attraverso una delle modalità indicate a sinistra.

Figura 3 - Modello di informativa relativa alla geolocalizzazione del veicolo

Allegati

- Linee guida del Gruppo di Lavoro dei Garanti Europei sul DPO
- Linee guida del gruppo dei Garanti Europei concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" - WP 243, rev. 01
- Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati - WP 248, rev. 01
- Delibera del Garante della Privacy 1° Marzo 2007, n. 13 - Le linee guida per posta elettronica e internet

Linee guida del Gruppo di Lavoro dei Garanti Europei sul DPO

Adottate il 13 dicembre 2016

1. Introduzione

Il regolamento generale sulla protezione dei dati (RGPD)[1], che esplicherà i propri effetti a partire dal 25 maggio 2018, offre un quadro di riferimento in termini di compliance per la protezione dei dati in Europa, aggiornato e fondato sul principio di responsabilizzazione (accountability). I responsabili della protezione dei dati (RPD) saranno al centro di questo nuovo quadro giuridico in molti ambiti, e saranno chiamati a facilitare l'osservanza delle disposizioni del RGPD.

In base al RGPD, alcuni titolari del trattamento e responsabili del trattamento sono tenuti a nominare un RPD[2]. Ciò vale per tutte le autorità pubbliche e tutti i soggetti pubblici, indipendentemente dai dati oggetto di trattamento, e per altri soggetti che, come attività principale, effettuino un monitoraggio regolare e su larga scala delle persone fisiche ovvero trattino su larga scala categorie particolari di dati personali.

Anche ove il regolamento non imponga in modo specifico la designazione di un RPD, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia gli approcci di questo genere.

1 Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119, 4.5.2016). Il RGPD è rilevante ai fini del SEE e sarà applicabile una volta incorporato nell'Accordo relativo al SEE.

2 La nomina di un RPD è obbligatoria anche con riguardo alle autorità competenti di cui all'articolo 32 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti ai fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati e che abroga la decisione quadro 2008/977/GAI del Consiglio (GU L 119, 4.5.2016), alla luce della normativa nazionale di recepimento. Le presenti linee guida guardano con particolare attenzione alla figura del RPD come prevista dal RGPD, ma le indicazioni in esse formulate valgono anche per i RPD previsti dalla direttiva 2016/680 con riferimento alle disposizioni di carattere analogo contenute nei due strumenti.

La figura del RPD non costituisce una novità assoluta. La direttiva 95/46/CE[3] non prevedeva alcun obbligo di nomina di un RPD, ma in molti Stati membri questa è divenuta una prassi nel corso degli anni.

Ancor prima dell'adozione del RGPD, il Gruppo di lavoro ha sostenuto che questa figura rappresenti un elemento fondante ai fini della responsabilizzazione, e che la nomina del RPD possa facilitare l'osservanza della normativa e aumentare il margine competitivo delle imprese[4]. Oltre a favorire l'osservanza attraverso strumenti di accountability (per esempio, supportando valutazioni di impatto e conducendo o supportando audit in materia di protezione dei dati), i RPD fungono da interfaccia fra i soggetti coinvolti: autorità di controllo, interessati, divisioni operative all'interno di un'azienda o di un ente.

I RPD non rispondono personalmente in caso di inosservanza del RGPD. Quest'ultimo chiarisce che spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che le operazioni di trattamento sono conformi alle disposizioni del regolamento stesso (articolo 24, paragrafo 1). L'onere di assicurare il rispetto della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

Inoltre, al titolare del trattamento o al responsabile del trattamento spetta il compito fondamentale di consentire lo svolgimento efficace dei compiti cui il RPD è preposto. La nomina di un RPD è solo il primo passo, perché il RPD deve disporre anche di autonomia e risorse sufficienti per svolgere in modo efficace i propri compiti.

Il RGPD riconosce nel RPD uno degli elementi chiave all'interno del nuovo sistema di governance dei dati, e prevede una serie di condizioni in rapporto alla nomina, allo status e ai compiti specifici. Le presenti linee guida intendono fare chiarezza sulle pertinenti disposizioni del regolamento al fine di favorire l'osservanza della normativa da parte di titolari del trattamento e responsabili del trattamento; inoltre, le linee guida vogliono essere di ausilio ai RPD nell'esecuzione dei compiti loro attribuiti. Il presente documento contiene anche alcune raccomandazioni, in termini di migliori prassi, che scaturiscono dall'esperienza accumulata in alcuni Stati membri. Il Gruppo di lavoro monitorerà l'attuazione delle linee guida qui presentate e provvederà alle integrazioni che si riveleranno opportune.

---

3 Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati (GU L 281, 23.11.95).

4 Si veda http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_en.pdf

2. Nomina di un RPD

2.1. Nomina obbligatoria

In base all'articolo 37, paragrafo 1, del RGPD, la nomina di un RPD è obbligatoria in tre casi specifici[5]:

a) se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico[6];
b) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
c) se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati[7] o[8] di dati personali relativi a condanne penali e reati[9].

Nelle sottosezioni che seguono, il Gruppo di lavoro fornisce indicazioni sui criteri e sulle formulazioni utilizzati all'articolo 37, paragrafo 1.

Tranne quando sia evidente che un soggetto non è tenuto a nominare un RPD, il Gruppo di lavoro raccomanda a titolari del trattamento e responsabili del trattamento di documentare le valutazioni compiute all'interno dell'azienda o dell'ente per stabilire se si applichi o meno l'obbligo di nomina di un RPD, così da poter dimostrare che l'analisi ha preso in esame correttamente i fattori pertinenti[10]. Tale analisi fa parte della documentazione da produrre in base al principio di responsabilizzazione. Può essere richiesta dall'autorità di controllo e dovrebbe essere aggiornata ove necessario, per esempio se i

5 Si osservi che, in base all'articolo 37, paragrafo 4, il diritto dell'Unione o dello Stato membro può prevedere casi ulteriori di nomina obbligatoria di un RPD.

6 Con l'eccezione delle autorità giudiziarie nell'esercizio delle funzioni giurisdizionali. V. articolo 32 della direttiva (UE) 2016/680.

7 Ai sensi dell'articolo 9, si tratta dei dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni filosofiche o religiose, o l'appartenenza sindacale, oltre al trattamento di dati genetici, dati biometrici al fine dell'identificazione univoca di una persona fisica, e di dati relativi alla salute, alla vita sessuale o all'orientamento sessuale di una persona fisica.

8 Nel testo in lingua inglese dell'articolo 37, paragrafo 1, lettera c) compare la congiunzione "and" (e); si veda il paragrafo 2.1.5 infra per maggiori chiarimenti sull'utilizzo della congiunzione "o" anziché "e" nello specifico contesto.

9 Articolo 10.

10 Si veda l'articolo 24, paragrafo 1.

titolari del trattamento o i responsabili del trattamento intraprendono nuove attività o forniscono nuovi servizi che potrebbero ricadere nel novero dei casi elencati all'articolo 37, paragrafo 1.

Se si procede alla nomina di un RPD su base volontaria, troveranno applicazione tutti i requisiti di cui agli articoli 37-39 per quanto concerne la nomina stessa, lo status e i compiti del RPD esattamente come nel caso di una nomina obbligatoria.

Nulla osta a che un'azienda o un ente, quando non sia soggetta all'obbligo di designare un RPD e non intenda procedere a tale designazione su base volontaria, ricorra comunque a personale o consulenti esterni incaricati di incombenze relative alla protezione dei dati personali. In tal caso è fondamentale garantire che non vi siano ambiguità in termini di denominazione, status e compiti di queste figure; è dunque essenziale che in tutte le comunicazioni interne all'azienda e anche in quelle esterne (con l'autorità di controllo, gli interessati, i soggetti esterni in genere), queste figure o consulenti non siano indicati con la denominazione di responsabile per la protezione dei dati (RPD)[11].

Il RPD viene designato, su base obbligatoria o meno, per tutti i trattamenti svolti dal titolare del trattamento o dal responsabile del trattamento.

2.1.1. "Autorità pubblica o organismo pubblico"

Nel regolamento non si rinviene alcuna definizione di "autorità pubblica" o "organismo pubblico". Il Gruppo di lavoro ritiene che tale definizione debba essere conforme al diritto nazionale; conseguentemente, sono autorità pubbliche o organismi pubblici le autorità nazionali, regionali e locali ma, a seconda del diritto nazionale applicabile, la nozione ricomprende anche tutta una serie di altri organismi di diritto pubblico[12]. In questi casi la nomina di un RPD è obbligatoria.

Lo svolgimento di funzioni pubbliche e l'esercizio di pubblici poteri[13] non pertengono esclusivamente alle autorità pubbliche e agli organismi pubblici, potendo riferirsi anche ad altre persone fisiche o giuridiche, di diritto pubblico o privato, in ambiti che variano a seconda delle disposizioni fissate nel diritto interno di ciascuno Stato membro: trasporti

11 Queste considerazioni valgono anche per i chief privacy officers (CPO) o altri professionisti in materia di privacy già operanti presso alcune aziende, che non sempre e non necessariamente si conformano ai requisiti fissati nel regolamento per quanto riguarda, per esempio, le risorse disponibili o le salvaguardie della loro indipendenza e che, in tal caso, non possono essere considerati e denominati "RPD".

12 Si vedano, per esempio, le definizioni di "ente pubblico" e "organismo di diritto pubblico" contenute nell'articolo 2, paragrafi 1 e 2, della direttiva 2003/98/CE del Parlamento europeo e del Consiglio, del 17 novembre 2003, relativa al riutilizzo dell'informazione del settore pubblico.

13 Articolo 6, paragrafo 1, lettera e).

pubblici, forniture idriche ed elettriche, infrastrutture stradali, emittenti radiotelevisive pubbliche, istituti per l'edilizia pubblica o organismi di disciplina professionale.
In tutti questi casi la situazione in cui versano gli interessati è probabilmente molto simile a quella in cui il trattamento è svolto da un'autorità pubblica o da un organismo pubblico. Più in particolare, i trattamenti perseguono finalità simili e spesso il singolo ha, in modo analogo, un margine esiguo o nullo rispetto alla possibilità di decidere se e come possano essere trattati i propri dati personali; pertanto, è verosimile che sia necessaria l'ulteriore tutela offerta dalla nomina di un RPD.
Benché nei casi sopra descritti non sussista l'obbligo di nominare un RPD, il Gruppo di lavoro raccomanda, in termini di buone prassi, che gli organismi privati incaricati di funzioni pubbliche o che esercitano pubblici poteri nominino un RPD. Le attività del RPD nominato nei termini sopra indicati si estendono a tutti i trattamenti svolti, compresi quelli che non sono connessi all'espletamento di funzioni pubbliche o all'esercizio di pubblici poteri quali, per esempio, la gestione di un database del personale.

2.1.2. "Attività principali"

L'articolo 37, paragrafo 1, lettere b) e c), del RGPD contiene un riferimento alle "attività principali del titolare del trattamento o del responsabile del trattamento". Nel considerando 97 si afferma che le attività principali di un titolare del trattamento "riguardano le sue attività primarie ed esulano dal trattamento dei dati personali come attività accessoria". Con "attività principali" si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento.
Tuttavia, l'espressione "attività principali" non va interpretata nel senso di escludere quei casi in cui il trattamento di dati costituisce una componente inscindibile dalle attività svolte dal titolare del trattamento o dal responsabile del trattamento. Per esempio, l'attività principale di un ospedale consiste nella prestazione di assistenza sanitaria, ma non sarebbe possibile prestare tale assistenza nel rispetto della sicurezza e in modo efficace senza trattare dati relativi alla salute, come le informazioni contenute nella cartella sanitaria di un paziente. Ne deriva che il trattamento di tali informazioni deve essere annoverato fra le attività principali di qualsiasi ospedale, e che gli ospedali sono tenuti a nominare un RPD.
A titolo di ulteriore esemplificazione, si può citare il caso di un'impresa di sicurezza privata incaricata della sorveglianza di più centri commerciali e aree pubbliche. L'attività principale dell'impresa consiste nella sorveglianza, e questa, a sua volta, è legata in modo inscindibile al trattamento di dati personali. Ne consegue che anche l'impresa in oggetto deve nominare un RPD.

D'altro canto, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale o la predisposizione di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell'attività principale o dell'oggetto principale del singolo organismo, ma pur essendo necessarie o essenziali sono considerate solitamente accessorie e non vengono annoverate fra le attività principali.

2.1.3. "Larga scala"

In base all'articolo 37, paragrafo 1, lettere b) e c), del RGPD, occorre che il trattamento di dati personali avvenga su larga scala per far scattare l'obbligo di nomina di un RPD. Nel regolamento non si dà alcuna definizione di trattamento su larga scala, anche se il considerando 91 fornisce indicazioni in proposito[14].

In realtà è impossibile precisare la quantità di dati oggetto di trattamento o il numero di interessati in modo da coprire tutte le eventualità; d'altra parte, ciò non significa che sia impossibile, col tempo, individuare alcuni standard utili a specificare in termini più specifici e/o quantitativi cosa debba intendersi per "larga scala" con riguardo ad alcune tipologie di trattamento maggiormente comuni. Anche il Gruppo di lavoro intende contribuire alla definizione di questi standard pubblicando e mettendo a fattor comune esempi delle soglie applicabili per la nomina di un RPD.

A ogni modo, il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell'attività di trattamento;
- la portata geografica dell'attività di trattamento.

---

14 Il considerando in questione vi ricomprende, in particolare, "trattamenti su larga scala, che mirano al trattamento di una notevole quantità di dati personali a livello regionale, nazionale o sovranazionale e che potrebbero incidere su un vasto numero di interessati e che potenzialmente presentano un rischio elevato". D'altro canto, lo stesso considerando prevede in modo specifico che "Il trattamento di dati personali non dovrebbe essere considerato un trattamento su larga scala qualora riguardi dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato". Si deve tener conto del fatto che il considerando offre alcune esemplificazioni ai due estremi della scala (trattamento svolto dal singolo medico / trattamento di dati relativi a un'intera nazione o a livello europeo) e che fra tali estremi si colloca un'ampia zona grigia. Inoltre, va sottolineato che il considerando citato si riferisce alle valutazioni di impatto sulla protezione dei dati; ciò significa che non tutti gli elementi citati sono necessariamente pertinenti alla nomina di un RPD negli stessi identici termini.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell'ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile del trattamento specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;
- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

2.1.4. "Monitoraggio regolare e sistematico"

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, il considerando 24 menziona il "monitoraggio del comportamento di detti interessati"[15] ricomprendendovi senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale.

15 "Per stabilire se un'attività di trattamento sia assimilabile al controllo del comportamento dell'interessato, è opportuno verificare se le persone fisiche sono tracciate su internet, compreso l'eventuale ricorso successivo a tecniche di trattamento dei dati personali che consistono nella profilazione della persona fisica, in particolare per adottare decisioni che la riguardano o analizzarne o prevederne le preferenze, i comportamenti e le posizioni personali."

Occorre rilevare, però, che la nozione di monitoraggio non trova applicazione solo con riguardo all'ambiente online, e che il tracciamento online va considerato solo uno dei possibili esempi di monitoraggio del comportamento degli interessati[16].
L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;
- che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

16 Si osservi che il considerando 24 riguarda l'applicazione extraterritoriale del RGPD; inoltre, vi è una differenza fra l'espressione "monitoraggio del loro comportamento" (articolo 3, paragrafo 2, lettera b)) e "monitoraggio regolare e sistematico degli interessati" (articolo 37, paragrafo 1, lettera b)), per cui le due espressioni potrebbero ben riferirsi a concetti distinti.

2.1.5. Categorie particolari di dati e dati relativi a condanne penali e a reati

Le disposizioni dell'articolo 37, paragrafo 1, lettera c), riguardano il trattamento di categorie particolari di dati ai sensi dell'articolo 9 e di dati personali relativi a condanne penali e a reati di cui all'articolo 10. Nonostante l'utilizzo della congiunzione "e" nel testo, non vi sono motivazioni sistematiche che impongano l'applicazione simultanea dei due criteri. Pertanto, il testo deve essere interpretato come se recasse la congiunzione "o". [NdT: il testo italiano del regolamento reca già la congiunzione "o"]

2.2. RPD del responsabile del trattamento

Per quanto riguarda la nomina di un RPD, l'articolo 37 non distingue fra titolari del trattamento[17] e responsabili del trattamento[18] in termini di sua applicabilità. A seconda di chi soddisfi i criteri relativi all'obbligatorietà della nomina, potrà essere il solo titolare del trattamento ovvero il solo responsabile del trattamento, oppure sia l'uno sia l'altro a dover nominare un RPD; questi ultimi saranno poi tenuti alla reciproca collaborazione. Vale la pena di evidenziare che anche qualora il titolare del trattamento sia tenuto, in base ai criteri suddetti, a nominare un RPD, il suo eventuale responsabile del trattamento non è detto sia egualmente tenuto a procedere a tale nomina – che però può costituire una buona prassi.

Alcuni esempi:

- Una piccola azienda a conduzione familiare operante nel settore della distribuzione di elettrodomestici in una città si serve di un responsabile del trattamento la cui attività principale consiste nel fornire servizi di tracciamento degli utenti del sito web oltre all'assistenza per attività di pubblicità e marketing mirati. Le attività svolte dall'azienda e dai clienti non generano trattamenti di dati "su larga scala", in considerazione del ridotto numero di clienti e della gamma relativamente limitata di attività. Tuttavia, il responsabile del trattamento, che conta numerosi clienti come questa piccola azienda familiare, svolge, nel suo complesso, trattamenti su larga scala. Ne deriva che il responsabile del trattamento deve nominare un RPD ai sensi dell'articolo 37, paragrafo 1, lettera b); al contempo, l'azienda in quanto tale non è soggetta all'obbligo di nomina del RPD.
- Un'azienda di medie dimensioni che produce rivestimenti in ceramica incarica un responsabile esterno della gestione dei servizi di salute occupazionale; tale respon-

17 Ai sensi della definizione contenuta all'articolo 4, punto 7, il titolare del trattamento è la persona o l'organismo che determina le finalità e i mezzi del trattamento.

18 Ai sensi della definizione contenuta all'articolo 4, punto 8, il responsabile del trattamento è la persona o l'organismo che tratta dati personali per conto del titolare del trattamento.

sabile ha un numero elevato di clienti con caratteristiche analoghe. Il responsabile del trattamento è tenuto a nominare un RPD ai sensi dell'articolo 37, paragrafo 1, lettera b), poiché svolge trattamenti su larga scala. Tuttavia, l'azienda non è tenuta necessariamente allo stesso adempimento.

Il RPD nominato da un soggetto responsabile del trattamento vigila anche sulle attività svolte da tale soggetto quando operi in qualità di autonomo titolare del trattamento – per esempio, rispetto ai dati concernenti il personale, le risorse informatiche, la logistica.

2.3. Designazione di un unico RPD per più organismi

L'articolo 37, paragrafo 2, consente a un gruppo imprenditoriale di nominare un unico RPD a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati[19], l'autorità di controllo[20] e i soggetti interni all'organismo o all'ente, visto che uno dei compiti del RPD consiste nell' "informare e fornire consulenza al titolare del trattamento o al responsabile del trattamento nonché ai dipendenti che eseguono il trattamento in merito agli obblighi derivanti dal presente regolamento"[21].
Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD[22].
Il RPD, se necessario con il supporto di un team di collaboratori, deve essere in grado di comunicare con gli interessati[23] in modo efficiente e di collaborare[24] con le autorità di controllo interessate. Ciò significa, fra l'altro, che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per vol-

19 V. articolo 38, paragrafo 4: "Gli interessati possono contattare il responsabile della protezione dei dati per tutte le questioni relative al trattamento dei loro dati personali e all'esercizio dei loro diritti derivanti dal presente regolamento."

20 V. articolo 39, paragrafo 1, lettera e): "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a qualunque altra questione."

21 Articolo 39, paragrafo 1, lettera a).

22 V. anche paragrafo 2.6 infra.

23 V. articolo 12, paragrafo 1: "Il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 e le comunicazioni di cui agli articoli da 15 a 22 e all'articolo 34 relative al trattamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro, in particolare nel caso di informazioni destinate specificamente ai minori."

24 V. articolo 39, paragrafo 1, lettera d: "cooperare con l'autorità di controllo."

ta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.
Ai sensi dell'articolo 37, paragrafo 3, è ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico RPD, se necessario supportato da un team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici.

2.4. Accessibilità e localizzazione del RPD

Ai sensi dell'articolo 4 [sic] del RGPD, l'accessibilità del RPD deve essere effettivamente tale. Per garantire tale accessibilità, il Gruppo di lavoro raccomanda che il RPD sia localizzato nel territorio dell'Unione europea, indipendentemente dal fatto che il titolare del trattamento o il responsabile del trattamento siano stabiliti nell'UE.
Tuttavia, non si può escludere che, in alcuni casi ove il titolare del trattamento o il responsabile del trattamento non sono stabiliti nell'UE[25], un RPD sia in grado di svolgere i propri compiti con maggiore efficacia operando al di fuori del territorio dell'UE.

2.5. Conoscenze e competenze del RPD

In base all'articolo 37, paragrafo 5, il RPD "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i compiti di cui all'articolo 39". Nel considerando 97 si prevede che il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento.

