Privacy e trattamento dei dati personali

Secondo il Regolamento UE 2016/679

di Dorina Cocca e Tiziano Argazzi [*]

Il nuovo Regolamento Europeo della Privacy, nel seguito **Regolamento**, è in vigore in via definitiva in ogni Stato dell'Unione Europea dal 25 maggio 2018.Il provvedimento è composto da 99 articoli (suddivisi fra nove Capi e 15 Sezioni) e da 173 "Considerando". Con l'indicato provvedimento la UE ha portato a sintesi le variegate normative in materia di privacy, via via poste in essere dagli Stati membri,con lo scopo di definire un quadro solido ed omogeneo in tutta l'Unione in grado, da un lato, di eliminare le incertezze giuridiche connesse con la privacy e garantire, dall'altro, una tutela specifica e qualificata a tutti i cittadini dell'Unione ed ai loro dati personali.Inoltre ai titolari ed ai responsabili del trattamento vengono assegnate maggiori responsabilità nel garantire l'efficace tutela dei dati personali delle persone fisiche.

Nei paragrafi che seguono si farà una breve disamina di alcune delle norme più innovative,attualmente in vigore e ci si soffermerà,in particolare, sul trattamento dei dati dei lavoratori da parte del datore di lavoro e delle prescrizioni del **Garante per la Protezione dei Dati Personali,fornite con provvedimento n. 146 del 5.06.2019.**

Dal diritto alla riservatezza alla tutela dei dati personali

Si ritiene utile ripercorrere, seppur brevemente, le tappe che in Italia hanno segnato la nascita della normativa in materia di privacy e di protezione dei dati personali.

Nell'ordinamento italiano la questione venne posta a livello giurisprudenziale a partire dalla metà degli anni '50, dagli eredi del tenore Enrico Caruso[1]. La Suprema Corte (Sent. 22 dicembre 1956 n. 4487) però stabilì che *"nell'ordinamento giuridico italiano non esiste un diritto alla riservatezza, ma soltanto sono riconosciuti e tutelati, in modi diversi, singoli diritti soggettivi della persona; pertanto non è vietato comunicare, sia privatamente sia pubblicamente, vicende, tanto più se immaginarie, della vita altrui, quando la conoscenza non ne sia stata ottenuta con mezzi di per sé illeciti o che impongano l'obbligo del segreto"*. Solo una decina di anni dopo la Corte di Cassazione pur ribadendo che "nell'ordinamento non esiste una norma che tuteli il semplice desiderio di riserbo" ha però ritenuto che, in ragione dell'art. 2 Cost, è tutelabile il diritto di personalità, che viene di fatto violato nel momento in cui sono divulgate notizie, da ritenersi riservate, afferenti la vita privata.

Sempre la Suprema Corte con successiva sentenza, 27 maggio 1975 n. 2129, ha riconosciuto che l'ordinamento giuridico italiano contempla e riconosce il *"diritto alla riservatezza, che consiste nella tutela di quelle situazioni e vicende strettamente personali e familiari le quali, anche se verificatesi fuori dal domicilio domestico, non hanno per i terzi un interesse socialmente apprezzabile, contro le ingerenze che, sia pure compiute con mezzi leciti, per scopi non esclusivamente speculativi e senza offesa per l'onore, la reputazione o il decoro, non sono giustificati da interessi pubblici preminenti"*.

È doveroso da subito riconoscere che il concetto di "riservatezza" definita in più occasioni dalla Cassazione, come uno strumento di tutela del singolo, contro le ingerenze di terzi, in vicende strettamente personali non coincide ancora con l'idea moderna di privacy. Dovranno passare altri 21 anni prima della piena codifica di tale concetto avvenuta con l'approvazione della prima normativa organica in materia di privacy[2], sostituita sette anni dopo dal Codice in materia di protezione dei dati personali, approvato con D.Lgs. 30.06.2003 n. 196. Il legislatore con tali ultime due norme ha fatto un enorme salto di qualità parlando non più di semplice diritto alla riservatezza ma di tutela dei dati personali a "tutto tondo". È stato parimenti riconosciuto che la tutela dei dati personali si estrinseca, da un lato, nel diritto a non vedere trattati i propri dati personali senza consenso esplicito e dall'altro nella piena e totale garanzia che il trattamento dei dati personali è stato preceduto dalla messa a punto di una serie di misure minime di sicurezza che ne scongiurino rischi di trattamenti non autorizzati[3].

