LABOR Il lavoro nel diritto

Pacini Giuridica

L'Autorità Garante per la protezione dei dati personali sanziona la Regione Lazio per l'illecito trattamento di dati relativi alle e-mail di propri dipendenti

di A. Ciracò - *11 Febbraio 2023*

Con l'ordinanza ingiunzione n. 409 del 01.12.2022, pronunciata dall'Autorità Garante per la protezione dei dati personali, è stata condotta un'indagine relativa al rispetto, da parte della Regione Lazio, della normativa in materia di *data protection* (intendendosi con tale termine l'insieme di principi, nazionali e sovranazionali, che si occupano di protezione e libera circolazione di dati a carattere personale) nel contesto lavoristico.

Lo scrutinio dell'Autorità ha investito la liceità del trattamento di dati personali relativi all'utilizzo della posta elettronica assegnata ad alcuni dipendenti regionali.

La questione riveste un'importanza centrale, ad opinione di chi scrive, poiché mostra, ancora una volta, la necessità impellente di trovare soluzioni giuridiche ed applicative che realizzino quel bilanciamento tra diritti dei lavoratori ed esigenze datoriali, in relazione all'uso di strumenti tecnologici.

La materia è complessa e definita, oltre che da norme di legge, da una corposa serie di atti c.d. di *soft law*, di Autorità interne e sovranazionali.

Evidentemente, la tematica è articolata e richiede un approfondimento, che esula dalla presente trattazione ma, ad essa, è stato doveroso far cenno, onde collocare correttamente il nucleo centrale delle riflessioni che di seguito verranno esposte.

La vicenda sottoposta al vaglio dell'Autorità

Il caso trae origine dalla segnalazione, presentata dal sindacato autonomo Fedirets, circa presunte indebite verifiche poste in essere dall'amministrazione regionale, sui flussi di posta elettronica in uscita dagli account istituzionali assegnati ai legali dell'avvocatura. La ragione che avrebbe dato luogo ai controlli, secondo la Regione Lazio, risiedeva nell'esigenza di verificare presunte rivelazioni di segreti d'ufficio realizzate dagli intestatari degli account istituzionali.

Questa la ricostruzione dei fatti e delle argomentazioni più significative avanzate dall'Amministrazione regionale a difesa del proprio operato:

1. in qualità di titolare del trattamento, per il tramite di una società IT – correttamente designata responsabile del trattamento – l'Ente effettuava la raccolta del traffico delle caselle di posta elettronica assegnate ai dipendenti aziendali e la conservazione dei dati per 180 giorni, per ragioni di sicurezza informatica,

2. il sistema era impostato affinché i dati trattati fossero limitati ai c.d. dati esteriori o metadati costituiti da giorno, ora, mittente, destinatario, oggetto e dimensione delle e-mail, non essendo possibile accedere né al contenuto, né ad eventuali allegati,

3. i controlli erano stati effettuati ex post, sull'indizio di presunti comportamenti illeciti dei lavoratori e non integravano una forma di monitoraggio dell'attività,

4. l'organizzazione aveva fornito ai lavoratori un'informativa *privacy* contemplando la possibilità di verificare *«nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia)»*.

Il quadro giuridico di riferimento

Prima di analizzare i rilievi dell'Autorità e per meglio comprendere la vicenda occorre ricostruire la cornice normativa nell'alveo della quale la tematica si inscrive. Ecco le principali disposizioni che assumono valenza:

1. 6 e 9 del Regolamento UE 2016/679 (di seguito anche GDPR), i quali si occupano di descrivere le condizioni di liceità del trattamento dei dati, rispettivamente, comuni e particolari,

2. 88 GDPR, che conferisce agli Stati membri la possibilità di prevedere norme più specifiche, per innalzare il livello di tutela dei diritti e delle libertà, con riguardo al trattamento dei dati personali dei dipendenti nell'ambito del rapporto di lavoro,

3. 113 e 114 del d.lgs. 30 giugno 2003 n.196 (anche detto codice privacy), che rimandano alla disciplina contenuta negli artt.4 e 8 della legge 20 maggio 1970, n.300 (nel prosieguo anche Statuto dei lavoratori) e nell'art.10 del d.lgs. 10 settembre 2003, n.276.

Come anticipato, ad integrazione e specificazione della normativa sopra descritta si pongono numerosi atti di *soft law:* le raccomandazioni e linee guida dell'European Data Protection Board (già Working Party 29), le linee guida e atti assimilabili adottati dall'Autorità Garante nazionale, ma anche, circolari del Ministero e dell'Ispettorato del lavoro.