Conoscenze specialistiche

Il livello di conoscenza specialistica richiesto non trova una definizione tassativa; piuttosto, deve essere proporzionato alla sensibilità, complessità e quantità dei dati sottoposti a trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto. Occorre anche

25 V. articolo 3 del RGPD per quanto concerne l'ambito territoriale di applicazione.

distinguere in base all'esistenza di trasferimenti sistematici ovvero occasionali di dati personali al di fuori dell'Unione europea. Ne consegue la necessità di una particolare attenzione nella scelta del RPD, in cui si tenga adeguatamente conto delle problematiche in materia di protezione dei dati con cui il singolo titolare deve confrontarsi.

Qualità professionali

L'articolo 37, paragrafo 5, non specifica le qualità professionali da prendere in considerazione nella nomina di un RPD; tuttavia, sono pertinenti al riguardo la conoscenza da parte del RPD della normativa e delle prassi nazionali ed europee in materia di protezione dei dati e un'approfondita conoscenza del RGPD. Proficua anche la promozione di una formazione adeguata e continua rivolta ai RPD da parte delle Autorità di controllo.
È utile la conoscenza dello specifico settore di attività e della struttura organizzativa del titolare del trattamento; inoltre, il RPD dovrebbe avere buona familiarità con le operazioni di trattamento svolte nonché con i sistemi informativi e le esigenze di sicurezza e protezione dati manifestate dal titolare.
Nel caso di un'autorità pubblica o di un organismo pubblico, il RPD dovrebbe possedere anche una conoscenza approfondita delle norme e procedure amministrative applicabili.

Capacità di assolvere i propri compiti

Per capacità di assolvere i propri compiti si deve intendere sia quanto è legato alle qualità personali e alle conoscenze del RPD, sia quanto dipende dalla posizione del RPD all'interno dell'azienda o dell'organismo. Le qualità personali dovrebbero comprendere, per esempio, l'integrità ed elevati standard deontologici; il RPD dovrebbe perseguire in via primaria l'osservanza delle disposizioni del RGPD. Il RPD svolge un ruolo chiave nel promuovere la cultura della protezione dei dati all'interno dell'azienda o dell'organismo, e contribuisce a dare attuazione a elementi essenziali del regolamento quali i principi fondamentali del trattamento[26], i diritti degli interessati[27], la protezione dei dati sin dalla fase di progettazione e per impostazione predefinita[28], i registri delle attività di trattamento[29], la sicurezza dei trattamenti[30] e la notifica e comunicazione delle violazioni di dati personali[31].

26 Capo II

27 Capo III

28 Articolo 25.

29 Articolo 30.

30 Articolo 32.

31 Articoli 33 e 34.

RPD sulla base di un contratto di servizi

La funzione di RPD può essere esercitata anche in base a un contratto di servizi stipulato con una persona fisica o giuridica esterna all'organismo o all'azienda titolare/responsabile del trattamento. In tal caso, è indispensabile che ciascun soggetto appartenente alla persona giuridica e operante quale RPD soddisfi tutti i requisiti applicabili come fissati nella Sezione 4 del RGPD; per esempio, è indispensabile che nessuno di tali soggetti versi in situazioni di conflitto di interessi. Pari importanza riveste il fatto che ciascuno dei soggetti in questione goda delle tutele previste dal RGPD: per esempio, non è ammissibile la risoluzione ingiustificata del contratto di servizi in rapporto alle attività svolte in quanto RPD, né è ammissibile l'ingiustificata rimozione di un singolo appartenente alla persona giuridica che svolga funzioni di RPD. Al contempo, si potranno associare le competenze e le capacità individuali affinché il contributo collettivo fornito da più soggetti consenta di rendere alla clientela un servizio più efficiente.
Per favorire una corretta e trasparente organizzazione interna e prevenire conflitti di interesse a carico dei componenti il team RPD, si raccomanda di procedere a una chiara ripartizione dei compiti all'interno del team RPD e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente. Sarà utile, in via generale, inserire specifiche disposizioni in merito nel contratto di servizi.

2.6. Pubblicazione e comunicazione dei dati di contatto del RPD

L'articolo 37, settimo paragrafo, del RGPD impone al titolare del trattamento o al responsabile del trattamento

- di pubblicare i dati di contatto del RPD, e
- di comunicare i dati di contatto del RPD alle pertinenti autorità di controllo.

Queste disposizioni mirano a garantire che tanto gli interessati (all'interno o all'esterno dell'ente/organismo titolare o responsabile del trattamento) quanto le autorità di controllo possano contattare il RPD in modo facile e diretto senza doversi rivolgere a un'altra struttura operante presso il titolare/responsabile del trattamento. Anche la confidenzialità riveste pari importanza; per esempio, i dipendenti possono essere riluttanti a presentare reclami al RPD se non viene garantita la confidenzialità delle loro comunicazioni. Il RPD è tenuto a osservare le norme in materia di segreto o confidenzialità nello svolgimento dei propri compiti, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5).

I dati di contatto del RPD dovrebbero comprendere tutte le informazioni che consentono agli interessati e all'autorità di controllo di raggiungere facilmente il RPD stesso: recapito postale, numero telefonico dedicato e/o indirizzo dedicato di posta elettronica. Se opportuno, per facilitare la comunicazione con il pubblico, si potrebbero indicare anche canali ulteriori: una hotline dedicata, un modulo specifico per contattare il RPD pubblicato sul sito del titolare/responsabile del trattamento.

In base all'articolo 37, settimo paragrafo, del RGPD non è necessario pubblicare anche il nominativo del RPD. Seppure ciò rappresenti con ogni probabilità di una buona prassi, spetta al titolare del trattamento o al responsabile del trattamento e allo stesso RPD stabilire se si tratti di un'informazione necessaria o utile nelle specifiche circostanze[32]. Tuttavia, comunicare il nominativo del RPD all'autorità di controllo è fondamentale affinché il RPD funga da punto di contatto fra il singolo ente o organismo e l'autorità di controllo stessa (articolo 39, paragrafo 1, lettera e)).

In termini di buone prassi, il Gruppo di lavoro raccomanda, inoltre, che il titolare/responsabile del trattamento comunichi ai dipendenti il nominativo e i dati di contatto del RPD. Per esempio, queste informazioni (nominativo e dati di contatto) potrebbero essere pubblicate sulla intranet del titolare/responsabile del trattamento, inserite nell'elenco telefonico interno e nei diversi organigrammi della struttura.

3. Posizione del RPD

3.1. Coinvolgimento del RPD in tutte le questioni riguardanti la protezione dei dati personali

Ai sensi dell'articolo 38 del RGPD, il titolare del trattamento e il responsabile del trattamento assicurano che il RPD sia "tempestivamente e adeguatamente coinvolto in tutte le questioni riguardanti la protezione dei dati personali".

È essenziale che il RPD, o il suo team di collaboratori, sia coinvolto quanto prima possibile in ogni questione attinente la protezione dei dati. Per quanto concerne le valutazioni di impatto sulla protezione dei dati, il regolamento prevede espressamente che il RPD vi sia coinvolto fin dalle fasi iniziali e specifica che il titolare del trattamento ha l'obbligo di consultarlo nell'effettuazione di tali valutazioni[33]. Assicurare il tempestivo e immediato

32 Si osservi che l'articolo 33, paragrafo 3, lettera b), ove sono indicate le informazioni da fornire all'autorità di controllo e agli interessati in caso di violazione dei dati personali, prevede, a differenza dell'articolo 37, paragrafo 7, che tali informazioni comprendano anche il nominativo (e non solo le informazioni di contatto) del RPD.

33 Articolo 35, paragrafo 2.

coinvolgimento del RPD, tramite la sua informazione e consultazione fin dalle fasi iniziali, faciliterà l'osservanza del RGPD e promuoverà l'applicazione del principio di privacy (e protezione dati) fin dalla fase di progettazione; pertanto, questo dovrebbe rappresentare l'approccio standard all'interno della struttura del titolare/responsabile del trattamento. Inoltre, è importante che il RPD sia annoverato fra gli interlocutori all'interno della struttura suddetta, e che partecipi ai gruppi di lavoro che volta per volta si occupano delle attività di trattamento.
Ciò significa che occorrerà garantire, per esempio:

- che il RPD sia invitato a partecipare su base regolare alle riunioni del management di alto e medio livello;
- la presenza del RPD ogniqualvolta debbano essere assunte decisioni che impattano sulla protezione dei dati. Il RPD deve disporre tempestivamente di tutte le informazioni pertinenti in modo da poter rendere una consulenza idonea;
- che il parere del RPD riceva sempre la dovuta considerazione. In caso di disaccordi, il Gruppo di lavoro raccomanda, quale buona prassi, di documentare le motivazioni che hanno portato a condotte difformi da quelle raccomandate dal RPD;
- che il RPD sia consultato tempestivamente qualora si verifichi una violazione dei dati o un altro incidente.

Ove opportuno, il titolare del trattamento o il responsabile del trattamento potrebbero mettere a punto linee guida ovvero programmazioni in materia di protezione dei dati che indichino i casi di consultazione obbligatoria del RPD.

3.2. Risorse necessarie

L'articolo 38, paragrafo 2, del RGPD obbliga il titolare del trattamento o il responsabile del trattamento a sostenere il RPD "fornendogli le risorse necessarie per assolvere tali compiti e accedere ai dati personali e ai trattamenti e per mantenere la propria conoscenza specialistica". Ciò si traduce, in modo particolare, nelle indicazioni seguenti:

- supporto attivo delle funzioni del RPD da parte del senior management (per esempio, a livello del consiglio di amministrazione);
- tempo sufficiente per l'espletamento dei compiti affidati al RPD. Ciò riveste particolare importanza se viene designato un RPD interno con un contratto part-time, oppure se il RPD esterno si occupa di protezione dati oltre a svolgere altre incombenze. In caso contrario, il rischio è che le attività cui il RPD è chiamato finiscano per essere trascurate a causa di conflitti con altre priorità. È fondamentale disporre

di tempo sufficiente da dedicare allo svolgimento dei compiti previsti per il RPD; una prassi da raccomandare consiste nel definire la percentuale del tempo lavorativo destinata alle attività di RPD quando quest'ultimo svolga anche altre funzioni. Un'altra buona prassi consiste nello stabilire il tempo necessario per adempiere alle relative incombenze, definire il livello di priorità spettante a tale incombenze, e prevedere che il RPD stesso (ovvero l'azienda/l'organismo titolare o responsabile) rediga un piano di lavoro;

- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della nomina del RPD a tutto il personale, in modo da garantire che la sua presenza e le sue funzioni siano note all'interno dell'azienda/dell'organismo;
- accesso garantito ad altri servizi (risorse umane, ufficio giuridico, IT, sicurezza, ecc.) così da fornire al RPD supporto, informazioni e input essenziali;
- formazione permanente. I RPD devono avere la possibilità di curare il proprio aggiornamento con riguardo agli sviluppi nel settore della protezione dati. Ciò mira, in ultima analisi, a consentire un incremento continuo del livello di competenze proprio dei RPD, che dovrebbero essere incoraggiati a partecipare a corsi di formazione su materie attinenti alla protezione dei dati e ad altre occasioni di professionalizzazione (forum in materia di privacy, workshop, ecc.);
- alla luce delle dimensioni e della struttura della singola azienda/del singolo organismo, può risultare necessario costituire un ufficio o un gruppo di lavoro RPD (formato dal RPD stesso e dal rispettivo personale). In casi del genere, è opportuno definire con precisione la struttura interna del gruppo di lavoro nonché i compiti e le responsabilità individuali. Analogamente, se la funzione di RPD viene esercitata da un fornitore di servizi esterno all'azienda/all'organismo, potrà aversi la costituzione di un gruppo di lavoro formato da soggetti operanti per conto di tale fornitore e incaricati di svolgere le funzioni di RPD sotto la direzione di un responsabile che funga da contatto per il cliente.

In linea di principio, quanto più aumentano complessità e/o sensibilità dei trattamenti, tanto maggiori devono essere le risorse messe a disposizione del RPD. La funzione "protezione dati" deve poter operare con efficienza e contare su risorse sufficienti in proporzione al trattamento svolto.

3.3. Istruzioni e [significato di] "adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente"

L'articolo 38, paragrafo 3, fissa alcune garanzie essenziali per consentire ai RPD di operare con un grado sufficiente di autonomia all'interno dell'organizzazione del titolare/responsabile del trattamento. In particolare, questi ultimi sono tenuti ad assicurare che il RPD "non riceva alcuna istruzione per quanto riguarda l'esecuzione di tali compiti". Il considerando 97 aggiunge che i RPD "dipendenti o meno del titolare del trattamento, dovrebbero poter adempiere alle funzioni e ai compiti loro incombenti in maniera indipendente".

Ciò significa che il RPD, nell'esecuzione dei compiti attribuitigli ai sensi dell'articolo 39, non deve ricevere istruzioni sull'approccio da seguire nel caso specifico – quali siano i risultati attesi, come condurre gli accertamenti su un reclamo, se consultare o meno l'autorità di controllo. Né deve ricevere istruzioni sull'interpretazione da dare a una specifica questione attinente alla normativa in materia di protezione dei dati.

Tuttavia, l'autonomia del RPD non significa che quest'ultimo disponga di un margine decisionale superiore al perimetro dei compiti fissati nell'articolo 39.

Il titolare del trattamento o il responsabile del trattamento mantengono la piena responsabilità dell'osservanza della normativa in materia di protezione dei dati e devono essere in grado di dimostrare tale osservanza[34]. Se il titolare del trattamento o il responsabile del trattamento assumono decisioni incompatibili con il RGPD e le indicazioni fornite dal RPD, quest'ultimo dovrebbe avere la possibilità di manifestare il proprio dissenso al più alto livello del management e ai decisori. Al riguardo, l'articolo 38, paragrafo 3, prevede che il RPD "riferisce direttamente al vertice gerarchico del titolare del trattamento o del responsabile del trattamento". Tale rapporto diretto garantisce che il vertice amministrativo (per esempio, il consiglio di amministrazione) sia a conoscenza delle indicazioni e delle raccomandazioni fornite dal RPD nel quadro della sue funzioni di informazione e consulenza a favore del titolare del trattamento o del responsabile del trattamento. Un altro esempio di tale rapporto diretto consiste nella redazione di una relazione annuale delle attività svolte dal RPD da sottoporre al vertice gerarchico.

3.4. Rimozione o penalizzazioni in rapporto all'adempimento dei compiti di RPD

L'articolo 38, paragrafo 3, prevede che il RPD "non è rimosso o penalizzato dal titolare del trattamento o dal responsabile del trattamento per l'adempimento dei propri compiti".

34 Articolo 5, paragrafo 2.

Questa prescrizione mira a potenziare l'autonomia del RPD e ad assicurarne l'indipendenza nell'adempimento dei compiti assegnatigli, attraverso la previsione di un'adeguata tutela.

Il divieto di penalizzazioni menzionato nel RGPD si applica solo con riguardo a quelle penalizzazioni eventualmente derivanti dallo svolgimento dei compiti propri del RPD. Per esempio, un RPD può ritenere che un determinato trattamento comporti un rischio elevato e quindi raccomandare al titolare del trattamento o al responsabile del trattamento di condurre una valutazione di impatto, ma questi ultimi non concordano con la valutazione del RPD. In casi del genere non è ammissibile che il RPD sia rimosso dall'incarico per avere formulato la raccomandazione in oggetto.

Le penalizzazioni possono assumere molte forme e avere natura diretta o indiretta. Per esempio, potrebbero consistere nella mancata o ritardata promozione, nel blocco delle progressioni di carriera, nella mancata concessione di incentivi rispetto ad altri dipendenti. Non è necessario che si arrivi all'effettiva applicazione di una penalizzazione, essendo sufficiente anche la sola minaccia nella misura in cui sia rivolta al RPD in rapporto alle attività da questi svolte.

Viceversa, e conformemente alle normali regole di gestione applicabili a ogni altro dipendente o fornitore soggetto alla disciplina del rispettivo contratto nazionale ovvero alle norme di diritto penale e del lavoro, sarebbe legittimamente possibile interrompere il rapporto con il RPD per motivazioni diverse dallo svolgimento dei compiti che gli sono propri: per esempio, in caso di furto, molestie sessuali o di altro genere, o altre analoghe e gravi violazioni deontologiche.

In questo ambito va rilevato che il RGPD non specifica le modalità e la tempistica riferite alla cessazione del rapporto di lavoro del RPD o alla sua sostituzione. Tuttavia, quanto maggiore è la stabilità del contratto stipulato con il RPD e maggiori le tutele previste contro l'ingiusto licenziamento, tanto maggiore sarà la probabilità che l'azione del RPD si svolga in modo indipendente. Il Gruppo di lavoro vede, quindi, con favore ogni iniziativa assunta in tal senso dai titolari del trattamento e responsabili del trattamento.

3.5. Conflitto di interessi

In base all'articolo 38, paragrafo 6, al RPD è consentito di "svolgere altri compiti e funzioni", ma a condizione che il titolare del trattamento o il responsabile del trattamento si assicuri che "tali compiti e funzioni non diano adito a un conflitto di interessi".

L'assenza di conflitti di interessi è strettamente connessa agli obblighi di indipendenza. Anche se un RPD può svolgere altre funzioni, l'affidamento di tali ulteriori compiti e funzioni è possibile solo a condizione che essi non diano adito a conflitti di interessi. Ciò significa, in modo particolare, che un RPD non può rivestire, all'interno dell'organizzazione

del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.
A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare o il responsabile in un giudizio che tocchi problematiche di protezione dei dati.
A seconda delle attività, delle dimensioni e della struttura organizzativa del titolare del trattamento o del responsabile del trattamento, si possono indicare le seguenti buone prassi:

- individuare le qualifiche e funzioni che sarebbero incompatibili con quella di RPD;
- redigere regole interne a tale scopo onde evitare conflitti di interessi;
- prevedere un'illustrazione più articolata dei casi di conflitto di interessi;
- dichiarare che il RPD non versa in alcuna situazione di conflitto di interessi con riguardo alle funzioni di RPD, al fine di sensibilizzare rispetto al requisito in questione;
- prevedere specifiche garanzie nelle regole interne e fare in modo che nel segnalare la disponibilità di una posizione lavorativa quale RPD ovvero nel redigere il contratto di servizi si utilizzino formulazioni sufficientemente precise e dettagliate così da prevenire conflitti di interessi. Al riguardo, si deve ricordare, inoltre, che un conflitto di interessi può assumere varie configurazioni a seconda che il RPD sia designato fra soggetti interni o esterni all'organizzazione.

4. Compiti del RPD

4.1. Sorvegliare l'osservanza del RGPD

L'articolo 39, paragrafo 1, lettera b), affida al RPD, fra gli altri, il compito di sorvegliare l'osservanza del RGPD. Nel considerando 97 si specifica che il titolare del trattamento

o il responsabile del trattamento dovrebbe essere "assistito [dal RPD] nel controllo del rispetto a livello interno del presente regolamento".
Fanno parte di questi compiti di controllo svolti dal RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità,
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare o responsabile.

Il controllo del rispetto del regolamento non significa che il RPD sia personalmente responsabile in caso di inosservanza. Il RGPD chiarisce che spetta al titolare, e non al RPD, "mette[re] in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento" (articolo 24, paragrafo 1). Il rispetto delle norme in materia di protezione dei dati fa parte della responsabilità d'impresa del titolare del trattamento, non del RPD.

4.2. Il ruolo del RPD nella valutazione di impatto sulla protezione dei dati

In base all'articolo 35, paragrafo 1, spetta al titolare del trattamento, e non al RPD, condurre, ove necessario, una valutazione di impatto sulla protezione dei dati (DPIA, nell'acronimo inglese). Tuttavia, il RPD svolge un ruolo fondamentale e di grande utilità assistendo il titolare nello svolgimento di tale DPIA. In ossequio al principio di "protezione dei dati fin dalla fase di progettazione" (o data protection by design), l'articolo 35, paragrafo 2, prevede in modo specifico che il titolare "si consulta" con il RPD quando svolge una DPIA. A sua volta, l'articolo 39, paragrafo 1, lettera c) affida al RPD il compito di "fornire, se richiesto, un parere in merito alla valutazione di impatto sulla protezione dei dati e sorvegliarne lo svolgimento ai sensi dell'articolo 35".
Il Gruppo di lavoro raccomanda che il titolare del trattamento si consulti con il RPD, fra l'altro, sulle seguenti tematiche[35]:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;

35 I compiti del RPD sono elencati all'articolo 39, paragrafo 1, ove si specifica che il RPD deve svolgere "almeno" i compiti in questione. Ne deriva che niente vieta al titolare di assegnare al RPD compiti ulteriori rispetto a quelli espressamente menzionati all'articolo 39, paragrafo 1, ovvero di specificare ulteriormente i suddetti compiti.

- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi al RGPD.

Qualora il titolare del trattamento non concordi con le indicazioni fornite dal RPD, è necessario che la documentazione relativa alla DPIA riporti specificamente per iscritto le motivazioni per cui si è ritenuto di non conformarsi a tali indicazioni[36].
Inoltre, il Gruppo di lavoro raccomanda che il titolare del trattamento definisca con chiarezza, per esempio nel contratto stipulato con il RPD, ma anche fornendo informative ai dipendenti, agli amministratori e, ove pertinente, ad altri aventi causa, i compiti specificamente affidati al RPD e i rispettivi ambiti, con particolare riguardo alla conduzione della DPIA.

