Tra GDPR e Statuto dei Lavoratori. I profili di privacy del lavoratore sotto la lente del Garante

02/10/2023

PRIVACY E CYBERSICUREZZA, DIRITTO DEL LAVORO E PREVIDENZA, SOCIETÀ, PROSPETTIVE.

Gaspare Roma
Jacopo Piemonte
Adriano Garofalo
Federico Aluigi

I. Quadro generale

Nell'attuale contesto dell'era digitale, l'intersezione tra la protezione dei dati personali e i diritti dei lavoratori riveste un ruolo di crescente importanza all'interno degli ambienti lavorativi. Le tecnologie avanzate hanno rivoluzionato la raccolta, l'elaborazione e la conservazione dei dati, offrendo nuove opportunità per l'ottimizzazione delle attività aziendali e la gestione delle risorse umane. Tuttavia, questo progresso tecnologico pone sfide e questioni giuridiche complesse. In particolare, il Regolamento Generale sulla Protezione dei Dati (*General Data Protection Regulation*, GDPR) dell'Unione Europea, operando una "rivoluzione copernicana" da un punto di vista giuridico e sociale, si è affermato come un pilastro fondamentale nella tutela della *privacy* individuale e ha introdotto importanti implicazioni nel rapporto tra datore di lavoro e lavoratore subordinato.

Più particolarmente, a guadagnare spesso gli onori della cronaca è il tema del controllo a distanza dei lavoratori, ove il rispetto della procedura prevista dalla legge 20 maggio 1970, n. 300 (Statuto dei Lavoratori) e dal Decreto legislativo 30 giugno 2003, n. 196 (Codice della Privacy) costituisce un requisito essenziale per la correttezza dei trattamenti dei dati personali dei lavoratori in azienda.

Il nucleo essenziale sul piano giuslavoristico è costituito dall'articolo 4,

comma 1, dello Statuto dei Lavoratori[1], ai sensi del quale, per poter utilizzare gli impianti audiovisivi e gli altri strumenti dai quali derivi la possibilità di controllo a distanza dell'attività dei lavoratori, deve sussistere alternativamente una delle seguenti condizioni: *i)* ragioni organizzative e produttive; *ii)* sicurezza dei luoghi di lavoro; *iii)* tutela del patrimonio aziendale. Inoltre, qualora ricorra almeno uno di detti requisiti, occorre ulteriormente ottenere il previo accordo con le Organizzazioni Sindacali o, in mancanza di tale accordo, la previa autorizzazione da parte della sede territoriale dell'Ispettorato Nazionale del Lavoro (I.T.L.).

Sul piano della regolamentazione *privacy* rilevano invece i già citati GDPR e Codice della privacy.

L'intersezione delle due normative configura una procedura di garanzia tale per cui il datore di lavoro (titolare del trattamento dei dati), prima di implementare strumenti da cui possa derivare un controllo anche solo potenziale o indiretto dell'attività di lavoro, è tenuto a osservare una serie di prescrizioni preliminari. In primo luogo, occorre informare il lavoratore (interessato al trattamento dei dati) circa le modalità d'uso degli strumenti e di effettuazione dei controlli come indicato dall'articolo 4, comma 3, dello Statuto dei Lavoratori, nonché circa gli altri aspetti richiamati dall'articolo 13 del GDPR. In secondo luogo, è richiesto esaminare se sia necessario procedere alle valutazione dell'impatto *privacy* degli strumenti di lavoro sui lavoratori dipendenti ai sensi dell'articolo 4 dello Statuto dei Lavoratori e dell'articolo 35 del GDPR.

Si consideri inoltre che l'interazione tra le suddette normative configura l'esposizione ad una responsabilità "a doppio binario" tale per cui da una parte, sussiste una responsabilità penale del datore di lavoro ai sensi dell'articolo 38 dello Statuto dei Lavoratori[2]; e dall'altra, vi è una responsabilità amministrativa dell'ente ai sensi dell'articolo 83 del GDPR[3].

---

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

[2] Specificamente, ai sensi dell'art. 171 del Codice della *privacy*, la violazione delle disposizioni in materia di controlli a distanza (articolo 4, comma 1, dello Statuto dei Lavoratori) è punita con la sanzione prevista dall'articolo 38 dello Statuto. In particolare, si esplicita come "… *sono punite, salvo che il fatto non costituisca più grave reato, con l'ammenda da euro 154 a euro 1.549 o con l'arresto da 15 giorni ad un anno. Nei casi più gravi le pene dell'arresto e dell'ammenda sono applicate congiuntamente. Quando, per le condizioni economiche del reo, l'ammenda stabilita nel primo comma può presumersi inefficace anche se applicata nel massimo, il giudice ha facoltà di aumentarla fino al quintuplo. Nei casi previsti dal secondo comma, l'autorità giudiziaria ordina la pubblicazione della sentenza penale di condanna nei modi stabiliti dall'articolo 36 del Codice penale …*".