Sicuramente di tutte le previsioni fin qui citate, l'art.4 dello Statuto dei lavorati riveste una importa centrale. La norma, rubricata *«Impianti audiovisivi e altri strumenti di controllo»*, consente al datore di lavoro di utilizzare sistemi tecnologici dai quali derivi, anche, la possibilità di controllo a distanza dell'attività lavorativa, delineando i limiti e le modalità di tale potere. In particolare, i 3 commi che compongono la disposizione prevedono:

1. i c.d. «controlli preterintenzionali», ammessi purché gli strumenti siano impiegati per perseguire tassative finalità (esigenze organizzative e produttive, sicurezza sul lavoro, tutela del patrimonio aziendale) e, sempreché, in precedenza, sia stato concluso un accordo sindacale o ottenuta un'autorizzazione dall'ispettorato del lavoro,

2. i controlli «leciti ab origine»: ammessi, in assenza dei requisiti di cui al comma 1, purché realizzati mediante strumenti funzionali a rendere la prestazione o finalizzati alla registrazione degli accessi e delle presenze,

3. la possibilità di utilizzare le informazioni raccolte, ai sensi dei due commi precedenti, a tutti i fini connessi al rapporto di lavoro, purché siano rispettati gli obblighi informativi circa

le modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto della normativa *data protection*.

Non sfugge, dunque, che ogni datore di lavoro è chiamato a comprendere se gli strumenti tecnologici che vorrà utilizzare ricadano nell'ambito di applicazione del comma 1 o del comma 2. Solo a valle di tale accertamento potranno essere individuati correttamente gli adempimenti necessari a garantire la *compliance* alla normativa.

La Regione Lazio, sul punto, ha sostenuto che i controlli effettuati non potessero essere ricondotti alla disciplina del comma 1 dell'art.4 dello Statuto dei lavoratori, dal momento che gli account di posta elettronica assegnati ai dipendenti erano «strumenti per rendere la prestazione lavorativa».

I rilievi dell'Autorità Garante

Al termine dell'istruttoria condotta, il Garante notificava alla Regione Lazio l'avvio di un procedimento, rilevando che il trattamento era stata realizzato:

1. in maniera non conforme ai principi di: «liceità, correttezza e trasparenza», «limitazione della conservazione» e «responsabilizzazione»,

2. in assenza di base giuridica e in maniera difforme dalla disciplina di settore in materia di controlli a distanza e di raccolta di dati non pertinenti all'attività lavorativa,

3. omettendo di fornire agli interessati una informativa adeguata,

4. violando i principi di *privacy by design* e *by default*,

5. omettendo di effettuare una valutazione di impatto privacy.

Le contestazioni sopra esposte meritano di essere approfondite richiamando le valutazioni effettuate dall'Autorità e poste a base delle censure. Così, dal provvedimento è possibile ricavare le seguenti considerazioni:

1. la posta elettronica, i metadati e gli allegati sono forme di corrispondenza assistite da specifiche garanzie di segretezza, che ricevono tutela, finanche costituzionale. Di talché, nel contesto lavorativo esiste una legittima aspettativa di riservatezza in relazione alla corrispondenza. Non è un caso, infatti, che i controlli effettuati dalla Regione abbiano portato a esaminare e-mail indirizzate a rappresentanti di specifiche sigle sindacali, fornendo al datore di lavoro, dunque, indicazioni su una circostanza, l'appartenenza sindacale del lavoratore, cui l'ordinamento accorda una particolare tutela;

2.la gestione dei dati esteriori (o metadati), definiti l'*envelope* del messaggio, e la loro conservazione possono essere giustificate da ragioni di sicurezza informatica, purchè la conservazione sia limitata a 7 giorni. Una conservazione più lunga, infatti, oltre che violare il principio di limitazione della conservazione (art.5, par.1, lett. e GDPR) sfugge all'applicazione del comma 2 dell'art.4 dello Statuto dei lavoratori, dovendo ricadere nell'ambito del comma 1. In particolare, nel provvedimento si legge che: «*per scelta espressa del legislatore, solo gli strumenti preordinati, anche in ragione delle caratteristiche tecniche di configurazione, alla registrazione degli accessi e delle presenze e allo svolgimento della prestazione non*

soggiacciono ai limiti e alle garanzie di cui al primo comma [art.4 Statuto dei lavoratori], *in quanto funzionali a consentire l'assolvimento degli obblighi che discendono direttamente dal contratto di lavoro, vale a dire, la presenza in servizio e l'esecuzione della prestazione lavorativa»*. Mentre se, come nel caso in commento, i metadati sono raccolti in modo generalizzato e preventivo e conservati per un tempo molto lungo, essi diventano funzionali ad assolvere una diversa finalità, quella della tutela dell'integrità del patrimonio informativo del titolare e sono riconducibili al comma 1 dell'art.4 dello Statuto dei lavoratori, richiedendo, come abbiamo visto, che il datore di lavoro compia una serie di valutazioni e di adempimenti specifici;