4.3. Cooperazione con l'autorità di controllo e funzione di punto di contatto

In base all'articolo 39, paragrafo 1, lettere d) ed e), il RPD deve "cooperare con l'autorità di controllo" e "fungere da punto di contatto per l'autorità di controllo per questioni connesse al trattamento, tra cui la consultazione preventiva di cui all'articolo 36, ed effettuare, se del caso, consultazioni relativamente a ogni altra questione".
Questi compiti attengono al ruolo di "facilitatore" attribuito al RPD e già menzionato nell'introduzione alle presenti linee guida. Il RPD funge da punto di contatto per facilitare l'accesso, da parte dell'autorità di controllo, ai documenti e alle informazioni necessarie per l'adempimento dei compiti attribuitile dall'articolo 57 nonché ai fini dell'esercizio dei poteri di indagine, correttivi, autorizzativi e consultivi di cui all'articolo 58. Si è già rilevato che il RPD è tenuto al rispetto delle norme in materia di segreto o riservatezza, in conformità del diritto dell'Unione o degli Stati membri (articolo 38, paragrafo 5); tuttavia, tali vincoli di segreto/riservatezza non precludono la possibilità per il RPD di contattare e chiedere lumi all'autorità di controllo. L'articolo 39, paragrafo 1, prevede che il RPD possa consultare l'autorità di controllo con riguardo a qualsiasi altra questione, se del caso.

36 L'articolo 24, paragrafo 1, prevede che "Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".

4.4. Approccio basato sul rischio

In base all'articolo 39, paragrafo 2, il RPD deve "considera[re] debitamente i rischi inerenti al trattamento, tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del medesimo".

Si tratta di una disposizione di portata generale e ispirata a criteri di buon senso, verosimilmente applicabile sotto molti riguardi all'attività quotidiana del RPD. In sostanza, si chiede al RPD di definire un ordine di priorità nell'attività svolta e di concentrarsi sulle questioni che presentino maggiori rischi in termini di protezione dei dati. Seppure ciò non significhi che il RPD debba trascurare di sorvegliare il grado di conformità di altri trattamenti associati a un livello di rischio comparativamente inferiore, di fatto la disposizione segnala l'opportunità di dedicare attenzione prioritaria agli ambiti che presentino rischi più elevati.

Attraverso questo approccio selettivo e pragmatico, il RPD dovrebbe essere più facilmente in grado di consigliare al titolare quale metodologia seguire nel condurre una DPIA, a quali settori riservare un audit interno o esterno in tema di protezione dei dati, quali attività di formazione interna prevedere per il personale o gli amministratori che trattino dati personali, e a quali trattamenti dedicare maggiori risorse e tempo.

4.5. Il ruolo del RPD nella tenuta del registro delle attività di trattamento

L'articolo 30, primo e paragrafo 2, prevede che sia il titolare del trattamento o il responsabile del trattamento, e non il RPD, a "ten[ere] un registro delle attività di trattamento svolte sotto la propria responsabilità" ovvero "un registro di tutte le categorie di trattamento svolte per conto di un titolare del trattamento".

Nella realtà, sono spesso i RPD a realizzare l'inventario dei trattamenti e tenere un registro di tali trattamenti sulla base delle informazioni fornite loro dai vari uffici o unità che trattano dati personali. È una prassi consolidata e fondata sulle disposizioni di numerose leggi nazionali nonché sulla normativa in materia di protezione dati applicabile alle istituzioni e agli organismi dell'UE[37].

L'articolo 39, paragrafo 1, contiene un elenco non esaustivo dei compiti affidati al RPD. Pertanto, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto

37 Si veda l'articolo 24, paragrafo 1, lettera d), del regolamento (CE) 45/2001.

del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.
In ogni caso, il registro la cui tenuta è obbligatoria ai sensi dell'articolo 30 deve essere considerato anche uno strumento che consente al titolare del trattamento e all'autorità di controllo, su richiesta, di disporre di un quadro complessivo dei trattamenti di dati personali svolti dallo specifico soggetto. In quanto tale, esso costituisce un presupposto indispensabile ai fini dell'osservanza delle norme e, pertanto, un'efficace misura di responsabilizzazione.

5. Allegato alle linee guida sul RPD - Indicazioni essenziali

L'allegato intende rispondere, in forma sintetica e semplificata, ad alcune delle domande fondamentali rispetto al nuovo obbligo di designazione di un RPD fissato nel regolamento generale sulla protezione dei dati.

Designazione del RPD

1. Chi è tenuto a designare un RPD?

La designazione di un RPD è obbligatoria:

- se il trattamento è svolto da un'autorità pubblica o da un organismo pubblico;
- se le attività principali del titolare del trattamento o del responsabile del trattamento consistono in trattamenti che richiedono il monitoraggio regolare e sistematico di interessati su larga scala; oppure
- se le attività principali del titolare del trattamento o del responsabile del trattamento consistono nel trattamento su larga scala di categorie particolari di dati o di dati personali relativi a condanne penali e reati.

Si tenga presente che la designazione obbligatoria di un RPD può essere prevista anche in casi ulteriori in base alla legge nazionale o al diritto dell'UE. Inoltre, anche ove la designazione di un RPD non sia obbligatoria, può risultare utile procedere a tale designazione su base volontaria. Il Gruppo di lavoro "Articolo 29" (Gruppo di lavoro) incoraggia un approccio di questo genere. Qualora si proceda alla designazione di un RPD su base volontaria, si applicano gli identici requisiti - in termini di criteri per la designazione, posizione e compiti - che valgono per i RPD designati in via obbligatoria.
Fonte: articolo 37(1) RGPD

2. Cosa significa “attività principali”?

Con “attività principali” si possono intendere le operazioni essenziali che sono necessarie al raggiungimento degli obiettivi perseguiti dal titolare del trattamento o dal responsabile del trattamento, comprese tutte quelle attività per le quali il trattamento dei dati è inscindibilmente connesso all’attività del titolare del trattamento o del responsabile del trattamento. Per esempio, il trattamento di dati relativi alla salute (come le cartelle sanitarie dei pazienti) è da ritenersi una delle attività principali di qualsiasi ospedale; ne deriva che tutti gli ospedali dovranno designare un RPD.

D’altra parte, tutti gli organismi (pubblici e privati) svolgono determinate attività quali il pagamento delle retribuzioni al personale ovvero dispongono di strutture standard di supporto informatico. Si tratta di esempi di funzioni di supporto necessarie ai fini dell’attività principale o dell’oggetto principale del singolo organismo, ma pur essendo necessarie o perfino essenziali sono considerate solitamente di natura accessoria e non vengono annoverate fra le attività principali.

Fonte: articolo 37, paragrafo 1, lettere b) e c) RGPD

3. Cosa significa “su larga scala”?

Il regolamento non definisce cosa rappresenti un trattamento “su larga scala”. Il Gruppo di lavoro raccomanda di tenere conto, in particolare, dei fattori qui elencati al fine di stabilire se un trattamento sia effettuato su larga scala:

- il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
- il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
- la durata, ovvero la persistenza, dell’attività di trattamento;
- la portata geografica dell’attività di trattamento.

Alcuni esempi di trattamento su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un ospedale nell’ambito delle ordinarie attività;
- trattamento di dati relativi agli spostamenti di utenti di un servizio di trasporto pubblico cittadino (per esempio, il loro tracciamento attraverso titoli di viaggio);
- trattamento di dati di geolocalizzazione raccolti in tempo reale per finalità statistiche da un responsabile specializzato nella prestazione di servizi di questo tipo rispetto ai clienti di una catena internazionale di fast food;

- trattamento di dati relativi alla clientela da parte di una compagnia assicurativa o di una banca nell'ambito delle ordinarie attività;
- trattamento di dati personali da parte di un motore di ricerca per finalità di pubblicità comportamentale;
- trattamento di dati (metadati, contenuti, ubicazione) da parte di fornitori di servizi telefonici o telematici.

Alcuni esempi di trattamento non su larga scala sono i seguenti:

- trattamento di dati relativi a pazienti svolto da un singolo professionista sanitario;
- trattamento di dati personali relativi a condanne penali e reati svolto da un singolo avvocato.

Fonte: articolo 37, paragrafo 1, lettere b) e c), RGPD

4. Cosa significa "monitoraggio regolare e sistematico"?

Il concetto di monitoraggio regolare e sistematico degli interessati non trova definizione all'interno del RGPD; tuttavia, esso comprende senza dubbio tutte le forme di tracciamento e profilazione su Internet anche per finalità di pubblicità comportamentale. Non si tratta, però, di un concetto riferito esclusivamente all'ambiente online.

Alcune esemplificazioni di attività che possono configurare un monitoraggio regolare e sistematico di interessati: curare il funzionamento di una rete di telecomunicazioni; la prestazione di servizi di telecomunicazioni; il reindirizzamento di messaggi di posta elettronica; attività di marketing basate sull'analisi dei dati raccolti; profilazione e scoring per finalità di valutazione del rischio (per esempio, a fini di valutazione del rischio creditizio, definizione dei premi assicurativi, prevenzione delle frodi, accertamento di forme di riciclaggio); tracciamento dell'ubicazione, per esempio da parte di app su dispositivi mobili; programmi di fidelizzazione; pubblicità comportamentale; monitoraggio di dati relativi allo stato di benessere psicofisico, alla forma fisica e alla salute attraverso dispositivi indossabili; utilizzo di telecamere a circuito chiuso; dispositivi connessi quali contatori intelligenti, automobili intelligenti, dispositivi per la domotica, ecc.

L'aggettivo "regolare" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

- che avviene in modo continuo ovvero a intervalli definiti per un arco di tempo definito;
- ricorrente o ripetuto a intervalli costanti;

› che avviene in modo costante o a intervalli periodici.

L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del Gruppo di lavoro:

› che avviene per sistema;
› predeterminato, organizzato o metodico;
› che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
› svolto nell'ambito di una strategia.

Fonte: articolo 37, paragrafo 1, lettera b), RGPD

5. È ammessa la designazione congiunta di uno stesso RPD da parte di più soggetti? E a quali condizioni?
Sì. Un gruppo imprenditoriale può nominare un unico RPD a condizione che quest'ultimo sia "facilmente raggiungibile da ciascuno stabilimento". Il concetto di raggiungibilità si riferisce ai compiti del RPD in quanto punto di contatto per gli interessati, l'autorità di controllo e i soggetti interni all'organismo o all'ente. Allo scopo di assicurare la raggiungibilità del RPD, interno o esterno, è importante garantire la disponibilità dei dati di contatto nei termini previsti dal RGPD. Il RPD, supportato da un apposito team se necessario, deve essere in grado di comunicare con gli interessati in modo efficiente e di collaborare con le autorità di controllo interessate. Ciò significa che le comunicazioni in questione devono avvenire nella lingua utilizzata dalle autorità di controllo e dagli interessati volta per volta in causa. Il fatto che il RPD sia raggiungibile – vuoi fisicamente all'interno dello stabile ove operano i dipendenti, vuoi attraverso una linea dedicata o altri mezzi idonei e sicuri di comunicazione – è fondamentale al fine di garantire all'interessato la possibilità di contattare il RPD stesso.
È ammessa la designazione di un unico RPD per più autorità pubbliche o organismi pubblici, tenuto conto della loro struttura organizzativa e dimensione. Valgono le stesse considerazioni svolte in tema di risorse e comunicazioni. Poiché il RPD è chiamato a una molteplicità di funzioni, il titolare del trattamento o il responsabile del trattamento deve assicurarsi che un unico RPD, se necessario supportato da un team di collaboratori, sia in grado di adempiere in modo efficiente a tali funzioni anche se designato da una molteplicità di autorità e organismi pubblici
Fonte: articolo 37, paragrafi 2) e 3), RGPD

6. Dove dovrebbe collocarsi il RPD?

Per garantire l'accessibilità del RPD, il Gruppo di lavoro raccomanda la sua collocazione nel territorio dell'Unione europea, indipendentemente dall'esistenza di uno stabilimento del titolare o del responsabile nell'UE. Tuttavia, non si può escludere che un RPD sia in grado di adempiere ai propri compiti con maggiore efficacia operando al di fuori dell'UE in alcuni casi ove titolare del trattamento o responsabile del trattamento non sono stabiliti nel territorio dell'Unione europea.

7. Si può designare un RPD esterno?

Sì. Il RPD può far parte del personale del titolare del trattamento o del responsabile del trattamento (RPD interno) ovvero "assolvere i suoi compiti in base a un contratto di servizi". In quest'ultimo caso il RPD sarà esterno e le sue funzioni saranno esercitate sulla base di un contratto di servizi stipulato con una persona fisica o giuridica.

Se la funzione di RPD è svolta da un fornitore esterno di servizi, i compiti stabiliti per il RPD potranno essere assolti efficacemente da un team operante sotto l'autorità di un contatto principale designato e "responsabile" per il singolo cliente. In tal caso, è indispensabile che ciascun soggetto appartenente al fornitore esterno operante quale RPD soddisfi tutti i requisiti applicabili come fissati nel RGPD.

Per favorire efficienza e correttezza e prevenire conflitti di interesse a carico dei componenti il team, le linee guida raccomandano di procedere a una chiara ripartizione dei compiti nel team del RPD esterno, attraverso il contratto di servizi, e di prevedere che sia un solo soggetto a fungere da contatto principale e "incaricato" per ciascun cliente.

Fonte: articolo 37, paragrafo 6, RGPD

8. Quali sono le qualità professionali che un RPD deve possedere?

Il RPD "è designato in funzione delle qualità professionali, in particolare della conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, e della capacità di assolvere i [rispettivi] compiti".

Il livello necessario di conoscenza specialistica dovrebbe essere determinato in base ai trattamenti di dati effettuati e alla protezione richiesta per i dati personali oggetto di trattamento. Per esempio, se un trattamento riveste particolare complessità oppure comporta un volume consistente di dati sensibili, il RPD avrà probabilmente bisogno di un livello più elevato di conoscenze specialistiche e di supporto.

Fra le competenze e conoscenze specialistiche pertinenti rientrano le seguenti:

- conoscenza della normativa e delle prassi nazionali ed europee in materia di protezione dei dati, compresa un'approfondita conoscenza del RGPD;

- familiarità con le operazioni di trattamento svolte;
- familiarità con tecnologie informatiche e misure di sicurezza dei dati;
- conoscenza dello specifico settore di attività e dell'organizzazione del titolare/del responsabile;
- capacità di promuovere una cultura della protezione dati all'interno dell'organizzazione del titolare/del responsabile.

Fonte: articolo 37, paragrafo 5, RGPD

Posizione del RPD

9. Quali sono le risorse che titolare del trattamento o responsabile del trattamento dovrebbero mettere a disposizione del RPD?

Il RPD deve disporre delle risorse necessarie per assolvere i propri compiti.
A seconda della natura dei trattamenti, e delle attività e dimensioni della struttura del titolare del trattamento o del responsabile del trattamento, il RPD dovrebbe poter contare sulle seguenti risorse:

- supporto attivo della funzione di RPD da parte del senior management;
- tempo sufficiente per l'espletamento dei compiti affidati;
- supporto adeguato in termini di risorse finanziarie, infrastrutture (sede, attrezzature, strumentazione) e, ove opportuno, personale;
- comunicazione ufficiale della designazione del RPD a tutto il personale;
- accesso garantito ad altri servizi all'interno della struttura del titolare/del responsabile del trattamento in modo da ricevere tutto il supporto, le informazioni o gli input necessari;
- formazione permanente.

Fonte: articolo 38, paragrafo 2, RGPD

10. Quali sono le garanzie che possono consentire al RPD di operare con indipendenza? Cosa significa "conflitto di interessi"?
Vi sono numerose garanzie che possono consentire al RPD di operare in modo indipendente:

- nessuna istruzione da parte del titolare del trattamento o del responsabile del trattamento per quanto riguarda lo svolgimento dei compiti affidati al RPD;
- nessuna penalizzazione o rimozione dall'incarico in rapporto allo svolgimento dei compiti affidati al RPD;
- nessun conflitto di interessi con eventuali ulteriori compiti e funzioni.

Gli "altri compiti e funzioni" del RPD non devono comportare conflitti di interessi. Ciò significa, in primo luogo, che il RPD non può rivestire, all'interno dell'organizzazione del titolare del trattamento o del responsabile del trattamento, un ruolo che comporti la definizione delle finalità o modalità del trattamento di dati personali. Si tratta di un elemento da tenere in considerazione caso per caso guardando alla specifica struttura organizzativa del singolo titolare del trattamento o responsabile del trattamento.
A grandi linee, possono sussistere situazioni di conflitto all'interno dell'organizzazione con riguardo a ruoli manageriali di vertice (amministratore delegato, responsabile operativo, responsabile finanziario, responsabile sanitario, direzione marketing, direzione risorse umane, responsabile IT), ma anche rispetto a posizioni gerarchicamente inferiori se queste ultime comportano la determinazione di finalità o mezzi del trattamento. Inoltre, può insorgere un conflitto di interessi se, per esempio, a un RPD esterno si chiede di rappresentare il titolare del trattamento o il responsabile del trattamento in un giudizio che tocchi problematiche di protezione dei dati.
Fonte: articolo 38, paragrafi 3 e 6, RGPD

Compiti del RPD

11. Che cosa si intende per "sorvegliare l'osservanza"
Fanno parte di questi compiti di controllo del RPD, in particolare,

- la raccolta di informazioni per individuare i trattamenti svolti;
- l'analisi e la verifica dei trattamenti in termini di loro conformità, e
- l'attività di informazione, consulenza e indirizzo nei confronti di titolare del trattamento o responsabile del trattamento.

Fonte: articolo 39, paragrafo 1, lettera b), RGPD

12. Il RPD è personalmente responsabile in caso di inosservanza degli obblighi in materia di protezione dei dati?

No, il RPD non è responsabile personalmente in caso di inosservanza degli obblighi in materia di protezione dei dati. Spetta al titolare del trattamento o al responsabile del trattamento garantire ed essere in grado di dimostrare che il trattamento è effettuato conformemente al regolamento. La responsabilità di garantire l'osservanza della normativa in materia di protezione dei dati ricade sul titolare del trattamento o sul responsabile del trattamento.

13. Quale ruolo spetta al RPD con riguardo alla valutazione di impatto sulla protezione dei dati e alla tenuta del registro dei trattamenti?

Per quanto concerne la valutazione di impatto sulla protezione dei dati, il titolare del trattamento o il responsabile del trattamento dovrebbero consultarsi con il RPD, fra l'altro, sulle seguenti tematiche:

- se condurre o meno una DPIA;
- quale metodologia adottare nel condurre una DPIA;
- se condurre la DPIA con le risorse interne ovvero esternalizzandola;
- quali salvaguardie applicare, comprese misure tecniche e organizzative, per attenuare i rischi per i diritti e gli interessi delle persone interessate;
- se la DPIA sia stata condotta correttamente o meno, e se le conclusioni raggiunte (procedere o meno con il trattamento, e quali salvaguardie applicare) siano conformi ai requisiti in materia di protezione dei dati.

Per quanto riguarda il registro dei trattamenti, la sua tenuta è un obbligo che ricade sul titolare del trattamento o sul responsabile del trattamento, e non sul RPD. Ciononostante, niente vieta al titolare del trattamento o al responsabile del trattamento di affidare al RPD il compito di tenere il registro delle attività di trattamento sotto la responsabilità del titolare o del responsabile stesso. Tale registro va considerato uno degli strumenti che consentono al RPD di adempiere agli obblighi di sorveglianza del rispetto del regolamento, informazione e consulenza nei riguardi del titolare del trattamento o del responsabile del trattamento.

Fonte: articolo 39, paragrafo 1, lettera c) e articolo 30, RGPD

Linee guida del gruppo dei Garanti Europei concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" - WP 243, rev. 01

Adottate il 4 aprile 2017

I. Introduzione

Il regolamento (UE) 2016/679[1] ("regolamento generale sulla protezione dei dati") si applicherà a partire dal 25 maggio 2018. L'articolo 35 del regolamento generale sulla protezione dei dati introduce il concetto di valutazione d'impatto sulla protezione dei dati[2], così come previsto anche dalla direttiva 2016/680[3].

Una valutazione d'impatto sulla protezione dei dati è un processo inteso a descrivere il trattamento, valutarne la necessità e la proporzionalità, nonché a contribuire a gestire i rischi per i diritti e le libertà delle persone fisiche derivanti dal trattamento di dati personali[4], valutando detti rischi e determinando le misure per affrontarli. Le valutazioni

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

2 In altri contesti il termine "valutazione dell'impatto sulla vita privata" è spesso utilizzato per fare riferimento allo stesso concetto.

3 L'articolo 27 della direttiva (UE) 2016/680 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, nonché alla libera circolazione di tali dati, prevede altresì che sia necessaria una valutazione dell'impatto sulla vita privata *"quando il trattamento può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*.

4 Il regolamento generale sulla protezione dei dati non definisce formalmente il concetto di valutazione d'impatto sulla protezione dei dati come tale, tuttavia

- il suo contenuto minimo è specificato dall'articolo 35, paragrafo 7, come segue:
  - *"a) una descrizione sistematica dei trattamenti previsti e delle finalità del trattamento, compreso, ove applicabile, l'interesse legittimo perseguito dal titolare del trattamento;*
  - *b) una valutazione della necessità e proporzionalità dei trattamenti in relazione alle finalità;*
  - *c) una valutazione dei rischi per i diritti e le libertà degli interessati di cui al paragrafo 1; e*

d'impatto sulla protezione dei dati sono strumenti importanti per la responsabilizzazione in quanto sostengono i titolari del trattamento non soltanto nel rispettare i requisiti del regolamento generale sulla protezione dei dati, ma anche nel dimostrare che sono state adottate misure appropriate per garantire il rispetto del regolamento (cfr. anche l'articolo 24)[5]. In altre parole, **una valutazione d'impatto sulla protezione dei dati è un processo inteso a garantire e dimostrare la conformità**.