Trattamento dei dati personali, le novità introdotte

Il **Regolamento** interviene sulle seguenti cinque macro aree:

(a) Le categorie di dati soggette alla nuova normativa;
(b) La liceità del trattamento e l'esplicitazione del consenso;
(c) La responsabilizzazione intesa come insieme degli obblighi in capo al titolare del trattamento;
(d) Le norme tecniche e procedurali idonee a garantire la sicurezza e la inviolabilità dei dati;
(e) Controlli e sanzioni applicabili in caso di non corretto trattamento dei dati personali.

Grande attenzione è stata dedicata, da un lato, alle figure del **Titolare** e dei **Responsabili del trattamento e della Protezione dei dati personali** e, dall'altro, agli strumenti del **Data Protection Impact Assessment (DPIA)** e della procedura di **Prior Consultation**, che si sostanzia nella presentazione di una istanza al Garante qualora il DPIA non produca risultati positivi. Altri tre concetti di nuova istituzione sono quelli della **Accountability**, della **Privacy by Design** e della **Privacy by Default**.

L'istituto del **Data Protection Impact Assessment** cioè la "Valutazione d'impatto sulla protezione dei dati", introdotto all'art. 35, prevede la valutazione degli eventuali rischi per diritti e libertà personali degli interessati in conseguenza di un ipotetico "**Data Breach**" cioè una violazione dei dati personali raccolti, a causa di loro perdita, furto o distruzione.

Risultano anche ampliati i diritti degli interessati con la previsione, ad esempio, del diritto alla "**Portabilità dei Dati**", in ragione del quale l'interessato può, in ogni momento, chiedere ed ottenere, in un formato strutturato, di uso comune e leggibile da dispositivo automatico i dati personali che lo riguardano forniti a un titolare del trattamento e ha il diritto di trasmettere tali dati ad un altro titolare del trattamento senza impedimenti.

Il legislatore italiano ha armonizzato la normativa preesistente al nuovo **Regolamento** a mezzo del D.Lgs. 10 agosto 2018, n. 101 (in vigore dal 19 settembre 2018), che ha abrogato e modificato diversi articoli, in contrasto con le nuove disposizioni introdotte dal legislatore europeo e, nel contempo, ne ha posti in essere di nuovi. Fra le norme che risultano superate c'è quella relativa alle "Misure minime" di sicurezza alla base del preesistente Codice sulla Privacy che sono state sostituite dalle "Misure adeguate".

Accountability, Privacy by Design e Privacy by Default

Accountability[4], ovvero principio di responsabilizzazione,

introdotto all'art. 5, par.2 ed ulteriormente esplicitato all'art. 24, par.1, è un concetto che nel **Regolamento** riveste grande importanza. Infatti con le nuove norme, la privacy ha "cambiato pelle" passando da "sommatoria" di adempimenti, molti dei quali formali, a processo aziendale complesso, che attraversa tutte le articolazioni dell'impresa. Il responsabile di tale processo è il titolare del trattamento il quale deve, tra l'altro, garantire che le misure tecniche e organizzative poste in essere siano adeguate per il corretto trattamento dei dati. Inoltre il medesimo, deve essere in grado di dimostrare, in qualunque momento, la conformità delle attività poste in essere con quanto disposto dal **Regolamento**, tenendo in debito conto la natura, l'ambito di applicazione, il contesto e le finalità del trattamento stesso.

Da quanto precede è di tutta evidenza che le procedure da adottarsi per garantire una efficace protezione dei dati **non sono statiche** (come in passato) **ma dinamiche**, e necessitano di una continua riattualizzazione per garantirne, nel tempo,la rispondenza alla legge anche a mezzo di specifici adeguamenti degli strumenti informatici con cui il trattamento viene effettuato.

Da ciò discende che ogni fase del trattamento deve essere visibile e trasparente per garantire la tutela dei dati, che debbono essere trattati in massima sicurezza, durante l'intero ciclo del prodotto o del servizio. **In tal modo, l'intero sistema deve porre l'utente al centro di ogni trattamento per garantirgli una tutela effettiva.**

Questi principi, definiti come **Privacy by Design** e **Privacy by Default** – che stanno ad indicare Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita – sono codificati all'art. 25. Un approccio innovativo che ha obbligato le Organizzazioni (private e pubbliche) ad avviare un progetto prevedendo, fin da subito, gli strumenti e le corrette impostazioni a tutela dei dati personali[5]. Al riguardo il titolare del trattamento - tenendo conto della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento e dei rischi per i diritti e le libertà delle persone fisiche a seguito del trattamento - mette in atto misure tecniche e organizzative adeguate volte ad attuare in modo efficace i principi di protezione dei dati, quali la minimizzazione, e a integrare nel trattamento le necessarie garanzie al fine di tutelare i diritti degli interessati (**Privacy by Design**).