[3] Specificamente, la responsabilità dell'ente è stata fatta derivare dalla violazione dell'articolo 114 del Codice della privacy che a sua volta richiama l'articolo 4 dello Statuto dei lavoratori. La cornice

II. Il provvedimento del Garante

Su queste premesse, è di particolare rilievo un provvedimento del Garante per la Protezione dei Dati Personali (Garante) del 1° giugno 2023[4], che è intervenuto su asserite molteplici violazioni della *privacy* da parte di una società che aveva installato tre distinti apparati tecnologici ed in particolare: *(i)* un sistema di allarme la cui attivazione e disattivazione si basava sull'uso delle impronte digitali; *(ii)* un impianto di videosorveglianza; e *(iii)* un applicativo per la geolocalizzazione di alcuni lavoratori.

In tale procedimento il Garante ha rilevato profili di illegittimità[5] in relazione all'utilizzo di tali sistemi e ha, *inter alia*, comminato alla società una sanzione amministrativa pari a 20.000 euro ai sensi dell'articolo 83 del GDPR.
Di seguito esamineremo in maniera partita le conclusioni raggiunte dal Garante in relazione ai singoli sistemi.

i) Il sistema di allarme

In primo luogo, il Garante ha posto sotto la propria "lente di ingrandimento" un particolare sistema di allarme utilizzato dalla Società che adottava rilevatori di impronte digitali e registrava attivazioni e disattivazioni dell'allarme, conservando le impronte dei dipendenti abilitati all'utilizzo di detto sistema.

In sostanza, dunque, il Garante ha lamentato che con quel sistema, in teoria finalizzato ad azionare allarmi in caso di intrusioni di terzi presso la sede societaria, la società operava invece un illecito trattamento di dati particolari dei dipendenti. Inoltre, si è contestato che non fosse stata data la necessaria informativa.

Nelle difese della società si è sostenuto che la rilevazione delle impronte digitali fosse avvenuta facendo riferimento alle linee guida fornite dal Garante e che, in proposito, fosse comunque stata data una comunicazione orale alle risorse aziendali sulle peculiarità del sistema.

Sul punto, l'Autorità ha osservato che tale trattamento (di regola vietato poiché compreso nella categoria dei *c.d.* dati particolari[6]) sarebbe stato consentito esclusivamente in presenza di una delle condizioni indicate dall'articolo 9, par. 2 del Regolamento. In altri termini, il sistema avrebbe dovuto essere "*… 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 …*"[7].

In tal senso, il Garante non ha ritenuto ricorrere il suddetto elemento nel caso di specie, posto che l'utilizzo dei dati biometrici sarebbe invece stato meramente finalizzato all'attivazione e disattivazione del sistema di allarme[8].

---

edittale in tale caso è stabilita dall'articolo 83 del GDPR che a seconda della gravità della violazione prevede come tetto massimo della sanzione il 2% del fatturato annuo dell'esercizio precedente o il 4 % del fatturato annuo dell'esercizio precedente.

[4] Garante per la Protezione dei Dati Personali, Provvedimento del 1° giugno 2023, doc. web n. 9913830.
Per il testo integrale del Provvedimento si veda il seguente LINK.

[5] Con tale provvedimento, l'Autorità Garante ha nuovamente rivendicato il proprio potere di far rispettare la normativa giuslavoristica sul controllo a distanza dei lavoratori sulla base dell'articolo 114 del Codice della privacy.

[6] Specificamente, l'articolo 9, par. 1, del GDPR, statuisce che "*è vietato trattare dati personali che rivelino l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o filosofiche, o l'appartenenza sindacale, nonché trattare 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.*".

[7] Si veda l'articolo 9, par. 2, lettera *b*) del GDPR.

[8] Più particolarmente, il Garante statuisce che *"… affinché, quindi, il trattamento dei dati biometrici, in ambito lavorativo, sia consentito, la fattispecie deve innanzitutto rientrare nelle ipotesi in cui il trattamento sia "necessario per assolvere gli obblighi ed esercitare i diritti specifici del titolare del*

Inoltre, si è ritenuto che la comunicazione orale nei confronti dei lavoratori circa la finalità e l'utilizzo del sistema non fosse sufficiente; al contrario il GDPR chiarisce all'articolo 12 che "*… il titolare del trattamento adotta misure appropriate per fornire all'interessato tutte le informazioni di cui agli articoli 13 e 14 […] in forma concisa, trasparente, intelligibile e facilmente accessibile […]. Le informazioni sono fornite per iscritto o con altri mezzi, anche se del caso, con mezzi elettronici …*".