A norma del regolamento generale sulla protezione dei dati, l'inosservanza dei requisiti stabiliti per la valutazione d'impatto sulla protezione dei dati può portare a sanzioni pecuniarie imposte dall'autorità di controllo competente. La mancata esecuzione di una valutazione d'impatto sulla protezione dei dati nei casi in cui il trattamento è soggetto alla stessa (articolo 35, paragrafi 1, 3 e 4), l'esecuzione in maniera errata di detta valutazione (articolo 35, paragrafi 2 e da 7 a 9) oppure la mancata consultazione dell'autorità di controllo laddove richiesto (articolo 36, paragrafo 3, lettera e)), possono comportare una sanzione amministrativa pecuniaria pari a un importo massimo di 10 milioni di EUR oppure, nel caso di un'impresa, pari a fino al 2% del fatturato annuo globale dell'anno precedente, a seconda di quale dei due importi sia quello superiore.

II. Campo di applicazione delle presenti linee guida

Le presenti linee guida tengono conto dei seguenti documenti:

› dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati (WP29) - 14/EN WP 218[6];

- *d) le misure previste per affrontare i rischi, includendo le garanzie, le misure di sicurezza e i meccanismi per garantire la protezione dei dati personali e dimostrare la conformità al presente regolamento, tenuto conto dei diritti e degli interessi legittimi degli interessati e delle altre persone in questione";*

- il suo significato e il suo ruolo sono chiariti dal considerando 84 come segue: *"[p]er potenziare il rispetto del presente regolamento qualora i trattamenti possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento dovrebbe essere responsabile dello svolgimento di una valutazione d'impatto sulla protezione dei dati per determinare, in particolare, l'origine, la natura, la particolarità e la gravità di tale rischio".*

5 Cfr. anche il considerando 84: *"[l]'esito della valutazione dovrebbe essere preso in considerazione nella determinazione delle opportune misure da adottare per dimostrare che il trattamento dei dati personali rispetta il presente regolamento".*

6 *"WP29 Statement 14/EN WP 218 on the role of a risk-based approach to data protection legal frameworks"* [Dichiarazione del WP29 14/EN WP 218 sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia

- linee guida sui responsabili della protezione dei dati del WP29 - 16/EN WP 243[7];
- parere del WP29 sulla limitazione della finalità - 13/EN WP 203[8];
- norme internazionali[9].

In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Infatti, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando il trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1). Al fine di assicurare un'interpretazione coerente delle circostanze in cui è obbligatorio realizzare una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 3), le presenti linee guida mirano innanzitutto a chiarire tale nozione e a fornire criteri per gli elenchi che devono essere adottati dalle autorità di protezione dei dati ai sensi dell'articolo 35, paragrafo 4.

A norma dell'articolo 70, paragrafo 1, lettera e), il comitato europeo per la protezione dei dati potrà pubblicare linee guida, raccomandazioni e migliori prassi al fine di promuovere l'applicazione coerente del regolamento generale sulla protezione dei dati. Lo scopo del presente documento è quindi quello di anticipare i futuri lavori del comitato europeo per la protezione dei dati e, di conseguenza, di chiarire le pertinenti disposizioni del regolamento generale sulla protezione dei dati in maniera da assistere i titolari del trattamento nel rispettare la legge, nonché da fornire la certezza del diritto a quei titolari del trattamento che sono tenuti a realizzare una valutazione d'impatto sulla protezione dei dati.

Le presenti linee guida mirano altresì a promuovere la redazione di:

---

di protezione dei dati], adottata il 30 maggio 2014. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp218_en.pdf?wb48617274=72C54532.

7 documento 16/EN WP 243 "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 adottate il 13 dicembre 2016. http://ec.europa.eu/information_society/newsroom/image/document/2016-51/wp243_en_40855.pdf?wb48617274=CD63BD9A.

8 *"WP29 Opinion 03/2013 on purpose limitation"* [Parere 03/2013 del WP29 sulla limitazione della finalità] - 13/EN WP 203, approvato il 2 aprile 2013. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf?wb48617274=39E0E409.

9 Ad esempio la norma ISO 31000:2009, Gestione del rischio - *Principi e linee guida*, Organizzazione internazionale per la normazione (ISO); ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO).

- un elenco comune dell'Unione europea delle tipologie di trattamento per le quali è obbligatorio procedere a una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4);
- un elenco comune dell'Unione europea delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5);
- criteri comuni sulla metodologia per la realizzazione di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5);
- criteri comuni che specifichino quando è necessario consultare l'autorità di controllo (articolo 36, paragrafo 1);
- raccomandazioni, ove possibile, basate sull'esperienza acquisita negli Stati membri dell'UE.

III. Valutazione d'impatto sulla protezione dei dati: spiegazione del regolamento

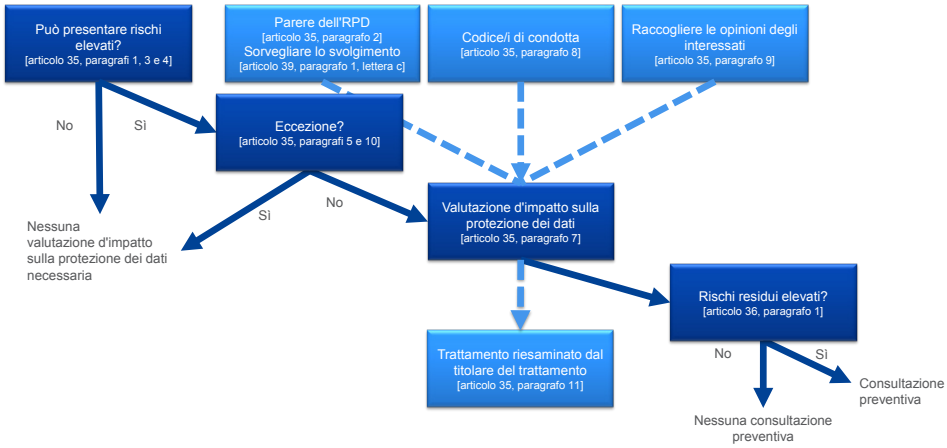
Il regolamento generale sulla protezione dei dati prevede che i titolari del trattamento attuino misure adeguate per garantire ed essere in grado di dimostrare il rispetto di detto regolamento, tenendo conto tra l'altro dei "rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche" (articolo 24, paragrafo 1) . L'obbligo per i titolari del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati va inteso nel contesto dell'obbligo generale, cui gli stessi sono soggetti, di gestire adeguatamente i rischi[10] presentati dal trattamento di dati personali.

Un "rischio" è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità. La "gestione dei rischi", invece, può essere definita come l'insieme delle attività coordinate volte a indirizzare e controllare un'organizzazione in relazione ai rischi.

L'articolo 35 fa riferimento al possibile rischio elevato "per i diritti e le libertà delle persone fisiche". Come indicato nella dichiarazione del gruppo di lavoro articolo 29 sulla protezione dei dati sul ruolo di un approccio basato sul rischio nei quadri giuridici in materia di protezione dei dati, il riferimento a "diritti e libertà" degli interessati riguarda principalmente i diritti alla protezione dei dati e alla vita privata, ma include anche altri

10 Va sottolineato che al fine di poter gestire i rischi per i diritti e le libertà delle persone fisiche, detti rischi devono essere regolarmente individuati, analizzati, stimati, valutati, trattati (ad esempio attenuati, ecc.) e riesaminati. I titolari del trattamento non possono sottrarsi alla loro responsabilità coprendo i rischi stipulando polizze assicurative.

diritti fondamentali quali la libertà di parola, la libertà di pensiero, la libertà di circolazione, il divieto di discriminazione, il diritto alla libertà di coscienza e di religione.
In linea con l'approccio basato sul rischio adottato dal regolamento generale sulla protezione dei dati, non è obbligatorio svolgere una valutazione d'impatto sulla protezione dei dati per ciascun trattamento. Al contrario, è necessario realizzare una valutazione d'impatto sulla protezione dei dati soltanto quando la tipologia di trattamento "può presentare un rischio elevato per i diritti e le libertà delle persone fisiche" (articolo 35, paragrafo 1). Il semplice fatto che le condizioni che comportano l'obbligo di realizzare una valutazione d'impatto sulla protezione dei dati non siano soddisfatte non diminuisce tuttavia l'obbligo generale, cui i titolari del trattamento sono soggetti, di attuare misure volte a gestire adeguatamente i rischi per i diritti e le libertà degli interessati. In pratica, ciò significa che i titolari del trattamento devono continuamente valutare i rischi creati dalle loro attività al fine di stabilire quando una tipologia di trattamento "possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche".
La figura che segue illustra i principi fondamentali relativi alla valutazione d'impatto sulla protezione dei dati di cui al regolamento generale sulla protezione dei dati:



A. Che cosa esamina una valutazione d'impatto sulla protezione dei dati? Un singolo trattamento o un insieme di trattamenti simili.

Una valutazione d'impatto sulla protezione dei dati può riguardare una singola operazione di trattamento dei dati. Tuttavia, l'articolo 35, paragrafo 1, indica che *"[u]na singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi". Il considerando 92 aggiunge che "[v]i sono circostanze in cui può essere ragionevole ed economico effettuare una valutazione d'impatto sulla protezione dei dati che*

verta su un oggetto più ampio di un unico progetto, per esempio quando autorità pubbliche o enti pubblici intendono istituire un'applicazione o una piattaforma di trattamento comuni o quando diversi titolari del trattamento progettano di introdurre un'applicazione o un ambiente di trattamento comuni in un settore o segmento industriale o per una attività trasversale ampiamente utilizzata".

Si potrebbe ricorrere a una singola valutazione d'impatto sulla protezione dei dati nel caso di trattamenti multipli simili tra loro in termini di natura, ambito di applicazione, contesto, finalità e rischi. In effetti, le valutazioni d'impatto sulla protezione dei dati mirano a studiare sistematicamente nuove situazioni che potrebbero portare a rischi elevati per i diritti e le libertà delle persone fisiche e non è necessario realizzare una valutazione d'impatto sulla protezione dei dati nei casi (ad esempio operazioni di trattamento in un contesto specifico e per una finalità specifica) che sono già stati studiati. Questo potrebbe essere il caso in cui si utilizzi una tecnologia simile per raccogliere la stessa tipologia di dati per le medesime finalità. Ad esempio, un gruppo di autorità comunali che istituiscono ciascuna un sistema di televisione a circuito chiuso simile potrebbe svolgere una singola valutazione d'impatto sulla protezione dei dati che copra il trattamento svolto da tali titolari del trattamento distinti; oppure un gestore ferroviario (un titolare del trattamento unico) potrebbe esaminare la videosorveglianza in tutte le sue stazioni ferroviarie realizzando una singola valutazione d'impatto sulla protezione dei dati. Ciò può essere applicabile anche a trattamenti simili attuati da vari titolari del trattamento di dati. In questi casi, è necessario condividere o rendere pubblicamente accessibile una valutazione d'impatto sulla protezione dei dati di riferimento, attuare le misure descritte nella stessa, e fornire una giustificazione per la realizzazione di una singola valutazione d'impatto sulla protezione dei dati.

Qualora il trattamento coinvolga contitolari del trattamento, questi ultimi devono definire con precisione le rispettive competenze. La loro valutazione d'impatto sulla protezione dei dati deve stabilire quale parte sia competente per le varie misure volte a trattare i rischi e a proteggere i diritti e le libertà degli interessati. Ciascun titolare del trattamento deve esprimere le proprie esigenze e condividere informazioni utili senza compromettere eventuali segreti (ad esempio protezione di segreti aziendali, proprietà intellettuale, informazioni aziendali riservate) o divulgare vulnerabilità.

Una valutazione d'impatto sulla protezione dei dati può essere altresì utile per valutare l'impatto sulla protezione dei dati di un prodotto tecnologico, ad esempio un dispositivo hardware o un software, qualora sia probabile che lo stesso venga utilizzato da titolari del trattamento distinti per svolgere tipologie diverse di trattamento. Ovviamente, il titolare del trattamento che utilizza detto prodotto resta soggetto all'obbligo di svolgere la propria valutazione d'impatto sulla protezione dei dati in relazione all'attuazione specifica, tuttavia tale valutazione del titolare del trattamento può utilizzare le informazioni

fornite da una valutazione analoga preparata dal fornitore del prodotto, se opportuno. Un esempio potrebbe essere rappresentato dalla relazione tra produttori di contatori intelligenti e società fornitrici di servizi pubblici. Ogni fornitore di prodotti o responsabile del trattamento dovrebbe condividere informazioni utili senza compromettere i segreti né generare rischi per la sicurezza, divulgando vulnerabilità.

B. Quali trattamenti sono soggetti a una valutazione d'impatto sulla protezione dei dati? Escludendo le eccezioni, in tutti i casi in cui tali trattamenti *"possono presentare un rischio elevato"*.

Questa sezione descrive i casi nei quali è richiesta una valutazione d'impatto sulla protezione dei dati e quelli che invece non la richiedono.

Fatti salvi i casi in cui un trattamento rientra nel campo di applicazione di un'eccezione (III.B.a), è necessario realizzare una valutazione d'impatto sulla protezione dei dati qualora un trattamento *"possa presentare un rischio elevato"* (III.B.b).

a) Quando è obbligatoria una valutazione d'impatto sulla protezione dei dati? Quando il trattamento *"può presentare un rischio elevato"*.

Il regolamento generale sulla protezione dei dati non richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati per ciascun trattamento che può presentare rischi per i diritti e le libertà delle persone fisiche. La realizzazione di una valutazione d'impatto sulla protezione dei dati è obbligatoria soltanto qualora il trattamento *"possa presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (articolo 35, paragrafo 1, illustrato dall'articolo 35, paragrafo 3, e integrato dall'articolo 35, paragrafo 4). Essa è particolarmente importante quando viene introdotta una nuova tecnologia di trattamento dei dati[11].

Nei casi in cui non è chiaro se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno, il WP29 raccomanda di effettuarla comunque, in quanto detta valutazione è uno strumento utile che assiste i titolari del trattamento a rispettare la legge in materia di protezione dei dati.

Sebbene una valutazione d'impatto sulla protezione dei dati possa essere richiesta anche in altre circostanze, l'articolo 35, paragrafo 3, fornisce alcuni esempi di casi nei quali un trattamento *"possa presentare rischi elevati"*:

- *"a) una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata su un trattamento automatizzato, compresa la profilazione, e sulla*

11 Cfr. i considerando 89 e 91 e l'articolo 35, paragrafi 1 e 3, per ulteriori esempi.

quale si fondano decisioni che hanno effetti giuridici o incidono in modo analogo significativamente su dette persone fisiche[12]*;*

- *b) il trattamento, su larga scala, di categorie particolari di dati personali di cui all'articolo 9, paragrafo 1, o di dati relativi a condanne penali e a reati di cui all'articolo 10*[13]*; o*
- *c) la sorveglianza sistematica su larga scala di una zona accessibile al pubblico".*

Come indicato dalle parole "*in particolare*" nella frase introduttiva dell'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati, questo va inteso come un elenco non esaustivo. Vi possono essere operazioni di trattamento a "rischio elevato" che non trovano collocazione in tale elenco ma che presentano tuttavia rischi altrettanto elevati. Anche tali trattamenti devono essere soggetti alla realizzazione di valutazioni d'impatto sulla protezione dei dati. Per questo motivo, i criteri sviluppati qui di seguito vanno, talvolta, al di là di una semplice spiegazione dell'interpretazione dei tre esempi di cui all'articolo 35, paragrafo 3, del regolamento generale sulla protezione dei dati.
Al fine di fornire un insieme più concreto di trattamenti che richiedono una valutazione d'impatto sulla protezione dei dati in virtù del loro rischio elevato intrinseco, tenendo conto degli elementi particolari di cui all'articolo 35, paragrafo 1 e all'articolo 35, paragrafo 3, lettere da a) a c), l'elenco da adottare a livello nazionale ai sensi dell'articolo 35, paragrafo 4, e dei considerando 71, 75 e 91, e di altri riferimenti del regolamento generale sulla protezione dei dati a trattamenti che *"possono presentare un rischio elevato"*[14], si devono considerare i seguenti nove criteri.

1) **Valutazione o assegnazione di un punteggio**, inclusiva di profilazione e previsione, in particolare in considerazione di *"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 dell'interessato*" (considerando 71 e 91). Esempi di ciò potrebbero includere: un ente finanziario che esamina i suoi clienti rispetto a una banca dati di riferimento in materia di crediti oppure rispetto a una banca dati in materia di lotta contro il riciclaggio e il finanziamento del terrorismo (AML/CTF) oppure contenente informazioni sulle frodi; oppure un'im-

12 Cfr. considerando 71: "*in particolare mediante l'analisi o la previsione di 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, al fine di creare o utilizzare profili personali".*

13 Cfr. considerando 75: *"se sono trattati dati personali che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, l'appartenenza sindacale, nonché dati genetici, dati relativi alla salute o i dati relativi alla vita sessuale o a condanne penali e a reati o alle relative misure di sicurezza" .*

14 Cfr. ad esempio i considerando 75, 76, 92 e 116.

presa di biotecnologie che offre test genetici direttamente ai consumatori per valutare e prevedere i rischi di malattia o per la salute; oppure un'impresa che crea profili comportamentali o per la commercializzazione basati sull'utilizzo del proprio sito web o sulla navigazione sullo stesso;

2) **processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente**: trattamento che mira a consentire l'adozione di decisioni in merito agli interessati che *"hanno effetti giuridici"* o che "*incidono in modo analogo significativamente su dette persone fisiche*" (articolo 35, paragrafo 3, lettera a)). Ad esempio, il trattamento può portare all'esclusione o alla discriminazione nei confronti delle persone. Il trattamento che non ha effetto o ha soltanto un effetto limitato sulle persone non risponde a questo criterio specifico. Ulteriori spiegazioni in merito a queste nozioni saranno fornite nelle linee guida sulla profilazione che saranno pubblicate prossimamente dal WP29;
3) **monitoraggio sistematico**: trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti o *"la sorveglianza sistematica su larga scala di una zona accessibile al pubblico"* (articolo 35, paragrafo 3, lettera c))[15]. Questo tipo di monitoraggio è un criterio in quanto i dati personali possono essere raccolti in circostanze nelle quali gli interessati possono non essere a conoscenza di chi sta raccogliendo i loro dati e di come li utilizzerà. Inoltre, può essere impossibile per le persone evitare di essere soggette a tale trattamento nel contesto di spazi pubblici (o accessibili al pubblico);
4) **dati sensibili o dati aventi carattere altamente personale**: questo criterio include categorie particolari di dati personali così come definite all'articolo 9 (ad esempio informazioni sulle opinioni politiche delle persone), nonché dati personali relativi a condanne penali o reati di cui all'articolo 10. Un esempio potrebbe essere quello di un ospedale generale che conserva le cartelle cliniche dei pazienti oppure quello di un investigatore privato che conserva i dettagli dei trasgressori. Al di là di queste disposizioni del regolamento generale sulla protezione dei dati, alcune categorie di dati possono essere considerate aumentare il possibile rischio per i diritti e le li-

15 L'aggettivo "sistematico" ha almeno uno dei seguenti significati a giudizio del WP29 (cfr. le "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243):
- che avviene per sistema;
- predeterminato, organizzato o metodico;
- che ha luogo nell'ambito di un progetto complessivo di raccolta di dati;
- svolto nell'ambito di una strategia.
Il termine *"zona accessibile al pubblico"*, a giudizio del WP29, indica qualsiasi luogo aperto a ciascun individuo della popolazione, come ad esempio una piazza, un centro commerciale, una strada, un mercato, una stazione ferroviaria o una biblioteca pubblica.

bertà delle persone fisiche. Tali dati personali sono considerati essere sensibili (nel senso in cui tale termine è comunemente compreso) perché sono legati ad attività a carattere personale o domestico (quali le comunicazioni elettroniche la cui riservatezza deve essere protetta) oppure perché influenzano l'esercizio di un diritto fondamentale (come ad esempio i dati relativi all'ubicazione, la cui raccolta mette in discussione la libertà di circolazione) oppure perché la violazione in relazione a tali dati implica chiaramente gravi ripercussioni sulla vita quotidiana dell'interessato (si pensi ad esempio a dati finanziari che potrebbero essere utilizzati per frodi relative ai pagamenti). A questo proposito, può essere rilevante il fatto che tali dati siano stati resi pubblici dall'interessato o da terzi. Il fatto che i dati personali siano di dominio pubblico può essere considerato un fattore da considerare nella valutazione qualora fosse previsto che i dati venissero utilizzati ulteriormente per determinate finalità. Questo criterio può includere anche dati quali documenti personali, messaggi di posta elettronica, diari, note ricavate da dispositivi elettronici di lettura dotati di funzionalità di annotazione, nonché informazioni molto personali contenute nelle applicazioni che registrano le attività quotidiane delle persone;

5) **trattamento di dati su larga scala**: il regolamento generale sulla protezione dei dati non definisce la nozione di "su larga scala", tuttavia fornisce un orientamento in merito al considerando 91. A ogni modo, il WP29 raccomanda di tenere conto, in particolare, dei fattori elencati nel prosieguo al fine di stabilire se un trattamento sia effettuato su larga scala[16]:
   a) il numero di soggetti interessati dal trattamento, in termini assoluti ovvero espressi in percentuale della popolazione di riferimento;
   b) il volume dei dati e/o le diverse tipologie di dati oggetto di trattamento;
   c) la durata, ovvero la persistenza, dell'attività di trattamento;
   d) la portata geografica dell'attività di trattamento;
6) **creazione di corrispondenze o combinazione di insiemi di dati**, ad esempio a partire da dati derivanti da due o più operazioni di trattamento svolte per finalità diverse e/o da titolari del trattamento diversi secondo una modalità che va oltre le ragionevoli aspettative dell'interessato[17];
7) **dati relativi a interessati vulnerabili** (considerando 75): il trattamento di questo tipo di dati è un criterio a motivo dell'aumento dello squilibrio di potere tra gli interessati e il titolare del trattamento, aspetto questo che fa sì che le persone possono non essere in grado di acconsentire od opporsi al trattamento dei loro dati o di

16 Cfr. "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

17 Cfr. spiegazione contenuta nel parere del WP29 sulla limitazione della finalità - 13/EN WP 203, pag. 24.

esercitare i propri diritti. Gli interessati vulnerabili possono includere i minori (i quali possono essere considerati non essere in grado di opporsi e acconsentire deliberatamente e consapevolmente al trattamento dei loro dati), i dipendenti, i segmenti più vulnerabili della popolazione che richiedono una protezione speciale (infermi di mente, richiedenti asilo o anziani, pazienti, ecc.) e, in ogni caso in cui sia possibile individuare uno squilibrio nella relazione tra la posizione dell'interessato e quella del titolare del trattamento;

8) **uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative**, quali la combinazione dell'uso dell'impronta digitale e del riconoscimento facciale per un miglior controllo degli accessi fisici, ecc. Il regolamento generale sulla protezione dei dati chiarisce (articolo 35, paragrafo 1 e considerando 89 e 91) che l'uso di una nuova tecnologia, definita *"in conformità con il grado di conoscenze tecnologiche raggiunto"* (considerando 91), può comportare la necessità di realizzare una valutazione d'impatto sulla protezione dei dati. Ciò è dovuto al fatto che il ricorso a tale tecnologia può comportare nuove forme di raccolta e di utilizzo dei dati, magari costituendo un rischio elevato per i diritti e le libertà delle persone. Infatti, le conseguenze personali e sociali dell'utilizzo di una nuova tecnologia potrebbero essere sconosciute. Una valutazione d'impatto sulla protezione dei dati aiuterà il titolare del trattamento a comprendere e trattare tali rischi. Ad esempio, alcune applicazioni di "Internet delle cose" potrebbero avere un impatto significativo sulla vita quotidiana e sulla vita privata delle persone e, di conseguenza, richiedono la realizzazione di una valutazione d'impatto sulla protezione dei dati;
9) quando il trattamento in sé ***"impedisce agli interessati di esercitare un diritto o di avvalersi di un servizio o di un contratto"*** (articolo 22 e considerando 91). Ciò include i trattamenti che mirano a consentire, modificare o rifiutare l'accesso degli interessati a un servizio oppure la stipula di un contratto. Un esempio di ciò è rappresentato dal caso in cui una banca esamina i suoi clienti rispetto a una banca dati di riferimento per il credito al fine di decidere se offrire loro un prestito o meno.