Il titolare deve inoltre garantire che siano trattati solo i dati personali necessari per ogni specifica finalità del trattamento. Tale obbligo, vale per la quantità dei dati personali raccolti, la portata del trattamento, il periodo di conservazione e l'accessibilità. In buona sostanza dette misure debbono garantire, **per impostazione predefinita**, che i dati personali siano accessibili solo a seguito di intervento della persona fisica autorizzata al trattamento e per le specifiche finalità del trattamento medesimo (**Privacy by Default**).

La puntuale interpretazione e gestione degli indicati criteri di privacy risulta fondamentale per una corretta gestione del rischio inerente al trattamento e, di conseguenza, l'approntamento delle misure tecniche e organizzative (anche di sicurezza) che il titolare ritiene di dover adottare per mitigare tali rischi.

Rapporto di lavoro e trattamento dei dati personali dei lavoratori da parte del datore

Uno degli argomenti di maggiore attualità, riguarda il trattamento dei dati personali nei rapporti di lavoro. Al riguardo l'art. 88 del **Regolamento** fa un generale rinvio alla legisla-

zione nazionale di ogni Stato membro ed alla disciplina pattizia[6]. Nello specifico,il legislatore europeo si limita a "sollecitare" i singoli Paesi ad introdurre norme ad "hoc" per assicurare la protezione dei diritti e delle libertà, con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro.

Uno dei capisaldi della normativa europea in materia di privacy è costituito dal fatto che il trattamento dei dati personali deve essere, da un lato, supportato da una **base giuridica** e dall'altro, **formare oggetto di informativa dettagliata all'interessato** anche per metterlo nelle condizioni di esercitare i propri diritti.

Con riguardo al tema in argomento, è di tutta evidenza che il trattamento dei dati personali dei dipendenti, elementi indispensabili per lo svolgimento del rapporto di lavoro, è da considerare di norma lecito, in quanto supportato da due basi legali rappresentate dal **contratto di assunzione** e dagli **obblighi** e dagli **adempimenti** connessi con il rapporto a cui è soggetto il datore di lavoro[7].

Inoltre per espressa previsione normativa[8] non rileva il generale divieto al trattamento dei dati personali "sensibili" di cui all'art. 9, se necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del trattamento o dell'interessato in materia di diritto del lavoro e di sicurezza e protezione sociale, nel rispetto dei diritti fondamentali e degli interessi di ogni singolo lavoratore.

Quindi in ambito lavorativo, il responsabile del trattamento dei dati (in genere il datore di lavoro od un suo delegato) è legittimato ad utilizzare i dati personali dei lavoratori nel rispetto del c.d. principio di **"minimizzazione"** dei dati"[9].

Appare comunque evidente, come già ricordato nei precedenti paragrafi, che la nuova normativa impone una valutazione dinamica della privacy, dovendo porre l'utente al centro di ogni trattamento per garantirgli una tutela effettiva. In tal senso quindi il **Regolamento** ha rappresentato e rappresenta uno stimolo per tutte le organizzazioni (private e pubbliche) a ridisegnare le varie attività correlate alla gestione del personale per elaborare un modello dinamico di trattamento dei dati personali, in ottica di **workflow dei processi lavorativi**, in grado di "garantire" un controllo costante sui flussi, in tutte le fasi del processo, elemento imprescindibile per minimizzare i rischi di un utilizzo non conforme dei dati.

In presenza di tale quadro normativo emerge l'importanza per il datore di stabilire per ogni dipendente quali dati personali è autorizzato a trattare e definirne, nel contempo, le responsabilità, in caso di utilizzo non conforme ed informarlo su eventuali attività aggiuntive di trattamento da parte del titolare (si pensi alla videosorveglianza) e sulle misure di sicurezza e di controllo attuate sugli strumenti di lavoro assegnati (quali ad esempio internet, posta elettronica, telefono, sistemi di rilevazione GPS su veicoli, eventuali sistemi di controllo accessi a mezzo badge di ultima generazione, app su smartphone ed impronte digitali).