Alla luce di quanto sopra si è dunque riconosciuta l'illegittima installazione del sistema di trattamento dei dati biometrici in parola.

ii) Il sistema di videosorveglianza

Il Garante ha contestato alla società anche l'utilizzo di un apparecchio preposto alla videosorveglianza.

In questo caso, era fuor di dubbio che la società non avesse dato corso alla specifica procedura di garanzia descritta *ex* articolo 4 dello Statuto dei Lavoratori, volta ad ottenere, in caso di assenza di rappresentanze sindacali aziendali (come nella fattispecie in esame), il rilascio di una apposita autorizzazione da parte dell'Ispettorato del Lavoro. Inoltre, non risultavano essere stati apposti cartelli informativi indicanti la presenza del sistema.

A riguardo, la Società si è difesa asserendo in primo luogo che l'autorizzazione non sarebbe stata necessaria. Il sistema sarebbe infatti stato installato in risposta ad un furto ed utilizzato per soli scopi di sicurezza al fine di proteggere il patrimonio aziendale. Non si sarebbe dunque potuto registrare alcun controllo sui lavoratori (risultando dunque non necessaria l'autorizzazione dell'ITL). Inoltre, non vi sarebbe nemmeno stata necessità di affiggere in società apposita cartellonistica dato che la telecamera avrebbe inquadrato solamente la *reception*.

All'esito dell'istruttoria, il Garante ha tuttavia accertato che tali apparecchi erano idonei ad operare un controllo a distanza dell'attività lavorativa. Si è infatti rilevato che il legale rappresentante della società e alcuni suoi famigliari potevano visionare in diretta via *app* quanto ripreso dalla telecamera[9]. Si è dunque concluso che, essendo il sistema idoneo ad operare un controllo dei lavoratori, sarebbe stato necessario ottenere l'autorizzazione dell'ITL per la sua installazione. Del pari, il Garante ha ribadito che anche in questo caso sarebbe stato necessario fornire apposita informativa (a nulla rilevando che il sistema inquadrasse solo certe aree della sede societaria).

Alla Società è stato dunque intimato il divieto di trattamento dei dati mediante il sistema di videosorveglianza fino a corretta implementazione della procedura di garanzia prevista dallo Statuto dei Lavoratori[10].

iii) Il tracciamento della posizione geografica dei lavoratori

Il Garante ha infine contestato l'utilizzo di un'applicazione che, installata sullo *smartphone* dei lavoratori, registrava la loro posizione geografica. Anche in

trattamento o dell'interessato in materia di diritto del lavoro [e della sicurezza sociale e protezione sociale]" (v. pure art. 88, par. 1, Regolamento). Tale elemento non ricorre nel caso di specie, considerato che il trattamento dei dati biometrici era finalizzato all'attivazione e alla disattivazione di un sistema di allarme installato presso la sede legale della Società …".

[9] Più particolarmente, il Garante riporta che *"… È stato altresì verificato che il sistema può captare anche i suoni, oltre alle immagini, e consente la registrazione di quanto ripreso. Attraverso l'applicativo è infatti possibile ammonire verbalmente, attraverso lo speaker della telecamera.*
È stato inoltre accertato che l'accesso al sistema di videosorveglianza è consentito a quattro account, dei quali uno risulta intestato alla moglie del rappresentante legale della società, uno al rappresentante legale della Società e due ai figli di quest'ultimo …".

[10] La condotta tenuta dalla società è stata considerata lesiva del principio di liceità del trattamento (si veda l'articolo 5, par. 1, lettera a) del GDPR) in relazione all'articolo 114 del Codice della privacy e dell'articolo 88 del GDPR quanto alla disciplina applicabile in materia.

questo caso si è asserito che ciò avrebbe costituito un indebito controllo a distanza dei lavoratori in assenza di necessaria autorizzazione ITL.

La società si è difesa sostenendo che detto tracciamento sarebbe avvenuto solo quando l'*app* era attiva o in uso e al solo fine di garantire la gestione degli interventi tecnici che si espletavano esternamente alla sede aziendale, specificamente per una corretta contabilizzazione dei servizi così forniti "… *onde evitare contestazioni in sede di fatturazione* …"[11].

Anche in tal caso, come sopra, il Garante ha rilevato l'insussistenza delle condizioni previste dall'articolo 4 dello Statuto dei Lavoratori concludendo per l'illegittimità dell'installazione del sistema.

Alla luce di tutto quanto sopra, il Garante ha disposto il divieto del monitoraggio continuo della posizione dei dipendenti attraverso l'*app* in parola fino ad ottenimento di autorizzazione da parte dell'ITL.