Nella maggior parte dei casi, un titolare del trattamento può considerare che un trattamento che soddisfi due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. In generale, il WP29 ritiene che maggiore è il numero di criteri soddisfatti dal trattamento, più è probabile che sia presente un rischio elevato per i diritti e le libertà degli interessati e, di conseguenza, che sia necessario realizzare una valutazione d'impatto sulla protezione dei dati, indipendentemente dalle misure che il titolare del trattamento ha previsto di adottare.

Tuttavia, in alcuni casi, **un titolare del trattamento può ritenere che un trattamento che soddisfa soltanto uno di questi criteri richieda una valutazione d'impatto sulla protezione dei dati.**

Gli esempi riportati di seguito illustrano come utilizzare i criteri per valutare se una particolare tipologia di trattamento richieda una valutazione d'impatto sulla protezione dei dati o meno.

Tabella 4

Esempi di trattamento	***Possibili criteri pertinenti***	***È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?***
Un ospedale che tratta i dati genetici e sanitari dei propri pazienti (sistema informativo ospedaliero).	› Dati sensibili o dati aventi carattere estremamente personale. › Dati riguardanti soggetti interessati vulnerabili. › Trattamento di dati su larga scala.	Sì
L'uso di un sistema di telecamere per monitorare il comportamento di guida sulle autostrade. Il titolare del trattamento prevede di utilizzare un sistema intelligente di analisi video per individuare le auto e riconoscere automaticamente le targhe.	› Monitoraggio sistematico. › Uso innovativo o applicazione di soluzioni tecnologiche od organizzative.	Sì
Un'azienda che monitora sistematicamente le attività dei suoi dipendenti, controllando anche la postazione di lavoro dei dipendenti, le loro attività in Internet, ecc.	› Monitoraggio sistematico. › Dati riguardanti soggetti interessati vulnerabili.	Sì
La raccolta di dati pubblici dei media sociali per la generazione di profili.	› Valutazione o assegnazione di un punteggio. › Trattamento di dati su larga scala. › Creazione di corrispondenze o combinazione di insiemi di dati. › Dati sensibili o dati aventi carattere estremamente personale.	Sì

Esempi di trattamento	*Possibili criteri pertinenti*	*È probabile che sia richiesta una valutazione d'impatto sulla protezione dei dati?*
Un'istituzione che crea una banca dati antifrode e di gestione del rating del credito a livello nazionale.	› Valutazione o assegnazione di un punteggio. › Processo decisionale automatizzato che ha effetto giuridico o incide in modo analogo significativamente. › Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto. › Dati sensibili o dati aventi carattere estremamente personale.	Sì
Conservazione per finalità di archiviazione di dati sensibili personali pseudonimizzati relativi a interessati vulnerabili coinvolti in progetti di ricerca o sperimentazioni cliniche.	› Dati sensibili. › Dati riguardanti soggetti interessati vulnerabili. › Impedisce agli interessati di esercitare un diritto o utilizzare un servizio o un contratto.	Sì
Un trattamento di "dati personali di pazienti o clienti da parte di un singolo medico, operatore sanitario o avvocato" (considerando 91).	› Dati sensibili o dati aventi carattere estremamente personale. › Dati riguardanti soggetti interessati vulnerabili.	No
Una rivista online che utilizza una lista di distribuzione per inviare una selezione quotidiana generica ai suoi abbonati.	› Trattamento di dati su larga scala.	No
Un sito web di commercio elettronico che visualizza annunci pubblicitari per parti di auto d'epoca che comporta una limitata profilazione basata sugli articoli visualizzati o acquistati sul proprio sito web.	› Valutazione o assegnazione di un punteggio.	No

Per contro, un trattamento può corrispondere ai casi di cui sopra ed essere comunque considerato dal titolare del trattamento un trattamento tale da non "presentare un rischio elevato". In tali casi il titolare del trattamento deve giustificare e documentare i motivi che lo hanno spinto a non effettuare una valutazione d'impatto sulla protezione dei dati, nonché includere/registrare i punti di vista del responsabile della protezione dei dati.

Inoltre, nel contesto del principio di responsabilizzazione, ogni titolare del trattamento deve tenere *"un registro delle attività di trattamento svolte sotto la propria responsabilità"* che includa, tra l'altro, le finalità del trattamento, una descrizione delle categorie di dati e di destinatari dei dati e *"ove possibile, una descrizione generale delle misure di*

sicurezza tecniche e organizzative di cui all'articolo 32, paragrafo 1" (articolo 30, paragrafo 1); inoltre, deve valutare la probabilità di un rischio elevato, anche qualora decida in ultima analisi di non realizzare una valutazione d'impatto sulla protezione dei dati.
Nota: le autorità di controllo sono tenute a stabilire, rendere pubblico e comunicare al comitato europeo per la protezione dei dati un elenco delle tipologie di trattamento che richiedono una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 4)[18]. I criteri di cui sopra possono aiutare le autorità di controllo a redigere un tale elenco, aggiungendo contenuti specifici nel corso del tempo, se applicabile. Ad esempio, anche il trattamento di qualsiasi tipo di dati biometrici o di dati di minori potrebbe essere considerato pertinente per lo sviluppo di un elenco ai sensi dell'articolo 35, paragrafo 4.

b) Quando non è richiesta una valutazione d'impatto sulla protezione dei dati? Quando il trattamento non è tale da *"presentare un rischio elevato"* oppure qualora esista una valutazione d'impatto sulla protezione dei dati analoga, o qualora il trattamento sia stato autorizzato prima del maggio 2018 oppure abbia una base giuridica o sia incluso nell'elenco delle tipologie di trattamento per le quali non è richiesta una valutazione d'impatto sulla protezione dei dati.

Il WP29 ritiene che una valutazione d'impatto sulla protezione dei dati non sia richiesta nei seguenti casi:

- **quando il trattamento non è tale da *"presentare un rischio elevato per i diritti e le libertà delle persone fisiche"*** (articolo 35, paragrafo 1);
- **quando la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono molto simili a un trattamento per il quale è stata svolta una valutazione d'impatto sulla protezione dei dati**. In tali casi, si possono utilizzare i risultati della valutazione d'impatto sulla protezione dei dati per un trattamento analogo (articolo 35, paragrafo 1[19]);
- quando le tipologie di trattamento sono state verificate da un'autorità di controllo prima del maggio 2018 in condizioni specifiche che non sono cambiate[20] (cfr. III.C);

---

18 In tale contesto, *"l'autorità di controllo competente applica il meccanismo di coerenza di cui all'articolo 63 se tali elenchi comprendono attività di trattamento finalizzate all'offerta di beni o servizi a interessati o al monitoraggio del loro comportamento in più Stati membri, o attività di trattamento che possono incidere significativamente sulla libera circolazione dei dati personali all'interno dell'Unione"* (articolo 35, paragrafo 6).

19 *"Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".*

20 *"Le decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate"* (considerando 171).

- **qualora un trattamento**, effettuato a norma dell'articolo 6, paragrafo 1, lettere c) o e), trovi **una base giuridica** nel diritto dell'Unione o nel diritto dello Stato membro, tale diritto disciplini il trattamento specifico o **sia già stata effettuata una valutazione d'impatto sulla protezione dei dati** nel contesto dell'adozione di tale base giuridica (articolo 35, paragrafo 10)[21], a meno che uno Stato membro non abbia dichiarato che è necessario effettuare tale valutazione prima di procedere alle attività di trattamento;
- **qualora il trattamento sia incluso nell'elenco facoltativo (stabilito dall'autorità di controllo) delle tipologie di trattamento** per le quali non è richiesta alcuna valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 5). Tale elenco può contenere attività di trattamento conformi alle condizioni specificate da detta autorità, in particolare attraverso linee guida, decisioni o autorizzazioni specifiche, norme di conformità, ecc. (ad esempio in Francia, autorizzazioni, esenzioni, norme semplificate, pacchetti di conformità, ecc.). In tali casi e a condizione che venga eseguita una nuova valutazione da parte dell'autorità di controllo competente, non è richiesta una valutazione d'impatto sulla protezione dei dati, ma soltanto se il trattamento rientra a tutti gli effetti nel campo di applicazione della procedura pertinente menzionata nell'elenco e continua a rispettare pienamente tutti i requisiti pertinenti del regolamento generale sulla protezione dei dati.

C. Quale regola si applica ai trattamenti già esistenti? In talune circostanze sono richieste valutazioni d'impatto sulla protezione dei dati.

L'obbligo di svolgere una valutazione d'impatto sulla protezione dei dati si applica alle operazioni di trattamento esistenti che possono presentare un rischio elevato per i diritti e le libertà delle persone fisiche e per le quali vi è stata una variazione dei rischi, tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento.

Non è necessaria una valutazione d'impatto sulla protezione dei dati per i trattamenti che sono stati verificati da un'autorità di controllo o dal responsabile della protezione

21 Quando viene svolta una valutazione d'impatto sulla protezione dei dati in fase di elaborazione della legislazione che fornisce una base giuridica per un trattamento, è probabile che la stessa richieda un riesame prima dell'avvio delle attività, in quanto la legislazione adottata può differire dalla proposta ed influenzare quindi questioni in materia di vita privata e protezione dei dati. Inoltre, potrebbero non esserci sufficienti dettagli tecnici per quanto riguarda il trattamento effettivo al momento dell'adozione della legislazione, anche qualora detto trattamento sia accompagnato da una valutazione d'impatto sulla protezione dei dati. In questi casi, può comunque essere necessario eseguire una valutazione d'impatto sulla protezione dei dati specifica prima di realizzare le attività di trattamento effettive.

dei dati, a norma dell'articolo 20 della direttiva 95/46/CE e che vengono eseguiti in maniera tale da fare sì che non si sia registrata alcuna variazione rispetto alla verifica precedente. In effetti, *"[l]e decisioni della Commissione e le autorizzazioni delle autorità di controllo basate sulla direttiva 95/46/CE rimangono in vigore fino a quando non vengono modificate, sostituite o abrogate"* (considerando 171).

Al contrario, ciò significa che qualsiasi trattamento di dati le cui condizioni di attuazione (ambito di applicazione, finalità, dati personali raccolti, identità dei titolari del trattamento o dei destinatari, periodo di conservazione dei dati, misure tecniche e organizzative, ecc.) sono mutate rispetto alla prima verifica effettuata dall'autorità di controllo o dal responsabile della protezione dei dati e che possono presentare un rischio elevato devono essere soggette a una valutazione d'impatto sulla protezione dei dati.

Inoltre, potrebbe essere richiesta una valutazione d'impatto sulla protezione dei dati in seguito a una variazione dei rischi derivante dalle operazioni di trattamento[22], ad esempio perché è entrata in uso una nuova tecnologia o perché i dati personali vengono utilizzati per una finalità diversa. Le operazioni di trattamento dei dati possono evolversi rapidamente e potrebbero emergere nuove vulnerabilità. Di conseguenza, va osservato che la revisione di una valutazione d'impatto sulla protezione dei dati non è utile soltanto ai fini di un miglioramento continuo, bensì anche fondamentale per mantenere il livello di protezione dei dati in un ambiente che muta nel corso del tempo. Una valutazione d'impatto sulla protezione dei dati potrebbe rendersi necessaria anche perché il contesto organizzativo o sociale per l'attività di trattamento è mutato, ad esempio perché gli effetti di determinate decisioni automatizzate sono diventati più significativi oppure perché nuove categorie di interessati sono diventati vulnerabili alla discriminazione. Ciascuno di questi esempi potrebbe costituire un aspetto che porta a una variazione del rischio derivante dall'attività di trattamento interessata.

Al contrario, talune modifiche potrebbero anche ridurre il rischio. Ad esempio, un trattamento potrebbe evolvere in modo tale da fare sì che le decisioni non siano più automatizzate oppure si pensi al caso in cui un'attività di monitoraggio non viene più eseguita in maniera sistematica. In questo caso, il riesame dell'analisi dei rischi può mostrare che non è più necessario eseguire una valutazione d'impatto sulla protezione dei dati.

Secondo le buone prassi, **una valutazione d'impatto sulla protezione dei dati va riesaminata continuamente e rivalutata con regolarità**. Di conseguenza, anche se una valutazione d'impatto sulla protezione dei dati non è richiesta il 25 maggio 2018, al momento

22 In termini di contesto, i dati raccolti, le finalità, le funzionalità, i dati personali trattati, i destinatari, le combinazioni di dati, i rischi (risorse di sostegno, fonti di rischio, impatti potenziali , minacce, ecc.), le misure di sicurezza e i trasferimenti internazionali.

opportuno, il titolare del trattamento sarà tenuto a svolgere tale valutazione nel contesto dei suoi obblighi generali di responsabilizzazione.

D. Come va svolta una valutazione d'impatto sulla protezione dei dati?

a) In quale momento va effettuata una valutazione d'impatto sulla protezione dei dati? Prima del trattamento.

La valutazione d'impatto sulla protezione dei dati va effettuata *"prima del trattamento"* (articolo 35, paragrafi 1 e 10, considerando 90 e 93)[23]. Ciò è coerente con i principi di protezione dei dati fin dalla progettazione e di protezione per impostazione predefinita (articolo 25 e considerando 78). La valutazione d'impatto sulla protezione dei dati va considerata come uno strumento atto a contribuire al processo decisionale in materia di trattamento.

La valutazione d'impatto sulla protezione dei dati va avviata il prima possibile nella fase di progettazione del trattamento anche se alcune delle operazioni di trattamento non sono ancora note. L'aggiornamento della valutazione d'impatto sulla protezione dei dati nel corso dell'intero ciclo di vita del progetto garantirà che la protezione dei dati e della vita privata sia presa in considerazione e favorisca la creazione di soluzioni che promuovono la conformità. Può essere altresì necessario ripetere singole fasi della valutazione man mano che il processo di sviluppo evolve, dato che la selezione di determinate misure tecniche od organizzative può influenzare la gravità o la probabilità dei rischi posti dal trattamento.

Il fatto che possa rendersi necessario aggiornare la valutazione d'impatto sulla protezione dei dati dopo l'effettivo avvio del trattamento non costituisce un motivo valido per rinviare o non svolgere una valutazione d'impatto sulla protezione dei dati. La valutazione d'impatto sulla protezione dei dati è un processo continuo, soprattutto quando un trattamento è dinamico ed è soggetto a variazioni continue.

Realizzare una valutazione d'impatto sulla protezione dei dati è un processo continuo, non un esercizio *una tantum*.

23 Fatto salvo il caso in cui si tratti di un trattamento già in essere che è stato preventivamente verificato dall'autorità di controllo, nel qual caso la valutazione d'impatto sulla protezione dei dati deve essere eseguita prima di attuare modifiche significative.

b) Chi è obbligato a effettuare la valutazione d'impatto sulla protezione dei dati? Il titolare del trattamento, con il responsabile della protezione dei dati e i responsabili del trattamento.

Al titolare del trattamento spetta assicurare che la valutazione d'impatto sulla protezione dei dati sia eseguita (articolo 35, paragrafo 2). La valutazione d'impatto sulla protezione dei dati può essere effettuata da qualcun altro, all'interno o all'esterno dell'organizzazione, tuttavia al titolare del trattamento spetta la responsabilità ultima per tale compito.

Inoltre il titolare del trattamento deve consultarsi con il responsabile della protezione dei dati (RPD), qualora ne sia designato uno (articolo 35, paragrafo 2) e il parere ricevuto, così come le decisioni prese dal titolare del trattamento, debbano essere documentate all'interno della valutazione d'impatto sulla protezione dei dati. Il responsabile della protezione dei dati deve altresì sorvegliare lo svolgimento della valutazione d'impatto sulla protezione dei dati (articolo 39, paragrafo 1, lettera c)). Ulteriori orientamenti in merito sono forniti nelle "Linee guida sui responsabili della protezione dei dati (RPD)" del WP29 - 16/EN WP 243.

Qualora il trattamento venga eseguito in toto o in parte da un responsabile del trattamento dei dati, **quest'ultimo deve assistere il titolare del trattamento nell'esecuzione della valutazione d'impatto sulla protezione dei dati** e fornire tutte le informazioni necessarie (conformemente all'articolo 28, paragrafo 3, lettera f)).

Il titolare del trattamento deve *"raccoglie[re] le opinioni degli interessati o dei loro rappresentanti"* (articolo 35, paragrafo 9), *"se del caso"*. Il WP29 ritiene che:

- tali opinioni possono essere raccolte attraverso una varietà di mezzi, a seconda del contesto (ad esempio uno studio generico relativo alla finalità e ai mezzi del trattamento, una domanda posta ai rappresentanti del personale oppure indagini abituali inviate ai futuri clienti del titolare del trattamento), assicurando che il titolare del trattamento disponga di una base giuridica valida per il trattamento di qualsiasi dato personale interessato nel raccogliere dette opinioni; sebbene sia opportuno osservare che il consenso al trattamento non è ovviamente un modo per raccogliere le opinioni degli interessati;
- qualora la decisione finale del titolare del trattamento si discosti dalle opinioni degli interessati, le sue motivazioni a sostegno del procedere o meno vanno documentate;
- il titolare del trattamento deve altresì documentare la sua giustificazione per la mancata raccolta delle opinioni degli interessati, qualora decida che ciò non sia

appropriato, ad esempio qualora ciò comporterebbe la riservatezza dei piani economici dell'impresa o sarebbe sproporzionato o impraticabile.

Infine, è buona prassi definire e documentare altri ruoli e responsabilità specifici, a seconda delle politiche, dei processi e delle norme interni, ad esempio:

- qualora specifiche unità aziendali propongano di svolgere una valutazione d'impatto sulla protezione dei dati, tali unità dovrebbero poi fornire contributi alla valutazione d'impatto sulla protezione dei dati ed essere coinvolte nel processo di convalida di detta valutazione;
- se del caso, si raccomanda di consultare esperti indipendenti che esercitano professioni diverse[24] (avvocati, esperti informatici, esperti di sicurezza, sociologi, esperti di etica, ecc.).
- i ruoli e le responsabilità dei responsabili del trattamento devono essere definiti contrattualmente; e la valutazione d'impatto sulla protezione dei dati deve essere svolta con l'assistenza di un responsabile del trattamento, tenendo conto della natura del trattamento e delle informazioni a disposizione di detto responsabile del trattamento (articolo 28, paragrafo 3, lettera f));
- il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, così come il responsabile della protezione dei dati, potrebbero suggerire al titolare del trattamento di realizzare una valutazione d'impatto sulla protezione dei dati in merito a una specifica operazione di trattamento e dovrebbero assistere le parti interessate in relazione alla metodologia, contribuire alla valutazione della qualità della valutazione dei rischi e del grado di accettabilità del rischio residuo, nonché allo sviluppo di conoscenze specifiche in merito al contesto del titolare del trattamento;
- il responsabile capo della sicurezza dei sistemi d'informazione (CISO), se nominato, e/o il dipartimento dedicato alle tecnologie dell'informazione, dovrebbero fornire assistenza al titolare del trattamento, nonché potrebbero proporre lo svolgimento di una valutazione d'impatto sulla protezione dei dati su un'operazione specifica di trattamento, a seconda delle esigenze operative e legate alla sicurezza.

