Ordinanza di ingiunzione nei confronti di Regione Lazio - 1 dicembre 2022 [9833530]

VEDI ANCHE: comunicato del 19 dicembre 2022

[doc. web n. 9833530]

Ordinanza di ingiunzione nei confronti di Regione Lazio - 1 dicembre 2022

Registro dei provvedimenti
n. 409 del 1 dicembre 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il cons. Fabio Mattei, segretario generale;

VISTO il 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" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al 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 (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

Vista la documentazione in atti;

Viste le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del Regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'ufficio del Garante per la protezione dei dati personali, doc. web n. 1098801;

Relatore il prof. Pasquale Stanzione;

PREMESSO

1. Introduzione.

Con una segnalazione presentata ai sensi dell'art. 144 del Codice, il sindacato autonomo Fedirets

(Federazione Dirigenti e Direttivi Enti Territoriali e Sanità) ha rappresentato che la Regione Lazio (di seguito, la "Regione"), a fronte della presunta rivelazione da parte di propri dipendenti di notizie d'ufficio, che avrebbero dovuto rimanere segrete, avrebbe effettuato "un controllo sulle email dei legali dell'Amministrazione regionale chiedendo al responsabile delle reti informatiche della Regione […] una verifica sui flussi di mail in uscita dalle caselle di posta elettronica istituzionale, attribuite agli avvocati dell'avvocatura regionale […]".

Ciò sarebbe stato effettuato analizzando informazioni quali "mittente, oggetto e destinatario delle mail inviate, oltre che ricognizione e pesatura di eventuali allegati alle mail stesse" nelle caselle di posta elettronica di "tutti gli Avvocati dell'Amministrazione regionale", senza che sussistessero "ragioni oggettive per l'effettuazione di un tale massivo ed indiscriminato controllo".

Il controllo in questione sarebbe stato, peraltro, richiesto non già dal datore di lavoro, da identificarsi "nel Direttore della Direzione regionale "Organizzazione e Personale", bensì, in via informale dal Segretario Generale, in assenza di "alcun Atto [o] Provvedimento Amministrativo, che abbia autorizzato [lo stesso]" e in mancanza di "procedure regolamentari e di policy sull'uso della posta elettronica e della Rete", non essendo stata fornita ai lavoratori alcuna informativa in relazione alla possibilità di detti controlli sulla posta elettronica.

Dalla documentazione in atti (v. nota prot. n. XX del XX della società LAZIOcrea S.p.A. - di seguito, "LazioCrea" – che ha effettuato lo stesso per conto della Regione) emerge che "per prassi il traffico delle email è conservato per 180 giorni circa prima di essere definitivamente cancellato" e che "per disporre di tale traffico non si accede né ai computer del personale né tantomeno alla loro casella di posta […] [in quanto] quando si parla di traffico di posta che il sistemista può vedere si [fa riferimento ai] dati a contorno come […] il giorno, l'ora, il mittente, il destinatario, l'oggetto e la dimensione dell'email stessa. Non è possibile vedere né il contenuto, né eventuali allegati. La presenza di allegati si desume (non si ha certezza) della dimensione dell'email stessa".

2. L'attività istruttoria.

In risconto a una richiesta d'informazioni dell'Autorità (nota prot. n. XX dell'XX), la Regione, con nota prot. n. XX dell'XX, ha dichiarato, in particolare, che:

> "la causa dei controlli effettuati deriva dall'obbligo per la Regione, in qualità di Titolare del trattamento, di assicurare la sicurezza dei trattamenti e, nel caso specifico, anche di tutelare la riservatezza delle informazioni gestite dagli avvocati: i dati personali contenuti nelle e-mail avrebbero potuto essere illecitamente diffusi";
>
> "l'iniziativa datoriale ha riguardato dati connessi al rapporto di lavoro e aveva l'obiettivo di accertare eventuali comportamenti illeciti del lavoratore, dei quali vi era ragionevole sospetto e che risultavano anche lesivi dell'immagine dell'Amministrazione. I comportamenti riguardano la presunta rivelazione da parte di propri dipendenti, nello specifico avvocati appartenenti all'Avvocatura regionale, di notizie d'ufficio che avrebbero dovuto rimanere segrete. I controlli sono stati disposti, in maniera riservata, dopo l'attuazione dei comportamenti stessi, in maniera puntuale e limitata ad alcuni dati, non configurando una forma di sorveglianza della prestazione lavorativa. Si precisa che non è stato oggetto del trattamento il contenuto stesso delle e-mail e che le attività di verifica sono state eseguite effettuando trattamenti non eccedenti rispetto alle finalità perseguite";
>
> "all'interno dell'informativa sul trattamento dei dati personali per il personale in servizio, pubblicata dal XX nella sezione della Intranet aziendale dedicata alla Privacy, è specificato che "Regione Lazio si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia)"";