In ragione di quanto appena esposto, risulta fondamentale l'elaborazione di una **Privacy Policy** sul trattamento e protezione dei dati personali con la specificazione del corretto utilizzo degli strumenti in dotazione e la identificazione dei comportamenti vietati. Sempre collegate con la Policy le altre due "parole d'ordine": istruzione e formazione. Due obblighi che hanno sfaccettature diverse ma che per certi versi risultano complementari. Infatti il datore, in ottemperanza all'art. 29 del Regolamento, dovrà porre in essere, per dipendenti e collaboratori,specifici percorsi di istruzione e di formazione[10].

È pure di pacifica evidenza che tutte le azioni datoriali debbano essere connotate dalla massima trasparenza anche per consentire al lavoratore, al quale sono obbligatoriamente dovute le informazioni di cui agli artt. 13 e

14 del Regolamento, di azionare i propri diritti di accesso (art. 15) e di richiedere rettifica e cancellazione dei dati trattati (artt. 16 – 20) in maniera non conforme a quanto in precedenza comunicatogli dal datore.

Prescrizioni del Garante Privacy per il trattamento di particolari categorie di dati nei rapporti di lavoro

Il Garante Privacy, con proprio provvedimento n. 146 del 5.06.2019[11], ha dettato le linee guida da seguire per il trattamento di categorie particolari di dati personali nei rapporti di lavoro. In tale categoria rientrano quelli che rivelano l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare dati genetici, dati biometrici, dati relativi alla salute ed all'orientamento sessuale di una persona. Le prescrizioni di interesse per quanto riguarda i rapporti di lavoro sono contenute nel primo capitolo.

Innanzi tutto il provvedimento *de quo* specifica che gli interessati al trattamento, cioè le persone fisiche a cui si riferiscono i dati personali, sono: **(a)** i candidati all'instaurazione dei rapporti di lavoro, anche in caso di curricula, spontaneamente inviati; **(b)** i lavoratori subordinati (con contratto di apprendistato, di formazione, a termine, di lavoro intermittente e di lavoro occasionale), i prestatori di lavoro nell'ambito di un contratto di somministrazione di lavoro o in rapporto di tirocinio, ovvero ad associati anche in compartecipazione; **(c)** familiari o conviventi dei lavoratori di cui al punto precedente per il rilascio di agevolazioni o permessi; **(d)** i consulenti ed i liberi professionisti, gli agenti, rappresentanti ed i mandatari; **(e)** i soggetti che svolgono collaborazioni organizzate dal committente, o altri lavoratori autonomi in rapporto di collaborazione, anche sotto forma di prestazioni di lavoro accessorio; **(f)** le persone fisiche titolari di cariche sociali o altri incarichi nelle società e negli organismi di cui al punto 1.1. del provvedimento qui in trattazione; **(g)** i terzi danneggiati nell'esercizio dell'attività lavorativa o professionale.

Il Garante inoltre precisa modalità e limiti per il trattamento di particolari categorie di dati in costanza di rapporto di lavoro. Viene specificato che il datore di lavoro è legittimato a trattare dati che rivelano: **(1)** le convinzioni religiose o filosofiche ovvero l'adesione ad associazioni od organizzazioni a carattere religioso **solo ed esclusivamente** in caso di fruizione di permessi in occasione di festività religiose o per le modalità di erogazione dei servizi di mensa o, nei casi previsti dalla legge, per l'esercizio dell'obiezione di coscienza; **(2)** le opinioni politiche o l'appartenenza sindacale, o l'esercizio di funzioni pubbliche e incarichi politici, di attività o di incarichi sindacali esclusivamente ai fini della fruizione di permessi o di periodi di aspettativa riconosciuti dalla legge o, eventualmente, dai contratti collettivi anche aziendali nonché per consentire l'esercizio dei diritti sindacali compreso il trattamento dei dati inerenti alle trattenute per il versamento delle quote di iscrizione ad associazioni od organizzazioni sindacali. Inoltre, in caso di partecipazione di dipendenti ad operazioni elettorali in qualità di rappresentanti di lista, il datore non può trattare dati che ne rivelino le opinioni politiche (ad esempio, non deve essere richiesto il documento che designa il rappresentante di lista essendo allo scopo sufficiente la certificazione del presidente di seggio).