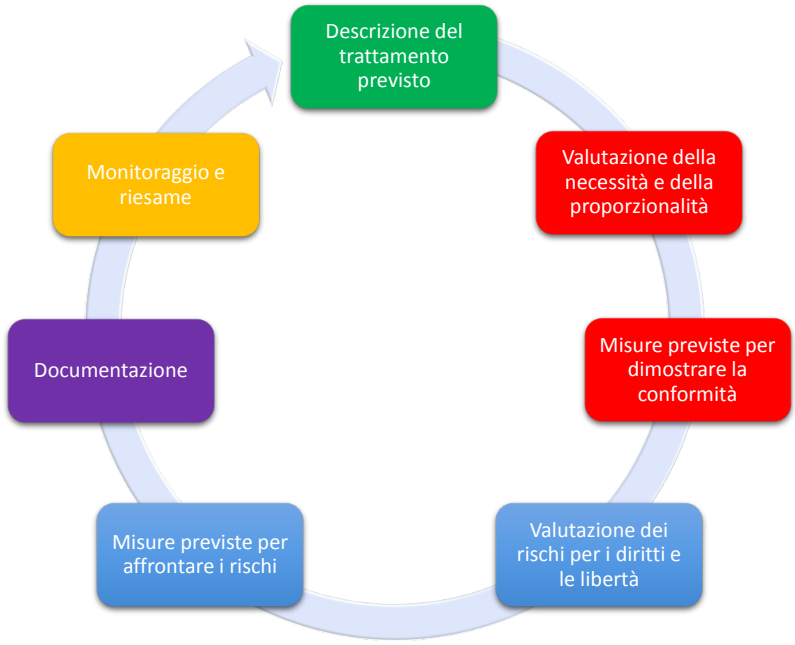
24 "*Recommendations for a privacy impact assessment framework for the European Union, Deliverable D3*": http://www.piafproject.eu/ref/PIAF_D3_final.pdf.

c) Qual è la metodologia da seguire per svolgere una valutazione d'impatto sulla protezione dei dati? Vi sono metodologie diverse, ma criteri comuni.

Il regolamento generale sulla protezione dei dati definisce le caratteristiche minime di una valutazione d'impatto sulla protezione dei dati (articolo 35, paragrafo 7, e considerando 84 e 90):

- *"una descrizione dei trattamenti previsti e delle finalità del trattamento";*
- *"una valutazione della necessità e proporzionalità dei trattamenti";*
- *"una valutazione dei rischi per i diritti e le libertà degli interessati";*
- *"le misure previste per:*
  - *"affrontare i rischi";*
  - *"dimostrare la conformità al presente regolamento".*

La figura che segue illustra il processo iterativo generico per lo svolgimento di una valutazione d'impatto sulla protezione dei dati[25]:



25 Va sottolineato che il processo descritto in questa sede è iterativo: in pratica, è probabile che ciascuna delle fasi venga riesaminata più volte prima che sia possibile completare la valutazione d'impatto sulla protezione dei dati.

Nel valutare l'impatto di un trattamento va tenuto conto (articolo 35, paragrafo 8) del rispetto di un codice di condotta (articolo 40). Ciò può essere utile per dimostrare che sono state scelte o messe in atto misure adeguate, a condizione che il codice di condotta sia adeguato all'operazione di trattamento interessata. Devono essere presi in considerazione anche certificazioni, sigilli e marchi al fine di dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati dei trattamenti effettuati dai titolari del trattamento e dai responsabili del trattamento (articolo 42), nonché rispetto alle norme vincolanti d'impresa.

Tutti i requisiti pertinenti stabiliti nel regolamento generale sulla protezione dei dati offrono un quadro ampio e generico per la progettazione e lo svolgimento di una valutazione d'impatto sulla protezione dei dati. L'attuazione pratica di una valutazione d'impatto sulla protezione dei dati dipenderà dai requisiti stabiliti nel regolamento generale sulla protezione dei dati che possono essere integrati da orientamenti pratici più dettagliati. L'attuazione della valutazione d'impatto sulla protezione dei dati è quindi modulabile. Ciò significa che anche un titolare del trattamento di piccole dimensioni può progettare e attuare una valutazione d'impatto sulla protezione dei dati adatta ai propri trattamenti.

Il considerando 90 del regolamento generale sulla protezione dei dati delinea una serie di elementi costituivi della valutazione d'impatto sulla protezione dei dati che si sovrappone a elementi ben definiti della gestione del rischio (ad esempio norma ISO 31000)[26]. In termini di gestione dei rischi, una valutazione d'impatto sulla protezione dei dati mira a "gestire i rischi" per i diritti e le libertà delle persone fisiche, utilizzando i seguenti processi:

- stabilendo il contesto: *"tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e delle fonti di rischio"*;
- valutando i rischi: *"valutare la particolare probabilità e gravità del rischio"*;
- trattando i rischi: *"atten[uando] tale rischio"* e *"assicurando la protezione dei dati personali"*, e *"dimostrando la conformità al presente regolamento"*.

Nota: la valutazione d'impatto sulla protezione dei dati svolta ai sensi del regolamento generale sulla protezione dei dati è uno strumento per gestire i rischi per i diritti degli interessati, di conseguenza, adotta la loro prospettiva, come avviene in taluni settori

26 Processi di gestione del rischio: comunicazione e consultazione, definizione del contesto, valutazione dei rischi, trattamento dei rischi, monitoraggio e riesame (cfr. termini e definizioni e l'indice nell'anteprima della norma ISO 31000 (in inglese): https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en).

(ad esempio, la sicurezza sociale). Al contrario, la gestione del rischio in altri settori (ad esempio in quello della sicurezza delle informazioni) è incentrata sull'organizzazione.
Il regolamento generale sulla protezione dei dati offre ai titolari del trattamento la flessibilità di stabilire la struttura e la forma precise della valutazione d'impatto sulla protezione dei dati in maniera da consentire che la stessa si adatti alle pratiche di lavoro esistenti. Esistono diversi processi stabiliti all'interno dell'UE e nel mondo che tengono conto degli elementi costitutivi descritti nel considerando 90. Tuttavia, indipendentemente dalla sua forma, una valutazione d'impatto sulla protezione dei dati deve essere una vera e propria valutazione dei rischi che consenta ai titolari del trattamento di adottare misure per affrontarli.
Si potrebbe ricorrere a metodologie diverse (cfr. allegato 1 per esempi di metodologie di valutazione dell'impatto sulla vita privata e sulla protezione dei dati) per contribuire all'attuazione dei requisiti essenziali stabiliti nel regolamento generale sulla protezione dei dati. Al fine di consentire l'esistenza di tali approcci distinti, permettendo comunque ai titolari del trattamento di rispettare il regolamento generale sulla protezione dei dati, sono stati individuati dei criteri comuni (cfr. allegato 2). Tali criteri chiariscono i requisiti essenziali del regolamento, ma offrono un campo di applicazione sufficiente da consentire la coesistenza di forme diverse di attuazione. Detti criteri possono essere utilizzati per dimostrare che una particolare metodologia di valutazione d'impatto sulla protezione dei dati soddisfa i parametri imposti dal regolamento generale sulla protezione dei dati. **Spetta al titolare del trattamento scegliere una metodologia che, comunque, deve essere conforme ai criteri di cui all'allegato 2.**
Il WP29 incoraggia lo sviluppo di quadri di valutazione d'impatto sulla protezione dei dati specifici dei vari settori. Ciò è dovuto al fatto che essi possono attingere a conoscenze specifiche settoriali, aspetto questo che fa sì che la valutazione d'impatto sulla protezione dei dati possa affrontare le specificità di un particolare tipo di trattamento (ad esempio tipi particolari di dati, risorse aziendali, impatti potenziali, minacce, misure). Ciò significa che la valutazione d'impatto sulla protezione dei dati può affrontare le problematiche che sorgono in un settore economico specifico oppure quando si utilizzano tecnologie particolari o si eseguono tipologie particolari di trattamento.
Infine, se necessario, "*il titolare del trattamento procede a un riesame per valutare se il trattamento dei dati personali sia effettuato conformemente alla valutazione d'impatto sulla protezione dei dati almeno quando insorgono variazioni del rischio rappresentato dalle attività relative al trattamento*" (articolo 35, paragrafo 11[27]).

27 L'articolo 35, paragrafo 10, esclude esplicitamente soltanto l'applicazione dell'articolo 35, paragrafi da 1 a 7.

d) Esiste l'obbligo di pubblicare la valutazione d'impatto sulla protezione dei dati? No, tuttavia pubblicarne una sintesi potrebbe favorire la fiducia e la valutazione d'impatto sulla protezione dei dati completa deve essere comunicata all'autorità di controllo in caso di consultazione preventiva o su richiesta da parte delle autorità competenti per la protezione dei dati personali.

La pubblicazione di una valutazione d'impatto sulla protezione dei dati non è un requisito giuridico sancito dal regolamento generale sulla protezione dei dati, è una decisione del titolari del trattamento procedere in tal senso. Tuttavia, i titolari del trattamento dovrebbero prendere in considerazione la pubblicazione di almeno alcune parti, ad esempio di una sintesi o della conclusione della loro valutazione d'impatto sulla protezione dei dati.

Lo scopo di un tale processo sarebbe quello di contribuire a stimolare la fiducia nei confronti dei trattamenti effettuati dal titolare del trattamento, nonché di dimostrare la responsabilizzazione e la trasparenza. Costituisce una prassi particolarmente buona pubblicare una valutazione d'impatto sulla protezione dei dati nel caso in cui individui della popolazione siano influenzati dal trattamento interessato. Nello specifico, ciò potrebbe essere il caso in cui un'autorità pubblica realizza una valutazione d'impatto sulla protezione dei dati.

La valutazione d'impatto sulla protezione dei dati pubblicata non deve necessariamente contenere l'intera valutazione, soprattutto qualora essa possa presentare informazioni specifiche relative ai rischi per la sicurezza per il titolare del trattamento o divulgare segreti commerciali o informazioni commerciali sensibili. In queste circostanze, la versione pubblicata potrebbe consistere soltanto in una sintesi delle principali risultanze della valutazione d'impatto sulla protezione dei dati o addirittura soltanto in una dichiarazione nella quale si afferma che la valutazione d'impatto sulla protezione dei dati è stata condotta.

Inoltre, laddove una valutazione d'impatto sulla protezione dei dati riveli la presenza di rischi residui elevati, il titolare del trattamento sarà tenuto a richiedere la consultazione preventiva dell'autorità di controllo in relazione al trattamento (articolo 36, paragrafo 1). In tale contesto, la valutazione d'impatto sulla protezione dei dati deve essere fornita completa (articolo 36, paragrafo 3, lettera e)).

L'autorità di controllo può fornire il proprio parere[28] e procurerà di non compromettere segreti commerciali né divulgare vulnerabilità di sicurezza, in conformità con i principi applicabili in ciascuno Stato membro in materia di accesso del pubblico a documenti ufficiali.

28 La formulazione di un parere scritto a favore del titolare del trattamento è necessaria soltanto quando l'autorità di controllo ritiene che il trattamento previsto non sia conforme al regolamento a norma dell'articolo 36, paragrafo 2.

E. Quando è necessario consultare l'autorità di controllo? Quando i rischi residui sono elevati.

Come spiegato in precedenza:

- è necessario realizzare una valutazione d'impatto sulla protezione dei dati quando il trattamento *"può presentare un rischio elevato per i diritti e le libertà delle persone fisiche"* (articolo 35, paragrafo 1; cfr. III.B.a). A titolo di esempio, il trattamento di dati sanitari su larga scala è considerato un trattamento tale da presentare un rischio elevato e richiede la realizzazione di una valutazione d'impatto sulla protezione dei dati;
- di conseguenza, spetta al titolare del trattamento valutare i rischi per i diritti e le libertà degli interessati e individuale le misure[29] previste per attenuare tali rischi a un livello accettabile e per dimostrare la conformità rispetto al regolamento generale sulla protezione dei dati (articolo 35, paragrafo 7; cfr. III.C.c). un esempio, in caso di conservazione di dati personali su computer portatili, potrebbe essere l'utilizzo di adeguate misure di sicurezza tecniche e organizzative (crittografia efficace completa del disco, gestione di chiavi robuste, opportuno controllo degli accessi, backup protetti, ecc.) oltre al ricorso a politiche esistenti (avviso, consenso, diritto di accesso, diritto di opposizione, ecc.).

Nell'esempio sopra riportato relativo ai computer portatili, qualora i rischi siano stati considerati sufficientemente attenuati dal titolare del trattamento e in seguito alla lettura dell'articolo 36, paragrafo 1 e dei considerando 84 e 94, il trattamento può procedere senza la consultazione dell'autorità di controllo. È nei casi in cui il titolare del trattamento non riesca a trattare in maniera sufficiente i rischi individuati (ossia i rischi residui rimangono elevati) che questi deve consultare l'autorità di controllo.
Un esempio di un rischio residuo elevato inaccettabile include casi in cui gli interessati possano subire conseguenze significative, o addirittura irreversibili, che non possono superare (ad esempio: accesso illegittimo a dati che comportano una minaccia per la vita degli interessati, un loro licenziamento, un rischio finanziario) e/o quando appare evidente che il rischio si verificherà (ad esempio: poiché non si è in grado di ridurre il numero di persone che accedono ai dati a causa delle loro modalità di condivisione, utilizzo o distribuzione o quando non si può porre rimedio a una vulnerabilità ben nota).

29 Tra le quali si annoverano la considerazione degli orientamenti esistenti formulati dal comitato europeo per la protezione dei dati e dalle autorità di controllo, nonché dello stato dell'arte e dei costi di attuazione, come previsto dall'articolo 35, paragrafo 1.

Ogniqualvolta il titolare del trattamento non è in grado di trovare misure sufficienti per ridurre i rischi a un livello accettabile (ossia i rischi residui restano comunque elevati) è necessario consultare l'autorità di controllo[30].

Inoltre, il titolare del trattamento dovrà consultare l'autorità di vigilanza qualora il diritto dello Stato membro in questione prescriva che i titolari del trattamento consultino l'autorità di controllo e/o ne ottengano l'autorizzazione preliminare, in relazione al trattamento da parte di un titolare del trattamento per l'esecuzione, da parte di questi, di un compito di interesse pubblico, tra cui il trattamento con riguardo alla protezione sociale e alla sanità pubblica (articolo 36, paragrafo 5).

Occorre tuttavia sottolineare che, indipendentemente dal fatto che la consultazione dell'autorità di controllo sia richiesta o meno in base al livello di rischio residuo, sussistono comunque gli obblighi di conservare una registrazione della valutazione d'impatto sulla protezione dei dati e di aggiornamento di detta valutazione al momento opportuno.

IV. Conclusioni e raccomandazioni

Le valutazioni d'impatto sulla protezione dei dati sono uno strumento utile di cui dispongono i titolari del trattamento per attuare sistemi di trattamento dei dati conformi al regolamento generale sulla protezione dei dati e possono essere obbligatorie per talune tipologie di trattamenti. Hanno natura modulabile e possono assumere forme diverse, tuttavia il regolamento generale sulla protezione dei dati stabilisce i requisiti essenziali di una valutazione d'impatto sulla protezione dei dati efficace. I titolari del trattamento dovrebbero considerare la realizzazione di una valutazione d'impatto sulla protezione dei dati come un'attività utile e positiva che contribuisce alla conformità giuridica.

L'articolo 24, paragrafo 1, definisce la responsabilità fondamentale del titolare del trattamento in termini di rispetto del regolamento generale sulla protezione dei dati: *"Tenuto conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, nonché dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche, il titolare del trattamento mette in atto misure tecniche e organizzative adeguate per garantire, ed essere in grado di dimostrare, che il trattamento è effettuato conformemente al presente regolamento. Dette misure sono riesaminate e aggiornate qualora necessario".*

30 Nota: *"la pseudonimizzazione e la cifratura dei dati personali"* (così come la minimizzazione dei dati, meccanismi di controllo, ecc.) non sono necessariamente misure appropriate. Sono soltanto esempi. Le misure adeguate dipendono dal contesto e dai rischi, aspetti specifici dei trattamenti effettuati.

La valutazione d'impatto sulla protezione dei dati è un aspetto fondamentale del rispetto del regolamento laddove si preveda di svolgere o si stia svolgendo un trattamento di dati soggetto a rischio elevato. Ciò significa che i titolari del trattamento dovrebbero utilizzare i criteri stabiliti nel presente documento per stabilire se devono realizzare una valutazione d'impatto sulla protezione dei dati o meno. La politica interna dei titolari del trattamento potrebbe estendere questo elenco andando oltre i requisiti giuridici sanciti dal regolamento generale sulla protezione dei dati. Ciò dovrebbe suscitare un maggior senso di fiducia e riservatezza negli interessati e in altri titolari del trattamento.
Qualora si preveda di effettuare un trattamento che possa presentare un rischio elevato, il titolare del trattamento deve:

- scegliere una metodologia per la valutazione d'impatto sulla protezione dei dati (esempi riportati nell'allegato 1) che soddisfi i criteri di cui all'allegato 2, oppure specificare ed attuare un processo sistematico di valutazione d'impatto sulla protezione dei dati che:
  - sia conforme ai criteri di cui all'allegato 2;
  - sia integrata nei processi in materia di progettazione, sviluppo, cambiamento, rischio e riesame operativo in conformità con i processi, il contesto e la cultura interni;
  - coinvolga le parti interessate appropriate e definisca chiaramente le loro responsabilità (titolare del trattamento, responsabile della protezione dei dati, interessati o loro rappresentanti, imprese, servizi tecnici, responsabili del trattamento, responsabile della sicurezza dei sistemi d'informazione, ecc.);
- fornire la relazione relativa alla valutazione d'impatto sulla protezione dei dati all'autorità di controllo, laddove gli venga richiesto di procedere in tal senso;
- consultare l'autorità di controllo, qualora il titolare del trattamento non sia riuscito a determinare misure sufficienti per attenuare i rischi elevati;
- riesaminare periodicamente la valutazione d'impatto sulla protezione dei dati e il trattamento che essa valuta, almeno quando si registra una variazione del rischio posto dal trattamento;
- documentare le decisioni prese.

Allegato 1 - Esempi di quadri UE esistenti di valutazione d'impatto sulla protezione dei dati

Il regolamento generale sulla protezione dei dati non specifica quale processo di valutazione d'impatto sulla protezione dei dati debba essere seguito, ma consente piuttosto ai titolari del trattamento di introdurre un quadro che integri le loro pratiche di lavoro esistenti, purché tenga conto degli elementi costitutivi di cui all'articolo 35, paragrafo 7. Tale quadro può essere personalizzato per lo specifico titolare del trattamento oppure essere comune a un determinato settore. I quadri precedentemente pubblicati sviluppati dalle autorità di protezione dei dati dell'UE e i quadri specifici di settore dell'UE includono (elenco non esaustivo):
esempi di quadri generici dell'UE:

- DE: modello per la protezione dei dati standard, V.1.0 - versione di prova, 2016[31]. https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf;
- ES: *Guía para una Evaluación de Impacto en la Protección de Datos Personales (EIPD)*, Agencia española de protección de datos (AGPD), 2014. https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf;
- FR: *Privacy Impact Assessment (PIA)*, Commission nationale de l'informatique et des libertés (CNIL), 2015. https://www.cnil.fr/fr/node/15798;
- UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014. https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf;

esempi di quadri UE specifici di settore:

- *Privacy and Data Protection Impact Assessment Framework for RFID Applications* [Quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID][32]. http://ec.europa.eu/justice/data-pro-

31 Approvato all'unanimità e affermativamente (con l'astensione della Baviera) dalla 92ª conferenza delle autorità indipendenti per la protezione dei dati del *Bund* e dei *Länder* di Kühlungsborn tenutasi il 9 e 10 novembre 2016.

32 Cfr. anche:

- Raccomandazione della Commissione, del 12 maggio 2009, sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza. http://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32009H0387&from=IT;

tection/article-29/documentation/opinion-recommendation/files/2011/wp180_annex_en.pdf;

- *Data Protection Impact Assessment Template for Smart Grid and Smart Metering systems* [Modello per la valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti][33] http://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf.
- Anche una norma internazionale fornirà orientamenti in merito alle metodologie utilizzate per la realizzazione di una valutazione d'impatto sulla protezione dei dati (ISO/IEC 29134)[34].