“il Segretario generale della Giunta regionale aveva il dovere ed i correlati poteri necessari per effettuare le verifiche secondo quanto previsto dall’art. 19 bis comma 2 lett. d) ed h) del “Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale” n. XX del XX vigente all’epoca dei fatti […]“;

“non risulta agli atti alcuna copia di disposizione, atto o provvedimento tramite i quali sia stata formalizzata la richiesta all’amministratore di sistema di procedere al controllo”;

“il controllo, dal punto di vista tecnico, non è stato effettuato dall’Amministrazione Regionale, ma direttamente dalla società in house LazioCrea, alla quale con il contratto-quadro di Servizio di cui alla DGR n. XX del XX sono affidate le “progettazione, realizzazione e gestione della strategia regionale di Agenda Digitale, incluso il Sistema Informativo Regionale”. La società è stata nominata responsabile del trattamento con DGR n. XX e sono state fornite specifiche istruzioni attraverso l’allegato G alla DGR n. XX. Si rappresenta che tra le medesime istruzioni è presente la seguente previsione “Qualora sorgesse la necessità di effettuare trattamenti su dati personali diversi ed eccezionali rispetto a quelli normalmente eseguiti, LAZIOCrea dovrà informare il Titolare del trattamento ed il Data Protection Officer (DPO) della Regione Lazio.”. A seguito di richiesta da parte del Titolare, la società LazioCrea ha relazionato in merito alle modalità tecniche di esecuzione del controllo con nota prot. XX del XX […]”;

“Regione Lazio non ha indicato il […] tempo di conservazione [dei metadati connessi all’utilizzo della posta elettronica] alla società LazioCrea: si deve pertanto ritenere che esso sia frutto di valutazioni della società stessa, che, nella citata nota prot. XX […] indica che “per prassi il traffico delle email è conservato per 180 giorni circa prima di essere definitivamente cancellato”;

“questa Regione all’epoca dei fatti non ha ritenuto di essere soggetta all’obbligo di redigere una valutazione d’impatto in quanto non si è ritenuto che sussistessero rischi elevati derivanti dal trattamento, non riguardando lo stesso dati particolari o dati di cui all’art 10 [del Regolamento] (ex sensibili o giudiziari) su larga scala, né determinando una valutazione sistematica di aspetti personali. Tuttavia, alla luce di quanto occorso, si sta al momento valutando la necessità di tale adempimento”.

Con nota del XX (prot. n. XX), l’Ufficio, sulla base degli elementi acquisiti, dalle verifiche compiute e dei fatti emersi a seguito dell’attività istruttoria, ha notificato alla Regione, ai sensi dell’art. 166, comma 5, del Codice, l’avvio del procedimento per l’adozione dei provvedimenti di cui all’art. 58, par. 2, del Regolamento, per aver posto in essere un trattamento di dati personali relativi all’utilizzo della posta elettronica da parte dei dipendenti:

- in maniera non conforme ai principi di “liceità, correttezza e trasparenza”, “limitazione della conservazione” e “responsabilizzazione” , in violazione dell’art. 5, par. 1, lett. a) ed e), e par. 2, del Regolamento;

- in assenza di una base giuridica e in maniera difforme dalla disciplina di settore in materia di controlli a distanza dei lavoratori e raccolta di dati non pertinenti rispetto all’attività lavorativa (artt. 4 e 8 della l. n. 300/1970), in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 113 e 114 del Codice;

- omettendo di fornire agli interessati un’informativa sul trattamento dei dati personali, in violazione degli artt. 12 e 13 del Regolamento;

- in maniera non conforme al principio di “protezione dei dati fin dalla progettazione e per impostazione predefinita”, in violazione dell’art. 25 del Regolamento;

- omettendo di effettuare una previa valutazione d'impatto sulla protezione dei dati, in violazione dell'art. 35 del Regolamento.