Da ultimo, non possono formare oggetto di trattamento i dati genetici di un candidato all'impiego, al fine stabilire l'idoneità professionale, neppure con il consenso dell'interessato,

Particolare attenzione deve essere posta nella trasmissione all'interessato di comunicazioni contenenti categorie particolari di dati. Al ricorrere di tale ipotesi, è **obbligatorio** per il datore utilizzare forme di trasmissione, anche elettroniche, individualizzate. Nel caso in cui si proceda alla trasmissione del documento cartaceo, questo andrà inviato, di regola, in plico

chiuso, salva la necessità di acquisire, anche mediante la sottoscrizione per ricevuta, la prova della ricezione dell'atto.

Inoltre, se per ragioni di organizzazione del lavoro e nell'ambito della predisposizione di turni di servizio, fosse necessario mettere a disposizione a soggetti diversi dall'interessato (ad esempio altri colleghi) dati relativi a presenze e assenze dal servizio, il datore di lavoro non deve esplicitare, nemmeno attraverso acronimi o sigle, le causali dell'assenza dalle quali sia possibile evincere la conoscibilità di particolari categorie di dati quali ad esempio permessi sindacali o dati sanitari.

Si fa da ultimo presente che la mancata ottemperanza alle prescrizioni generali sopra riportate, comporta l'applicazione, ex art. 21 co.5 del D.Lgs.n. 101 del 10.08.2018, di una sanzione amministrativa pecuniaria di importo rilevante. Infatti la medesima può arrivare a 20 milioni di euro (o fino al 4% del fatturato mondiale annuo dell'esercizio precedente, se superiore) in applicazione dell'art. 83 par.5 del **Regolamento**.

Alcuni anni fa il presidente **Soro**, intervenendo ad un convegno, ha sottolineato che la protezione dei dati personali in un presente, e soprattutto in un futuro sempre più digitale, *"significa innanzitutto proteggere noi stessi e le nostre vite e affermare il principio secondo il quale le esigenze del mercato e delle aziende multinazionali che vi operano non devono necessariamente prevalere in caso di conflitto con i diritti dei cittadini"*[12].

Ebbene, in una società dove la raccolta massificata di dati aumenta in modo esponenziale la loro protezione diventa un elemento vitale. I rischi sono comunque tanti. Le norme contenute nel Regolamento, anche se ad una prima lettura possono apparire di difficile comprensione, danno una prima importante risposta a livello comunitario e rappresentano una grande opportunità per tutte le Organizzazioni pubbliche e private.

Il motivo è presto detto: da un lato si dà valore ai dati personali ed alla loro protezione e, dall'altro il tutto potrebbe funzionare da "innesco" per fare in modo che ognuno diventi veramente "Garante" dei propri dati personali e della propria privacy.

(Continua sul prossimo numero)

Note

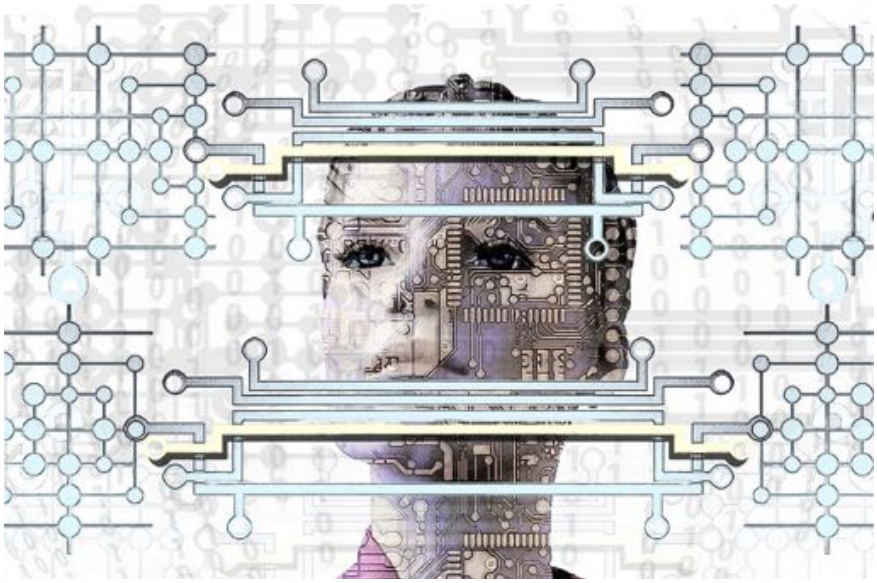
[1] Legaldesk: "Diritto alla riservatezza: riconoscimento ed evoluzione normativa" dell'Avv. Fabrizio Corona. Gli eredi di Enrico Caruso chiesero al giudice il ritiro dal mercato di un film perché ritenuto lesivo della riservatezza e della sfera privata del famoso tenore;