3. quanto alla supposta liceità del trattamento invocata dalla Regione per aver effettuato controlli sul flusso di e-mail successivi alle presunte rivelazioni di segreto (c.d. ex post), rileva il Garante che il trattamento ha avuto inizio con la raccolta dei dati che, per essere lecita, deve avvenire nel rispetto dei principi generali di cui al GDPR e delle garanzie richieste dalla normativa lavoristica. Ne consegue che, qualunque trattamento, ulteriore e/o successivo, debba considerarsi effettuato in violazione degli artt. 5, par.1, lett. a), 6 e 88, par.1 GDPR e 113-114 codice privacy;

4. Una informativa che, come quella adottata dall'Ente reciti: «*ci riserviamo di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei nostri sistemi informatici e di telefonica»*, non presenta tutti i requisiti di legge e non risulta idonea ad assolvere agli obblighi informativi posti a presidio del diritto alla autodeterminazione dei lavoratori, i quali devono essere edotti, prima che il trattamento abbia inizio, delle caratteristiche dello stesso, tra le quali si annoverano, con una rilevanza particolare, la base giuridica ed il periodo di conservazione dei dati.

L'ordinanza ingiunzione, prendendo atto che le dichiarazioni e argomentazioni rese dalla Regione non abbiano consentito di superare i rilievi notificati con l'atto di avvio del procedimento, commina alla PA una sanzione pecuniaria di importante valore (100.000,00 euro), ordinando altresì di limitare il trattamento, vietando il compimento di operazioni ulteriori, e di comunicare, entro 30 giorni, le azioni intraprese per la messa in conformità del sistema.

Conclusioni

Ebbene, quanto sin qui descritto conferma che la protezione dei dati personali sia una materia «trasversale», che investe tutti gli ambiti del diritto imponendo, nel contesto lavoristico, alla parte datoriale una piena consapevolezza sull'uso di strumenti tecnologici e sulle loro implicazioni; ciò assumendo rilevanza, sia sotto il profilo della fisiologia del rapporto, richiedendo al datore di lavoro uno sforzo di trasparenza e di informazione verso i lavatori, che della patologia, visto che l'uso delle informazioni raccolte, in maniera non conforme, ne limita fortemente l'utilizzabilità.

Le prescrizioni imposte costituiscono un ulteriore elemento di riflessione posto che, oltre l'ammontare della sanzione pecuniaria – di certo non di poco valore – l'Autorità ha imposto all'Ente di arrestare le operazioni di trattamento censurate e di pianificare azioni e misure correttive, in un termine molto breve. In questa occasione, il perimetro dei rilievi è stato limitato alla raccolta, elaborazione e conservazione dei soli flussi di posta elettronica, ma

l'uso di strumenti tecnologici spesso è deputato ad assolvere a finalità ben più penetranti: alla gestione delle reti informatiche, al funzionamento di macchinari, al lavoro da remoto, alle attività di recruitment, solo per fare alcuni esempi. Dunque, la necessità di effettuare valutazioni preliminari e consapevoli costituisce per qualunque datore di lavoro un fattore imprescindibile, onde evitare rischi, non solo di sanzioni pecuniarie ma, soprattutto, di sospensioni o arresti delle attività.

E che un'opera di bilanciamento tra diritti dei lavoratori ed interessi datoriali sia necessaria e non più rinviabile lo mostra la velocità con cui l'uso di strumenti tecnologici, sempre più avanzati, si sta affermando, anche nel contesto delle relazioni industriali. Basti pensare alla diffusione di software di rilevazione delle presenze che usano la biometria, di tool per la selezione del personale basati su algoritmi di intelligenza artificiale, di sistemi IoT che, migliorando il tracciamento della produzione, indirettamente monitorano l'attività lavorativa. Questi solo alcuni esempi.

Ciò che occorre fare, per affrontare le nuove sfide, è individuare soluzioni giuridiche, tecnologiche e, soprattutto, operative capaci di contemperare le diverse esigenze in campo.

Arianna Ciracò, avvocato in Prato

Visualizza il documento: Garante per la Protezione dei dati personali, 1° dicembre 2022, n. 409