Con la medesima nota, la Regione è stata invitata a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentita dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, dalla l. 24 novembre 1981, n. 689).

Con nota prot. n. XX del XX, la Regione ha fatto pervenire la propria memoria difensiva, dichiarando, in particolare, che:

"il trattamento risulta lecito in quanto "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" e per legittimo interesse del Titolare. L'Amministrazione regionale ha compiuto infatti un accertamento ex post, ovvero dopo l'attuazione del presunto comportamento illecito, in presenza di ragionevoli sospetti di comportamenti illeciti da parte di alcuni avvocati dell'avvocatura regionale, consistenti nella rivelazione a terzi di notizie d'ufficio sottoposte al vincolo di segretezza. Si ritiene che tale fattispecie sia estranea al campo di applicazione degli artt. 4 e 8 della l. 300/1970";

"[…] inoltre […] il comma 2 dell'art. 4 della l. 300/1970 esclud[e] dalle disposizioni di cui al comma 1 [della l. 300/1970] gli strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa tra i quali, per i soggetti di interesse, rientra certamente la posta elettronica";

"l'informativa […] pubblicata nella sezione della Intranet aziendale dedicata alla Privacy, indica che "Regione Lazio si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia)". Si prende atto che, a parere dell'Autorità, tale informativa non risulta sufficientemente specifica, pertanto è intenzione dell'Amministrazione integrarla […]";

"l'Amministrazione ha inoltre stabilito di dotarsi di un disciplinare interno […] che descriva i controlli ai quali possono essere sottoposti i dipendenti, che sarà adeguatamente diffuso agli stessi. Si rappresenta inoltre che, con determinazione XX del XX della Direzione Affari Istituzionali, Personale e Sistemi Informativi, l'Amministrazione si è già dotata di un disciplinare";

[…] per l'utilizzo delle dotazioni ICT per il personale in servizio presso gli uffici della Giunta regionale, che, al capitolo 8, introduce delle previsioni relative ai controlli. Tali previsioni saranno armonizzate con il nuovo disciplinare interno in tema di controlli";

"la [Regione, successivamente all'avvio dell'istruttoria,] ha provveduto a redigere una valutazione di impatto sulla protezione dei dati personali relativa alla gestione dei log […]";

"con riferimento alla conservazione dei dati, si rinvia alla DPIA in merito alla gestione dei log […]. Si ritiene congruo un tempo di almeno 6 mesi di conservazione in ragione della possibilità per l'Amministrazione di porre in essere azioni di indagine relative, ad esempio, ad attacchi informatici che non vengano tempestivamente rilevati, nonché della complessità dei sistemi gestiti. Tale considerazione deriva anche dall'analogia con quanto disposto dai provvedimenti [del Garante] "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle attribuzioni delle funzioni di amministratore di sistema - 27 novembre 2008" e "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie - 12 maggio 2011" […]";

la circostanza che non "sia stata formalizzata la richiesta all'amministratore di sistema di procedere al controllo […] esclud[e] un trattamento di monitoraggio e ancor più un

trattamento di “monitoraggio sistematico” dell’Attività dei dipendenti da parte dell’Amministrazione regionale [ed è] da interpretare come un evento isolato accaduto una tantum”;

“non si condivide, dal punto di vista logico, la deduzione che “dalla circostanza che codesta Regione abbia chiesto a LAZIOCrea di effettuare i controlli in questione su tali metadati si desume che la stessa fosse a conoscenza della raccolta degli stessi, che veniva effettuata per proprio conto e nel proprio esclusivo interesse, da parte del responsabile del trattamento”, in quanto dalla richiesta si può derivare unicamente una presunzione, in quanto la Società avrebbe potuto rispondere di non disporre dei dati o di disporne per un diverso periodo. In ogni caso, l’Amministrazione anche a seguito della valutazione di impatto sulla protezione dei dati personali relativa alla gestione dei log […], provvederà ad impartire a LAZIOCrea opportune istruzioni al fine di rimodulare i tempi di conservazione dei metadati […]”;