III. Considerazioni conclusive

Il provvedimento emesso dal Garante si mostra come eloquente esempio della complessa interazione tra GDPR e diritto del lavoro. L'attenzione rivolta al caso esaminato evidenzia l'importanza della corretta gestione dei dati personali nell'ambito giuslavoristico e sottolinea il difficile equilibrio esistente tra la protezione dei diritti dei lavoratori e le legittime esigenze aziendali[12].

Parallelamente, il provvedimento solleva questioni riguardo tale bilanciamento: la necessità di monitorare l'accesso fisico alle strutture aziendali o di garantire un ambiente di lavoro sicuro, si scontra infatti con temi relativi alla sorveglianza e al trattamento eccessivo dei dati personali dei lavoratori. Inoltre, le osservazioni del Garante ed i limiti imposti alle attività di monitoraggio dei datori di lavoro, sebbene aventi una genesi estranea al contesto normativo giuslavoristico, nondimeno potrebbero avere un impatto non da poco anche in un'ottica contenziosa lavoristica. Infatti, la violazione od anche solo la non corretta puntuale applicazione delle disposizioni (normative o regolamentari) in materia di trattamento dei dati personali, potrebbe inficiare la raccolta e soprattutto l'utilizzo di dati ed informazioni ottenute dal datore di lavoro con l'obiettivo di gestire correttamente (ed efficacemente) i rapporti di lavoro, limitando, in tal modo, il diritto costituzionale dell'imprenditore ad esercitare liberamente la propria iniziativa economica privata (art. 41 Cost.). A tale osservazione si potrebbe tuttavia obiettare che, già in Costituzione, il diritto di esercitare liberamente l'iniziativa economica privata è subordinato al rispetto di altri diritti pur costituzionalmente riconosciuti, quali quelli alla salute, all'ambiente, alla sicurezza, alla libertà ed alla dignità umana, questi ultimi, appunto, oggetto di specifica tutela da parte del Garante.

Da tutto quanto sopra, si evidenzia come risulti di cruciale importanza: *(i)* una pianificazione oculata nell'implementazione di sistemi di videosorveglianza e di rilevamento della posizione (tenendo a mente la necessità di adottare ove necessario la procedura di garanzia prevista dallo Statuto dei Lavoratori); *(ii)* l'effettuazione di

[11] Più particolarmente, il Garante riporta che *"… attraverso il predetto applicativo è risultata tracciata, tramite GPS, la posizione del dispositivo mobile sul quale viene scaricato l'applicativo predetto, in modo continuativo quando il tecnico usa l'applicativo […], comunque all'interno del periodo temporale compreso dal lunedì al venerdì, dalle 8 alle 18. Oltre al dato relativo alla posizione geografica, risultano essere stati raccolti anche il dato relativo all'ora e alla data della rilevazione della posizione stessa, tra l'altro anche dati relativi a periodi molto risalenti nel tempo (2014). È stato inoltre accertato che la Società raccoglie anche gli specifici dati relativi alla posizione geografica, alla data e all'ora della chiusura dell'intervento svolto dal tecnico.*
In tal modo risulta tracciata, in modo continuativo, la posizione del lavoratore nello svolgimento della propria attività lavorativa quando l'applicativo risulta in uso …".
[12] Per approfondimenti si veda il nostro precedente contributo al seguente LINK.

un’analisi di tali sistemi per verificare che siano conformi ai principi sanciti dal GDPR; e *(iii)* un preventivo accurato bilanciamento, da parte dell’imprenditore, tra il proprio diritto costituzionalmente garantito al libero esercizio dell’iniziativa economica privata e quello dei lavoratori, altrettanto costituzionalmente garantito, alla libertà ed alla dignità umana (che la normativa in tema di protezione dei dati personali mira a tutelare.

Gaspare Roma

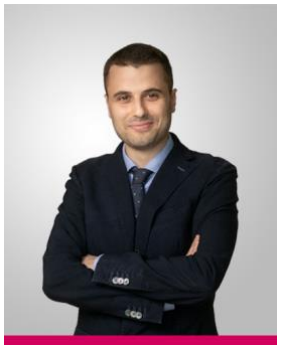
PARTNER

g.roma@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Jacopo Piemonte

ASSOCIATE

j.piemonte@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 – Milano
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles



Adriano Garofalo

ASSOCIATE

a.garofalo@dejalex.com
+39 02 72554.1
Via San Paolo 7
20121 - Milano

Federico Aluigi

ASSOCIATE

f.aluigi@dejalex.com
+32 (0)26455670
Chaussée de La Hulpe 187
1170 - Bruxelles