Allegato 2 - Criteri per una valutazione d'impatto sulla protezione dei dati accettabile

Il WP29 propone i seguenti criteri che i titolari del trattamento possono utilizzare per stabilire se sia richiesta una valutazione d'impatto sulla protezione dei dati o meno oppure se una metodologia per lo svolgimento di una tale valutazione sia sufficientemente completa per garantire il rispetto del regolamento generale sulla protezione dei dati:

- ☐ **una descrizione sistematica del trattamento è fornita** (articolo 35, paragrafo 7, lettera a)):
  - ☐ la natura, l'ambito di applicazione, il contesto e le finalità del trattamento sono presi in considerazione (considerando 90);
  - ☐ vengono registrati i dati personali, i destinatari e il periodo di conservazione dei dati personali;
  - ☐ viene fornita una descrizione funzionale del trattamento;
  - ☐ sono individuate le risorse sulle quali si basano i dati personali (hardware, software, reti, persone, canali cartacei o di trasmissione cartacea);

• Parere 9/2011 sulla proposta rivista dell'industria relativa a un quadro per la realizzazione di valutazioni di impatto sulla protezione della vita privata e dei dati per le applicazioni RFID. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp180_it.pdf.

33 Cfr. anche il "Parere 07/2013 concernente il modello di valutazione d'impatto sulla protezione dei dati per la rete intelligente e i sistemi di misurazione intelligenti ("modello di valutazione d'impatto sulla protezione dei dati") elaborato dal gruppo di esperti n. 2 della task force della Commissione per le reti intelligenti. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp209_it.pdf.

34 ISO/IEC 29134 (progetto), *Information technology – Security techniques – Privacy impact assessment – Guidelines* (in inglese), Organizzazione internazionale per la normazione (ISO).

- ☐ si tiene conto del rispetto dei codici di condotta approvati (articolo 35, paragrafo 8);

☐ **la necessità e la proporzionalità sono valutate** (articolo 35, paragrafo 7, lettera b)):

- ☐ sono state determinate le misure previste per garantire il rispetto del regolamento (articolo 35, paragrafo 7, lettera d) e considerando 90):
  - ☐ misure che contribuiscono alla proporzionalità e alla necessità del trattamento sulla base di:
    - ☐ finalità determinate, esplicite e legittime (articolo 5, paragrafo 1, lettera b));
    - ☐ liceità del trattamento (articolo 6);
    - ☐ dati personali adeguati, pertinenti e limitati a quanto necessario (articolo 5, paragrafo 1, lettera c));
    - ☐ limitazione della conservazione (articolo 5, paragrafo 1, lettera e));
  - ☐ misure che contribuiscono ai diritti degli interessati:
    - ☐ informazioni fornite all'interessato (articoli 12, 13 e 14);
    - ☐ diritto di accesso e portabilità dei dati (articoli 15 e 20);
    - ☐ diritto di rettifica e alla cancellazione (articoli 16, 17 e 19);
    - ☐ diritto di opposizione e di limitazione di trattamento (articoli 18, 19 e 21);
    - ☐ rapporti con i responsabili del trattamento (articolo 28);
    - ☐ garanzie riguardanti trattamenti internazionali (capo V);
    - ☐ consultazione preventiva (articolo 36).

☐ **i rischi per i diritti e le libertà degli interessati sono gestiti** (articolo 35, paragrafo 7 lettera c)):

- ☐ l'origine, la natura, la particolarità e la gravità dei rischi (cfr. considerando 84) o, più in particolare, per ciascun rischio (accesso illegittimo, modifica indesiderata e scomparsa dei dati) vengono determinate dalla prospettiva degli interessati:
  - ☐ si considerano le fonti di rischio (considerando 90);
  - ☐ sono individuati gli impatti potenziali per i diritti e le libertà degli interessati in caso di eventi che includono l'accesso illegittimo, la modifica indesiderata e la scomparsa dei dati;
  - ☐ sono individuate minacce che potrebbero determinare un accesso illegittimo, una modifica indesiderata e la scomparsa dei dati;
  - ☐ sono stimate la probabilità e la gravità (considerando 90);
- ☐ sono determinate le misure previste per gestire tali rischi (articolo 35, paragrafo 7, lettera d) e considerando 90);

☐ **le parti interessate sono coinvolte:**

- ☐ si consulta il responsabile della protezione dei dati (articolo 35, paragrafo 2);
- ☐ si raccolgono le opinioni degli interessati o dei loro rappresentanti, ove opportuno (articolo 35, paragrafo 9).

Elenco delle tipologie di trattamenti soggetti al requisito di una valutazione d'impatto sulla protezione dei dati - WP 248, rev. 01

ALLEGATO 1 Elenco delle tipologie di trattamenti soggetti al meccanismo di coerenza, da sottoporre a valutazione d'impatto:

1) Trattamenti valutativi o di *scoring* su larga scala, nonché trattamenti che comportano la profilazione degli interessati nonché lo svolgimento di attività predittive effettuate anche *on-line* o attraverso *app*, relativi ad *"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 dell'interessato"*.
2) Trattamenti automatizzati finalizzati ad assumere decisioni che producono *"effetti giuridici"* oppure che incidono *"in modo analogo significativamente"* sull'interessato, comprese le decisioni che impediscono di esercitare un diritto o di avvalersi di un bene o di un servizio o di continuare ad esser parte di un contratto in essere (ad es. *screening* dei clienti di una banca attraverso l'utilizzo di dati registrati in una centrale rischi).
3) Trattamenti che prevedono un utilizzo sistematico di dati per l'osservazione, il monitoraggio o il controllo degli interessati, compresa la raccolta di dati attraverso reti, effettuati anche *on-line* o attraverso *app*, nonché il trattamento di identificativi univoci in grado di identificare gli utenti di servizi della società dell'informazione inclusi servizi *web*, tv interattiva, ecc. rispetto alle abitudini d'uso e ai dati di visione per periodi prolungati. Rientrano in tale previsione anche i trattamenti di metadati ad es. in ambito telecomunicazioni, banche, ecc. effettuati non soltanto per profilazione, ma più in generale per ragioni organizzative, diprevisioni di *budget*, di *upgrade* tecnologico, miglioramento reti, offerta di servizi antifrode, antispam, sicurezza etc.
4) Trattamenti su larga scala di dati aventi carattere estremamente personale (v. WP 248, rev. 01): si fa riferimento, fra gli altri, ai dati connessi alla vita familiare o privata (quali i dati relativi alle comunicazioni elettroniche dei quali occorre tutelare la riservatezza), o che incidono sull'esercizio di un diritto fondamentale (quali i dati sull'ubicazione, la cui raccolta mette in gioco la libertà di circolazione) oppure la cui violazione comporta un grave impatto sulla vita quotidiana dell'interessato (quali

i dati finanziari che potrebbero essere utilizzati per commettere frodi in materia di pagamenti).

5) Trattamenti effettuati nell'ambito del rapporto di lavoro mediante sistemi tecnologici (anche con riguardo ai sistemi di videosorveglianza e di geolocalizzazione) dai quali derivi la possibilità di effettuare un controllo a distanza dell'attività dei dipendenti (si veda quanto stabilito dal WP 248, rev. 01, in relazione ai criteri nn. 3, 7 e 8).
6) Trattamenti non occasionali di dati relativi a soggetti vulnerabili (minori, disabili, anziani, infermi di mente, pazienti, richiedenti asilo).
7) Trattamenti effettuati attraverso l'uso di tecnologie innovative, anche con particolari misure di carattere organizzativo (es. IoT; sistemi di intelligenza artificiale; utilizzo di assistenti vocali on-line attraverso lo scanning vocale e testuale; monitoraggi effettuati da dispositivi *wearable*; tracciamenti di prossimità come ad es. il *wi-fi tracking*) ogniqualvolta ricorra anche almeno un altro dei criteri individuati nel WP 248, rev. 01.
8) Trattamenti che comportano lo scambio tra diversi titolari di dati su larga scala con modalità telematiche.
9) Trattamenti di dati personali effettuati mediante interconnessione, combinazione o raffronto di informazioni, compresi i trattamenti che prevedono l'incrocio dei dati di consumo di beni digitali con dati di pagamento (es. *mobile payment*).
10) Trattamenti di categorie particolari di dati ai sensi dell'art. 9 oppure di dati relativi a condanne penali e a reati di cui all'art. 10 interconnessi con altri dati personali raccolti per finalità diverse.
11) Trattamenti sistematici di dati biometrici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.
12) Trattamenti sistematici di dati genetici, tenendo conto, in particolare, del volume dei dati, della durata, ovvero della persistenza, dell'attività di trattamento.

Delibera del Garante della Privacy 1° Marzo 2007, n. 13 - Le linee guida per posta elettronica e internet

1. Utilizzo della posta elettronica e della rete Internet nel rapporto di lavoro

1.1. Premessa

Dall´esame di diversi reclami, segnalazioni e quesiti è emersa l´esigenza di prescrivere ai datori di lavoro alcune misure, necessarie o opportune, per conformare alle disposizioni vigenti il trattamento di dati personali effettuato per verificare il corretto utilizzo nel rapporto di lavoro della posta elettronica e della rete Internet.
Occorre muovere da alcune premesse:

a) compete ai datori di lavoro assicurare la funzionalità e il corretto impiego di tali mezzi da parte dei lavoratori, definendone le modalità d´uso nell´organizzazione dell´attività lavorativa, tenendo conto della disciplina in tema di diritti e relazioni sindacali;
b) spetta ad essi adottare idonee misure di sicurezza per assicurare la disponibilità e l´integrità di sistemi informativi e di dati, anche per prevenire utilizzi indebiti che possono essere fonte di responsabilità (artt. 15, 31 ss., 167 e 169 del Codice);
c) emerge l´esigenza di tutelare i lavoratori interessati anche perché l´utilizzazione dei predetti mezzi, già ampiamente diffusi nel contesto lavorativo, è destinata ad un rapido incremento in numerose attività svolte anche fuori della sede lavorativa;
d) l´utilizzo di Internet da parte dei lavoratori può infatti formare oggetto di analisi, profilazione e integrale ricostruzione mediante elaborazione di *log file* della navigazione *web* ottenuti, ad esempio, da un *proxy server* o da un altro strumento di registrazione delle informazioni. I servizi di posta elettronica sono parimenti suscettibili (anche attraverso la tenuta di *log file* di traffico *e-mail* e l´archiviazione di messaggi) di controlli che possono giungere fino alla conoscenza da parte del datore di lavoro (titolare del trattamento) del contenuto della corrispondenza;

e) le informazioni così trattate contengono dati personali anche sensibili riguardanti lavoratori o terzi, identificati o identificabili[1].

1.2. Tutela del lavoratore

Le informazioni di carattere personale trattate possono riguardare, oltre all´attività lavorativa, la sfera personale e la vita privata di lavoratori e di terzi. La linea di confine tra questi ambiti, come affermato dalla Corte europea dei diritti dell´uomo, può essere tracciata a volte solo con difficoltà[2].

Il luogo di lavoro è una formazione sociale nella quale va assicurata la tutela dei diritti, delle libertà fondamentali e della dignità degli interessati garantendo che, in una cornice di reciproci diritti e doveri, sia assicurata l´esplicazione della personalità del lavoratore e una ragionevole protezione della sua sfera di riservatezza nelle relazioni personali e professionali (artt. 2 e 41, secondo comma, Cost.; art. 2087 cod. civ.; cfr. altresì l´art. 2, comma 5, Codice dell´amministrazione digitale (d.lg. 7 marzo 2005, n. 82), riguardo al diritto ad ottenere che il trattamento dei dati effettuato mediante l´uso di tecnologie telematiche sia conformato al rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell´interessato)[3].

Non a caso, nell´organizzare l´attività lavorativa e gli strumenti utilizzati, diversi datori di lavoro hanno prefigurato modalità d´uso che, tenendo conto del crescente lavoro in rete e di nuove tariffe di traffico forfettarie, assegnano aree di lavoro riservate per appunti strettamente personali, ovvero consentono usi moderati di strumenti per finalità private.

2. Codice in materia di protezione dei dati e discipline di settore

2.1. Principi generali

Nell´impartire le seguenti prescrizioni il Garante tiene conto del diritto alla protezione dei dati personali, della necessità che il trattamento sia disciplinato assicurando un elevato livello di tutela delle persone, nonché dei principi di semplificazione, armonizza-

1 Cfr. Gruppo Art. 29 sulla protezione dei dati, Parere n. 8/2001 sul trattamento dei dati personali nel contesto dell´occupazione, 13 settembre 2001, punti 5 e 12.

2 Cfr. Niemitz v. Germany, 23 novembre 1992, par. 29; v. pure Halford v. United Kingdom, 25 giugno 1997, parr. 44-46.

3 V. pure Gruppo Art. 29 cit., Documento di lavoro riguardante la vigilanza sulle comunicazioni elettroniche sul posto di lavoro, Wp 55, 29 maggio 2002, p. 4.

zione ed efficacia (artt. 1 e 2 del Codice). Le prescrizioni potranno essere aggiornate alla luce dell´esperienza e dell´innovazione tecnologica.

2.2. Discipline di settore

Alcune disposizioni di settore, fatte salve dal Codice, prevedono specifici divieti o limiti, come quelli posti dallo Statuto dei lavoratori sul controllo a distanza (artt. 113, 114 e 184, comma 3, del Codice; artt. 4 e 8 l. 20 maggio 1970, n. 300).

La disciplina di protezione dei dati va coordinata con regole di settore riguardanti il rapporto di lavoro e il connesso utilizzo di tecnologie, nelle quali è fatta salva o richiamata espressamente (art. 47, comma 3, lett. b) Codice dell´amministrazione digitale)[4].

2.3. Principi del Codice

I trattamenti devono rispettare le garanzie in materia di protezione dei dati e svolgersi nell´osservanza di alcuni cogenti principi:

a) il principio di *necessità*, secondo cui i sistemi informativi e i programmi informatici devono essere configurati riducendo al minimo l´utilizzazione di dati personali e di dati identificativi in relazione alle finalità perseguite (art. 3 del Codice; par. 5.2);
b) il principio di *correttezza*, secondo cui le caratteristiche essenziali dei trattamenti devono essere rese note ai lavoratori (art. 11, comma 1, lett. a), del Codice). Le tecnologie dell´informazione (in modo più marcato rispetto ad apparecchiature tradizionali) permettono di svolgere trattamenti ulteriori rispetto a quelli connessi ordinariamente all´attività lavorativa. Ciò, all´insaputa o senza la piena consapevolezza dei lavoratori, considerate anche le potenziali applicazioni di regola non adeguatamente conosciute dagli interessati (v. par. 3);
c) i trattamenti devono essere effettuati per finalità *determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice: par. 4 e 5)*, osservando il principio di pertinenza e non eccedenza (par. 6). Il datore di lavoro deve trattare i dati *"nella misura meno invasiva possibile"*; le attività di monitoraggio devono essere svolte solo da soggetti preposti (par. 8) ed essere *"mirate sull´area di rischio, tenendo conto della normativa sulla protezione dei dati e, se pertinente, del principio di segretezza della corrispondenza"* (Parere n. 8/2001, cit., punti 5 e 12).

4 V. pure la Direttiva per l´impiego della posta elettronica nelle pubbliche amministrazioni del 27 novembre 2003; Raccomandazione n. R (89)2 del Consiglio d´Europa in materia di protezione dei dati personali nel contesto del rapporto di lavoro; Parere n. 8/2001 , cit., punto 5.

3. Controlli e correttezza nel trattamento

3.1. Disciplina interna

In base al richiamato principio di correttezza, l´eventuale trattamento deve essere ispirato ad un canone di trasparenza, come prevede anche la disciplina di settore (art. 4, secondo comma, Statuto dei lavoratori; allegato VII, par. 3 d.lg. n. 626/1994 e successive integrazioni e modificazioni in materia di *"uso di attrezzature munite di videoterminali", il quale esclude la possibilità del controllo informatico "all´insaputa dei lavoratori"*)[5].

Grava quindi sul datore di lavoro l´onere di indicare in ogni caso, chiaramente e in modo particolareggiato, quali siano le modalità di utilizzo degli strumenti messi a disposizione ritenute corrette e se, in che misura e con quali modalità vengano effettuati controlli. Ciò, tenendo conto della pertinente disciplina applicabile in tema di informazione, concertazione e consultazione delle organizzazioni sindacali.

Per la predetta indicazione il datore ha a disposizione vari mezzi, a seconda del genere e della complessità delle attività svolte, e informando il personale con modalità diverse anche a seconda delle dimensioni della struttura, tenendo conto, ad esempio, di piccole realtà dove vi è una continua condivisione interpersonale di risorse informative.

3.2. Linee guida

In questo quadro, può risultare opportuno adottare un disciplinare interno redatto in modo chiaro e senza formule generiche, da pubblicizzare adeguatamente (verso i singoli lavoratori, nella rete interna, mediante affissioni sui luoghi di lavoro con modalità analoghe a quelle previste dall´art. 7 dello Statuto dei lavoratori, ecc.) e da sottoporre ad aggiornamento periodico.

A seconda dei casi andrebbe ad esempio specificato:

- se determinati comportamenti non sono tollerati rispetto alla "navigazione" in Internet (ad es., il *download* di software o di *file* musicali), oppure alla tenuta di *file* nella rete interna;
- in quale misura è consentito utilizzare anche per ragioni personali servizi di posta elettronica o di rete, anche solo da determinate postazioni di lavoro o caselle oppure ricorrendo a sistemi di *webmail*, indicandone le modalità e l´arco temporale di utilizzo (ad es., fuori dall´orario di lavoro o durante le pause, o consentendone un uso moderato anche nel tempo di lavoro);

5 V. altresì la Raccomandazione n. R (89) 2, cit., punto 3; Parere n. 8/2001 , cit., punto 9.1 e Wp 55, cit., punto 3.1.3.

- quali informazioni sono memorizzate temporaneamente (ad es., le componenti di *file* di *log* eventualmente registrati) e chi (anche all´esterno) vi può accedere legittimamente;
- se e quali informazioni sono eventualmente conservate per un periodo più lungo, in forma centralizzata o meno (anche per effetto di copie di *back up*, della gestione tecnica della rete o di *file* di *log*);
- se, e in quale misura, il datore di lavoro si riserva di effettuare controlli in conformità alla legge, anche saltuari o occasionali, indicando le ragioni legittime–specifiche e non generiche–per cui verrebbero effettuati (anche per verifiche sulla funzionalità e sicurezza del sistema) e le relative modalità (precisando se, in caso di abusi singoli o reiterati, vengono inoltrati preventivi avvisi collettivi o individuali ed effettuati controlli nominativi o su singoli dispositivi e postazioni);
- quali conseguenze, anche di tipo disciplinare, il datore di lavoro si riserva di trarre qualora constati che la posta elettronica e la rete Internet sono utilizzate indebitamente;
- le soluzioni prefigurate per garantire, con la cooperazione del lavoratore, la continuità dell´attività lavorativa in caso di assenza del lavoratore stesso (specie se programmata), con particolare riferimento all´attivazione di sistemi di risposta automatica ai messaggi di posta elettronica ricevuti;
- se sono utilizzabili modalità di uso personale di mezzi con pagamento o fatturazione a carico dell´interessato;
- quali misure sono adottate per particolari realtà lavorative nelle quali debba essere rispettato l´eventuale segreto professionale cui siano tenute specifiche figure professionali;
- le prescrizioni interne sulla sicurezza dei dati e dei sistemi (art. 34 del Codice, nonché Allegato B), in particolare regole 4, 9, 10).

3.3. Informativa (art. 13 del Codice)

All´onere del datore di lavoro di prefigurare e pubblicizzare una *policy* interna rispetto al corretto uso dei mezzi e agli eventuali controlli, si affianca il dovere di informare comunque gli interessati ai sensi dell´art. 13 del Codice, anche unitamente agli elementi indicati ai punti 3.1. e 3.2.

Rispetto a eventuali controlli gli interessati hanno infatti il diritto di essere informati preventivamente, e in modo chiaro, sui trattamenti di dati che possono riguardarli.

Le finalità da indicare possono essere connesse a specifiche esigenze organizzative, produttive e di sicurezza del lavoro, quando

comportano un trattamento lecito di dati (art. 4, secondo comma, l. n. 300/1970); possono anche riguardare l´esercizio di un diritto in sede giudiziaria.
Devono essere tra l´altro indicate le principali caratteristiche dei trattamenti, nonché il soggetto o l´unità organizzativa ai quali i lavoratori possono rivolgersi per esercitare i propri diritti.

4. Apparecchiature preordinate al controllo a distanza

Con riguardo al principio secondo cui occorre perseguire finalità determinate, esplicite e legittime (art. 11, comma 1, lett. b), del Codice), il datore di lavoro può riservarsi di controllare (direttamente o attraverso la propria struttura) l´effettivo adempimento della prestazione lavorativa e, se necessario, il corretto utilizzo degli strumenti di lavoro (cfr. artt. 2086, 2087 e 2104 cod. civ.).
Nell´esercizio di tale prerogativa occorre rispettare la libertà e la dignità dei lavoratori, in particolare per ciò che attiene al divieto di installare *"apparecchiature per finalità di controllo a distanza dell´attività dei lavoratori"* (art. 4, primo comma, l. n. 300/1970), tra cui
sono certamente comprese strumentazioni *hardware* e *software* mirate al controllo dell´utente di un sistema di comunicazione elettronica.
Il trattamento dei dati che ne consegue è illecito, a prescindere dall´illiceità dell´installazione stessa. Ciò, anche quando i singoli lavoratori ne siano consapevoli[6].
In particolare non può ritenersi consentito il trattamento effettuato mediante sistemi *hardware* e *software* preordinati al controllo a distanza, grazie ai quali sia possibile ricostruire–a volte anche minuziosamente–l´attività di lavoratori. É il caso, ad esempio:

- della lettura e della registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio *e-mail*;
- della riproduzione ed eventuale memorizzazione sistematica delle pagine *web* visualizzate dal lavoratore;
- della lettura e della registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
- dell´analisi occulta di computer portatili affidati in uso.