“l’obbligo di effettuare una previa valutazione d’impatto sulla protezione dei dati sussiste in presenza di “un rischio elevato per i diritti e le libertà delle persone fisiche” (art. 35 comma 1 del Regolamento). Un rischio è uno scenario che descrive un evento e le sue conseguenze, stimato in termini di gravità e probabilità.” I log presentano una probabilità estremamente ridotta di essere acceduti per finalità diverse da quelle di tutelare la sicurezza dei sistemi informatici e, pur in presenza di un livello elevato di gravità della rivelazione dei dati, il rischio risultante è stato stimato medio[…] La valutazione non è stata condotta in quanto non sono stati rilevati almeno due criteri applicabili [tra quelli indicati dal Comitato europeo per la protezione dei dati nelle “Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento "possa presentare un rischio elevato" ai fini del regolamento (UE) 2016/679”] […] si è [comunque] proceduto [, su base volontaria e successivamente all’avvio dell’istruttoria] ad effettuare e documentare una valutazione di impatto sulla protezione dei dati personali relativa alla gestione dei log”.

In occasione dell’audizione, richiesta ai sensi dell’art. 166, comma 6, del Codice e tenutasi in data XX (verbale prot. n. XX del XX), la Regione ha dichiarato, in particolare, che:

“la Regione Lazio, ancor prima di ricevere la contestazione da parte dell’Autorità, aveva messo in campo una serie di misure per rendere edotti i lavoratori in merito alle corrette modalità di utilizzo degli strumenti informatici (v. disciplinare interno del XX, al cui interno figura un paragrafo sull’utilizzo della posta elettronica e sui controlli che la Regione si riserva di effettuare) […]”;

“in merito alla liceità del trattamento, la Regione Lazio ritiene che non vi siano i presupposti per l’applicazione dell’art. 4 della l. 300/1970, stante la possibilità per il datore di lavoro, come riconosciuto dalla Corte di Cassazione, di effettuare controlli difensivi a tutela del proprio patrimonio. Occorre effettuare, infatti, un bilanciamento di interessi tra il diritto alla protezione dei dati dei lavoratori e il diritto del datore di lavoro a tutelare i propri interessi”;

“la raccolta dei metadati relativi all’utilizzo della posta elettronica non persegue la finalità di controllare l’attività dei lavoratori, essendo strumentale esclusivamente a garantire la sicurezza informatica”;

“il controllo in questione non riguardava la corretta esecuzione dell’attività lavorativa da parte dei dipendenti ma era finalizzato ad accertare una presunta condotta illecita”;

“sussistono valide ragioni per giustificare la conservazione dei predetti metadati per un tempo maggiore di sette giorni, al fine di garantire la sicurezza dei sistemi informativi. Ad esempio, con riguardo agli attacchi informatici del 2021, gli accertamenti successivamente

condotti non sarebbero stati possibili se non fossero stati conservati i log per periodi di tempo sufficientemente lunghi, di almeno sei mesi. I motivi che giustificano tali tempi di conservazione sono meglio esposti nella bozza di valutazione d'impatto sulla protezione dei dati fornita dalla Regione in allegato alle proprie memorie difensive";

"la Regione Lazio si riserva di fornire all'Autorità ulteriori elementi ed informazioni, entro quindici giorni dalla data dell'audizione, in merito all'attuale conservazione dei metadati utilizzati nell'ambito dei controlli oggetto di segnalazione".