[2] La legge in questione è la n. 675 del 31.12.1996 e conteneva norme a tutela delle persone e di altri soggetti rispetto al trattamento dei dati personali;

[3] Ad onor del vero già nello "Statuto dei lavoratori" approvato con legge 20.05.1970 n. 300 vennero inserite alcune previsioni per limitare il potere di controllo del datore sui propri lavoratori, a tutela della privacy di questi ultimi e vietando di fatto controlli lesivi dei loro diritti inviolabili;

[4] Accountability è un termine composto da "to account" ed "ability". Il primo è un verbo che significa "rendere conto" o "dare conto". Il secondo è un sostantivo che può tradursi come "essere in grado di". In definitiva Accountability identifica in modo puntuale una "responsibility for outcome" cioè una specifica "responsabilità di risultato" che grava, per la materia qui in

trattazione, sul titolare del trattamento che deve essere sempre in grado di dimostrare le procedure poste in essere ed i risultati ottenuti. In definitiva il principio di accountability, come ben espresso da Stefano Aterno in un recente articolo pubblicato su www.agendadigitale.eu, può essere ben inteso come "un faro nella notte" capace di fornire la chiave di lettura rispetto a certe situazioni di criticità;



[5] "Privacy by design e by default" articolo di Bruno Saetta. Pubblicato il 25.05.2018 su https://protezionedatipersonali.it;

[6] Il par.1 dell'art.88 del Regolamento si premura di specificare che i singoli Paesi possono prevedere "con legge o tramite contratti collettivi, norme più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro". Il par.2 del medesimo articolo entra nel dettaglio e stabilisce che le indicate norme debbono includere anche "misure appropriate e specifiche a salvaguardia della dignità umana, degli interessi legittimi e dei diritti fondamentali degli interessati, in particolare per quanto riguarda la trasparenza del trattamento, il trasferimento di dati personali nell'ambito di un gruppo imprenditoriale o di un gruppo di imprese che svolge un'attività economica comune e i sistemi di monitoraggio sul posto di lavoro";

[7] L'art. 6 del Regolamento, per quanto qui in commento, riconosce come lecito il trattamento solo se lo stesso è necessario per: (a) l'esecuzione di un contratto di cui l'interessato è parte o all'esecuzione di misure precontrattuali adottate su richiesta dello stesso; (b) adempiere ad un obbligo legale al quale è soggetto il titolare del trattamento;

[8] Art. 9, par. 2 lett. b) del Regolamento che testualmente stabilisce che il generale divieto al trattamento dei dati personale non si applica se: "il trattamento è 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";

[9] Per la gestione del rapporto di lavoro la liceità al trattamento è automatica solo se i dati di cui trattasi sono "adeguati, pertinenti, e limitati a quanto necessario, rispetto alle finalità per le quali sono trattati" (art. 5 par.1 lett. c). Si pensi ad esempio alla elaborazione dei prospetti paga, dove il trattamento di alcuni dati personali risulta indispensabile per assolvere ad obblighi di legge.

[10] Il Regolamento stabilisce che il lavoratore deve ricevere specifica indicazione ed autorizzazione in merito al trattamento dei dati personali (art. 29) ed alle specifiche misure di sicurezza da porre in essere per evitare utilizzi non conforme (art. 32);

[11] Il provvedimento, pubblicato sulla GU, Serie Generale, n. 176 del 29 luglio 2019, riguarda tutti i soggetti che, a vario titolo (titolare/responsabile del trattamento), effettuano trattamenti per l'instaurazione, la gestione e l'estinzione del rapporto di lavoro: dai datori di lavoro, al medico competente in materia di salute e sicurezza sul lavoro (che opera in qualità di libero professionista o di dipendente del datore di lavoro o di strutture convenzionate), dalle agenzie per il lavoro, ai consulenti del lavoro e liberi professionisti fino al rappresentante dei lavoratori per la sicurezza;

[12] "La protezione dei dati bussola nel futuro digitale". Roma 21.10.2015. Intervento di Antonello Soro,Presidente del Garante per la protezione dei dati personali.

---

[*] Dorina Cocca in servizio presso la sede di Rovigo dell'Ispettorato Territoriale del Lavoro di Ferrara Rovigo. Tiziano Argazzi giornalista, esperto in comunicazione e in materia lavoristica.