6 Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

Il controllo a distanza vietato dalla legge riguarda l´attività lavorativa in senso stretto e altre condotte personali poste in essere nel luogo di lavoro[7]. A parte eventuali responsabilità civili e penali, i dati trattati illecitamente non sono utilizzabili (art. 11, comma 2, del Codice)[8].

5. Programmi che consentono controlli "indiretti"

5.1.

Il datore di lavoro, utilizzando sistemi informativi per esigenze produttive o organizzative (ad es., per rilevare anomalie o per manutenzioni) o, comunque, quando gli stessi si rivelano necessari per la sicurezza sul lavoro, può avvalersi legittimamente, nel rispetto dello Statuto dei lavoratori (art. 4, comma 2), di sistemi che consentono indirettamente un controllo a distanza (c.d. controllo preterintenzionale) e determinano un trattamento di dati personali riferiti o riferibili ai lavoratori[9]. Ciò, anche in presenza di attività di controllo discontinue[10].

Il trattamento di dati che ne consegue può risultare lecito. Resta ferma la necessità di rispettare le procedure di informazione e di consultazione di lavoratori e sindacati in relazione all´introduzione o alla modifica di sistemi automatizzati per la raccolta e l´utilizzazione dei dati[11], nonché in caso di introduzione o di modificazione di procedimenti tecnici destinati a controllare i movimenti o la produttività dei lavoratori[12].

5.2. Principio di necessità

In applicazione del menzionato principio di necessità il datore di lavoro è chiamato a promuovere ogni opportuna misura, organizzativa e tecnologica volta a prevenire il rischio di utilizzi impropri (da preferire rispetto all´adozione di misure "repressive") e, co-

7 Cfr. Cass. 11 marzo 1986, n. 1490.

8 Cfr. anche Cass., 17 giugno 2000, n. 8250 rispetto all´uso probatorio.

9 Cass. 18 febbraio 1983, n. 1236 e 16 settembre 1997, n. 9211.

10 Cass. 11 marzo 1986, n. 1490 cit.

11 Raccomandazione n. R (89)2, cit., art. 3, comma 1.

12 Raccomandazione n. R (89)2, art. 3, comma 2; disposizione in base alla quale, in presenza di rischi "per il diritto al rispetto della vita privata e della dignità umana dei lavoratori, dovrà essere ricercato l´accordo dei lavoratori o dei loro rappresentanti prima dell´introduzione o della modifica di tali sistemi o procedimenti, a meno che altre garanzie specifiche non siano previste dalla legislazione nazionale": art. 3, comma 3.

munque, a "minimizzare" l´uso di dati riferibili ai lavoratori (artt. 3, 11, comma 1, lett. d) e 22, commi 3 e 5, del Codice; aut. gen. al trattamento dei dati sensibili n. 1/2005, punto 4). Dal punto di vista organizzativo è quindi opportuno che:

- si valuti attentamente l´impatto sui diritti dei lavoratori (prima dell´installazione di apparecchiature suscettibili di consentire il controllo a distanza e dell´eventuale trattamento);
- si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l´utilizzo della posta elettronica e l´accesso a Internet[13];
- si determini quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di un loro impiego abusivo.

Il datore di lavoro ha inoltre l´onere di adottare tutte le misure tecnologiche volte a minimizzare l´uso di dati identificativi (c.d. *privacy enhancing technologies–PETs*). Le misure possono essere differenziate a seconda della tecnologia impiegata (ad es., posta elettronica o navigazione in Internet).

a) Internet: la navigazione web

Il datore di lavoro, per ridurre il rischio di usi impropri della "navigazione" in Internet (consistenti in attività non correlate alla prestazione lavorativa quali la visione di siti non pertinenti, l´*upload* o il *download* di *file*, l´uso di servizi di rete con finalità ludiche o estranee all´attività), deve adottare opportune misure che possono, così, prevenire controlli successivi sul lavoratore. Tali controlli, leciti o meno a seconda dei casi, possono determinare il trattamento di informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale (art. 8 l. n. 300/1970; artt. 26 e 113 del Codice; Provv. 2 febbraio 2006, cit.).
In particolare, il datore di lavoro può adottare una o più delle seguenti misure opportune, tenendo conto delle peculiarità proprie di ciascuna organizzazione produttiva e dei diversi profili professionali:

- individuazione di categorie di siti considerati correlati o meno con la prestazione lavorativa;
- configurazione di sistemi o utilizzo di filtri che prevengano determinate operazioni–reputate inconferenti con l´attività lavorativa–quali l´*upload* o l´accesso a determi-

13 Cfr. Provv. 2 febbraio 2006 , in , doc. web n. 1229854.

nati siti (inseriti in una sorta di *black list*) e/o il *download* di file o *software* aventi particolari caratteristiche (dimensionali o di tipologia di dato);

- trattamento di dati in forma anonima o tale da precludere l´immediata identificazione di utenti mediante loro opportune aggregazioni (ad es., con riguardo ai *file* di *log* riferiti al traffico *web*, su base collettiva o per gruppi sufficientemente ampi di lavoratori);
- eventuale conservazione nel tempo dei dati strettamente limitata al perseguimento di finalità organizzative, produttive e di sicurezza.

b) Posta elettronica

Il contenuto dei messaggi di posta elettronica–come pure i dati esteriori delle comunicazioni e i file allegati–riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente, la cui *ratio* risiede nel proteggere il nucleo essenziale della dignità umana e il pieno sviluppo della personalità nelle formazioni sociali; un´ulteriore protezione deriva dalle norme penali a tutela dell´inviolabilità dei segreti (artt. 2 e 15 Cost.; Corte cost. 17 luglio 1998, n. 281 e 11 marzo 1993, n. 81; art. 616, quarto comma, c.p.; art. 49 Codice dell´amministrazione digitale)[14].

Tuttavia, con specifico riferimento all´impiego della posta elettronica nel contesto lavorativo e in ragione della veste esteriore attribuita all´indirizzo di posta elettronica nei singoli casi, può risultare dubbio se il lavoratore, in qualità di destinatario o mittente, utilizzi la posta elettronica operando quale espressione dell´organizzazione datoriale o ne faccia un uso personale pur operando in una struttura lavorativa.

La mancata esplicitazione di una *policy* al riguardo può determinare anche una legittima aspettativa del lavoratore, o di terzi, di confidenzialità rispetto ad alcune forme di comunicazione.

Tali incertezze si riverberano sulla qualificazione, in termini di liceità, del comportamento del datore di lavoro che intenda apprendere il contenuto di messaggi inviati all'indirizzo di posta elettronica usato dal lavoratore (posta "in entrata") o di quelli inviati da quest´ultimo (posta "in uscita").

É quindi particolarmente opportuno che si adottino accorgimenti anche per prevenire eventuali trattamenti in violazione dei principi di pertinenza e non eccedenza. Si tratta di soluzioni che possono risultare utili per contemperare le esigenze di ordinato svolgimento dell´attività lavorativa con la prevenzione di inutili intrusioni nella sfera personale dei lavoratori, nonché violazioni della disciplina sull´eventuale segretezza della corrispondenza.

---

14 Cfr. nota del Garante 16 giugno 1999 , Boll. n. 9, giugno 1999 , p. 96; Tar Lazio, Sez. I ter, 15 novembre 2001, n. 9425.

In questo quadro è opportuno che:

- il datore di lavoro renda disponibili indirizzi di posta elettronica condivisi tra più lavoratori (ad esempio, info@ente.it, ufficiovendite@ente.it, ufficioreclami@società.com, urp@ente.it, etc.), eventualmente affiancandoli a quelli individuali (ad esempio, m.rossi@ente.it, rossi@società.com, mario.rossi@società.it);
- il datore di lavoro valuti la possibilità di attribuire al lavoratore un diverso indirizzo destinato ad uso privato del lavoratore[15];
- il datore di lavoro metta a disposizione di ciascun lavoratore apposite funzionalità di sistema, di agevole utilizzo, che consentano di inviare automaticamente, in caso di assenze (ad es., per ferie o attività di lavoro fuori sede), messaggi di risposta contenenti le "coordinate" (anche elettroniche o telefoniche) di un altro soggetto o altre utili modalità di contatto della struttura. É parimenti opportuno prescrivere ai lavoratori di avvalersi di tali modalità, prevenendo così l´apertura della posta elettronica[16]. In caso di eventuali assenze non programmate (ad es., per malattia), qualora il lavoratore non possa attivare la procedura descritta (anche avvalendosi di servizi *webmail*), il titolare del trattamento, perdurando l´assenza oltre un determinato limite temporale, potrebbe disporre lecitamente, sempre che sia necessario e mediante personale appositamente incaricato (ad es., l´amministratore di sistema oppure, se presente, un incaricato aziendale per la protezione dei dati),
- l´attivazione di un analogo accorgimento, avvertendo gli interessati;
- in previsione della possibilità che, in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all´attività lavorativa, si debba conoscere il contenuto dei messaggi di posta elettronica, l´interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa. A cura del titolare del trattamento, di tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;
- i messaggi di posta elettronica contengano un avvertimento ai destinatari nel quale sia dichiarata l´eventuale natura non personale dei messaggi stessi, precisando se le risposte potranno essere conosciute nell´organizzazione di appartenenza del mittente e con eventuale rinvio alla predetta *policy* datoriale.

15 Cfr. il documento Wp 55, cit., p. 23.

16 Cfr. il documento Wp 55, cit., p. 5.

6. Pertinenza e non eccedenza

6.1. Graduazione dei controlli

Nell´effettuare controlli sull´uso degli strumenti elettronici deve essere evitata un´interferenza ingiustificata sui diritti e sulle libertà fondamentali di lavoratori, come pure di soggetti esterni che ricevono o inviano comunicazioni elettroniche di natura personale o privata.

L´eventuale controllo è lecito solo se sono rispettati i principi di pertinenza e non eccedenza.

Nel caso in cui un evento dannoso o una situazione di pericolo non sia stato impedito con preventivi accorgimenti tecnici, il datore di lavoro può adottare eventuali misure che consentano la verifica di comportamenti anomali.

Deve essere per quanto possibile preferito un controllo preliminare su dati aggregati, riferiti all´intera struttura lavorativa o a sue aree.

Il controllo anonimo può concludersi con un avviso generalizzato relativo ad un rilevato utilizzo anomalo degli strumenti aziendali e con l´invito ad attenersi scrupolosamente a compiti assegnati e istruzioni impartite. L´avviso può essere circoscritto a dipendenti afferenti all´area o settore in cui è stata rilevata l´anomalia. In assenza di successive anomalie non è di regola giustificato effettuare controlli su base individuale.

Va esclusa l´ammissibilità di controlli prolungati, costanti o indiscriminati.

6.2. Conservazione

I sistemi *software* devono essere programmati e configurati in modo da cancellare periodicamente ed automaticamente (attraverso procedure di sovraregistrazione come, ad esempio, la cd. rotazione dei *log file*) i dati personali relativi agli accessi ad Internet e al traffico telematico, la cui conservazione non sia necessaria.

In assenza di particolari esigenze tecniche o di sicurezza, la conservazione temporanea dei dati relativi all´uso degli strumenti elettronici deve essere giustificata da una finalità specifica e comprovata e limitata al tempo necessario–e predeterminato–a raggiungerla (v. art. 11, comma 1, lett. e), del Codice).

Un eventuale prolungamento dei tempi di conservazione va valutato come eccezionale e può aver luogo solo in relazione:

- ad esigenze tecniche o di sicurezza del tutto particolari;
- all´indispensabilità del dato rispetto all´esercizio o alla difesa di un diritto in sede giudiziaria;

› all´obbligo di custodire o consegnare i dati per ottemperare ad una specifica richiesta dell´autorità giudiziaria o della polizia giudiziaria.

In questi casi, il trattamento dei dati personali (tenendo conto, con riguardo ai dati sensibili, delle prescrizioni contenute nelle autorizzazioni generali nn. 1/2005 e 5/2005 adottate dal Garante) deve essere limitato alle sole informazioni indispensabili per perseguire finalità preventivamente determinate ed essere effettuato con logiche e forme di organizzazione strettamente correlate agli obblighi, compiti e finalità già esplicitati.

7. Presupposti di liceità del trattamento: bilanciamento di interessi

7.1. Datori di lavoro privati

I datori di lavoro privati e gli enti pubblici economici, se ricorrono i presupposti sopra indicati (v., in particolare, art. 4, secondo comma, dello Statuto), possono effettuare lecitamente il trattamento dei dati personali diversi da quelli sensibili.
Ciò, può avvenire:

a) se ricorrono gli estremi del legittimo esercizio di un diritto in sede giudiziaria (art. 24, comma 1, lett. f) del Codice);
b) in caso di valida manifestazione di un libero consenso;
c) anche in assenza del consenso, ma per effetto del presente provvedimento che individua un legittimo interesse al trattamento in applicazione della disciplina sul c.d. bilanciamento di interessi (art. 24, comma 1, lett. g), del Codice).

Per tale bilanciamento si è tenuto conto delle garanzie che lo Statuto prevede per il controllo "indiretto" a distanza presupponendo non il consenso degli interessati, ma un accordo con le rappresentanze sindacali (o, in difetto, l´autorizzazione di un organo periferico dell´amministrazione del lavoro).
L´eventuale trattamento di dati sensibili è consentito con il consenso degli interessati o, senza il consenso, nei casi previsti dal Codice (in particolare, esercizio di un diritto in sede giudiziaria, salvaguardia della vita o incolumità fisica; specifici obblighi di legge anche in caso di indagine giudiziaria: art. 26).

7.2. Datori di lavoro pubblici

Per quanto riguarda i soggetti pubblici restano fermi i differenti presupposti previsti dal Codice a seconda della natura dei dati, sensibili o meno (artt. 18-22 e 112).
In tutti i casi predetti resta impregiudicata la facoltà del lavoratore di opporsi al trattamento per motivi legittimi (art. 7, comma 4, lett. a), del Codice).

8. Individuazione dei soggetti preposti

Il datore di lavoro può ritenere utile la designazione (facoltativa), specie in strutture articolate, di uno o più responsabili del trattamento cui impartire precise istruzioni sul tipo di controlli ammessi e sulle relative modalità (art. 29 del Codice).
Nel caso di eventuali interventi per esigenze di manutenzione del sistema, va posta opportuna cura nel prevenire l´accesso a dati personali presenti in cartelle o spazi di memoria assegnati a dipendenti.
Resta fermo l´obbligo dei soggetti preposti al connesso trattamento dei dati (in particolare, gli incaricati della manutenzione) di svolgere solo operazioni strettamente necessarie al perseguimento delle relative finalità, senza realizzare attività di controllo a distanza, anche di propria iniziativa.
Resta parimenti ferma la necessità che, nell´individuare regole di condotta dei soggetti che operano quali amministratori di sistema o figure analoghe cui siano rimesse operazioni connesse al regolare funzionamento dei sistemi, sia svolta un´attività formativa sui profili tecnico-gestionali e di sicurezza delle reti, sui principi di protezione dei dati personali e sul segreto nelle comunicazioni (cfr. Allegato B) al Codice, regola n. 19.6; Parere n. 8/2001 cit., punto 9).

Tutto ciò premesso il garante

1) prescrive ai datori di lavoro privati e pubblici, ai sensi dell´art. 154, comma 1, lett. c), del Codice, di adottare la misura necessaria a garanzia degli interessati, nei termini di cui in motivazione, riguardante l´onere di specificare le modalità di utilizzo della posta elettronica e della rete Internet da parte dei lavoratori (punto 3.1.), indicando chiaramente le modalità di uso degli strumenti messi a disposizione e se, in che misura e con quali modalità vengano effettuati controlli;

2) indica inoltre, ai medesimi datori di lavoro, le seguenti linee guida a garanzia degli interessati, nei termini di cui in motivazione, per ciò che riguarda:
   a) l´adozione e la pubblicizzazione di un disciplinare interno (punto 3.2.);
   b) l´adozione di misure di tipo organizzativo (punto 5.2.) affinché, segnatamente:
      - si proceda ad un´attenta valutazione dell´impatto sui diritti dei lavoratori;
      - si individui preventivamente (anche per tipologie) a quali lavoratori è accordato l´utilizzo della posta elettronica e dell´accesso a Internet;
      - si individui quale ubicazione è riservata alle postazioni di lavoro per ridurre il rischio di impieghi abusivi;
   c) l´adozione di misure di tipo tecnologico, e segnatamente:
      I) rispetto alla "navigazione" in Internet (punto 5.2., a):
         - l´individuazione di categorie di siti considerati correlati o non correlati con la prestazione lavorativa;
         - la configurazione di sistemi o l´utilizzo di filtri che prevengano determinate operazioni;
         - il trattamento di dati in forma anonima o tale da precludere l´immediata identificazione degli utenti mediante opportune aggregazioni;
         - l´eventuale conservazione di dati per il tempo strettamente limitato al perseguimento di finalità organizzative, produttive e di sicurezza;
         - la graduazione dei controlli (punto 6.1.);
      II) rispetto all´utilizzo della posta elettronica (punto 5.2., b):
         - la messa a disposizione di indirizzi di posta elettronica condivisi tra più lavoratori, eventualmente affiancandoli a quelli individuali;
         - l´eventuale attribuzione al lavoratore di un diverso indirizzo destinato ad uso privato;
         - la messa a disposizione di ciascun lavoratore, con modalità di agevole esecuzione, di apposite funzionalità di sistema che consentano di inviare automaticamente, in caso di assenze programmate, messaggi di risposta che contengano le "coordinate" di altro soggetto o altre utili modalità di contatto dell´istituzione presso la quale opera il lavoratore assente;
         - consentire che, qualora si debba conoscere il contenuto dei messaggi di posta elettronica in caso di assenza improvvisa o prolungata e per improrogabili necessità legate all´attività lavorativa, l´interessato sia messo in grado di delegare un altro lavoratore (fiduciario) a verificare il contenuto di messaggi e a inoltrare al titolare del trattamento quelli ritenuti rilevanti per lo svolgimento dell´attività lavorativa. Di

tale attività dovrebbe essere redatto apposito verbale e informato il lavoratore interessato alla prima occasione utile;

- l´inserzione nei messaggi di un avvertimento ai destinatari nel quale sia dichiarata l´eventuale natura non personale del messaggio e sia specificato se le risposte potranno essere conosciute nell´organizzazione di appartenenza del mittente;
- la graduazione dei controlli (punto 6.1.);

3) vieta ai datori di lavoro privati e pubblici, ai sensi dell´art. 154, comma 1, lett. d), del Codice, di effettuare trattamenti di dati personali mediante sistemi *hardware* e *software* che mirano al controllo a distanza di lavoratori (punto 4), svolti in particolare mediante:
   a) la lettura e la registrazione sistematica dei messaggi di posta elettronica ovvero dei relativi dati esteriori, al di là di quanto tecnicamente necessario per svolgere il servizio e-mail;
   b) la riproduzione e l´eventuale memorizzazione sistematica delle pagine web visualizzate dal lavoratore;
   c) la lettura e la registrazione dei caratteri inseriti tramite la tastiera o analogo dispositivo;
   d) l´analisi occulta di computer portatili affidati in uso;

4) individua, ai sensi dell´art. 24, comma 1, lett. g), del Codice, nei termini di cui in motivazione (punto 7), i casi nei quali il trattamento dei dati personali di natura non sensibile possono essere effettuati per perseguire un legittimo interesse del datore di lavoro anche senza il consenso degli interessati;

5) dispone che copia del presente provvedimento sia trasmessa al Ministero della giustizia-Ufficio pubblicazione leggi e decreti, per la sua pubblicazione sulla *Gazzetta Ufficiale* della Repubblica italiana ai sensi dell´art. 143, comma 2, del Codice.

Composizione del Consiglio Nazionale dei Dottori Commercialisti e degli Esperti Contabili

Presidente
Massimo Miani

Vice Presidente
Davide Di Russo

Consigliere Segretario
Achille Coppola

Consigliere Tesoriere
Roberto Cunsolo

Consiglieri
Antonio Borrelli
Andrea Foschi
Marcella Galvani
Gilberto Gelosa
Valeria Giancola
Maurizio G. Grosso
Giuseppe Laurino
Giorgio Luchetta
Raffaele Marcello
Francesco Muraca
Maurizio Postal
Sandro Santi
Massimo Scotton
Remigio E. M. Sequi
Lorenzo Sirch
Alessandro Solidoro
Giuseppe Tedesco

CNDCEC
Piazza della Repubblica, 59
00185 - Roma
Tel. 06.47863300
Fax. 06.47863349
E-mail info@commercialisti.it
Web. www.commercialisti.it

Direttore Generale
Francesca Maione

Composizione della Fondazione Nazionale di Ricerca dei Commercialisti

Segretario Generale
Andrea Foschi

Coordinatore dipartimenti ricerca scientifica
Gianpaolo Valente

Consiglieri
Nicolino Cavalluzzo
Nicolò La Barbera
Vittorio Raccamari
Paolo Rollo
Sandro Santi
Ermanno Werthhammer

FNC
Piazza della Repubblica, 68
00185 - Roma
Tel. 06.4782901
Fax. 06.4874756
E-mail info@fncommercialisti.it
Web. www.fondazionenazionalecommercialisti.it

FNC

ISBN 978-88-99517-20-5

www.fondazionenazionalecommercialisti.it