Successivamente, con nota prot. n. XX del XX, la Regione ha fatto pervenire tali ulteriori elementi e informazioni, dichiarando, in particolare, che:

"con nota prot. XX del XX, acquisita al protocollo regionale n.XX del XX, […] [il] Direttore della Direzione Sistemi Infrastrutturali della società in house LAZIOCREA, nominata responsabile del trattamento ai sensi dell'art. 28 del Regolamento 2016/679, ha dichiarato che "i dati dei log relativi al traffico delle mail delle utenze in questione riferiti al procedimento XX del Garante […], sono stati a suo tempo cancellati secondo quando previsto dalle nostre procedure. Il periodo di conservazione massimo dei log era all'epoca stabilito in 180 giorni decorsi i quali sono state automaticamente cancellate. La copia delle già menzionate estrazioni è nella disponibilità della Autorità Giudiziaria che le ha fatte oggetto di un autonomo trattamento avendone provveduto al sequestro in data XX"";

"con nota prot. reg. XX del XX l'Avv. […], Avvocato Coordinatore dell'Avvocatura Regionale ha rappresentato che "La Direr-Dirl Lazio, che aderisce alla Fedirets, ha reputato questa attività di verifica sul flusso informatico (limitato ad un numero sparuto di account e durata poche ore) espressione di attività antisindacale (sebbene il mittente, autore dell'indebito utilizzo della posta elettronica istituzionale, era un soggetto non rivestente ruoli gestionali nell'Organizzazione), al pari della mancata risposta della Direzione Affari istituzionali volta ad attivare un confronto per la regolamentazione dell'uso degli account aziendali: ed ha così adito il Tribunale con ricorso ex art. 28 L. n. 300 del 1970. Il Tribunale, con decreto del 6 luglio 2021, nel contraddittorio delle parti, respingeva il ricorso. La Direr-Dirl Lazio, allora, proponeva opposizione, la quale – con sentenza del 7 marzo 2022 (che si produce con i necessari omissis, attenendo le altre parti della decisione a questioni irrilevanti in questa sede e coinvolgenti altri soggetti) […] veniva respinta dal Tribunale di Roma […] a conferma della totale infondatezza dell'avversa pretesa";

"con riferimento all'attività di revisione dell'informativa relativa al personale dipendente, si rappresenta che, con nota prot. reg. n. XX del XX, il […] Direttore della Direzione Regionale Affari Istituzionali e Personale ha comunicato che "[…] la Direzione sta ultimando le attività di analisi dei processi di trattamento nonché le attività di dettaglio di tutte le operazioni di trattamento dati che la stessa opera nello svolgimento delle proprie funzioni istituzionali".

Con la medesima nota, la Regione ha depositato agli atti copia dei seguenti documenti: "DGR n. XX del XX: revisione del modello organizzativo adottato dalla Giunta Regionale in tema di protezione dei dati personali (DGR di adeguamento del regolamento n. XX "Regolamento di organizzazione degli uffici e dei servizi della Giunta regionale")" e "determinazione XX del XX della Direzione Affari Istituzionale, Personale e Sistemi Informativi approvazione del "Disciplinare per l'assegnazione e l'utilizzo delle dotazioni ICT per il personale in servizio presso gli uffici della Giunta regionale del Lazio".".

3. Esito dell'attività istruttoria.

3.1 La normativa in materia di protezione dei dati.

In base alla disciplina in materia di protezione dei dati personali, il datore di lavoro può trattare i dati personali, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1, del Regolamento) dei lavoratori se il trattamento è necessario, in generale, per la gestione del rapporto di lavoro e per adempiere a specifici obblighi o compiti derivanti dalla disciplina di settore (artt. 6, par. 1, lett. c), 9, par. 2, lett. b) e 4; 88 del Regolamento). Il trattamento è, inoltre, lecito quando sia "necessario per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (artt. 6, parr. 1, lett. e), 2 e 3 del Regolamento; 2-ter del Codice, nel testo anteriore alle modifiche apportate dal d.l. 8 ottobre 2021, n. 139, vigente all'epoca dei fatti oggetto di segnalazione).

Il datore di lavoro deve, inoltre, rispettare le norme nazionali, che "includono 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 […] e i sistemi di monitoraggio sul posto di lavoro" (artt. 6, par. 2, e 88, par. 2, del Regolamento). Sul punto il Codice, confermando l'impianto anteriore alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101, fa espresso rinvio alle disposizioni nazionali di settore che tutelano la dignità delle persone sul luogo di lavoro, con particolare riferimento ai possibili controlli da parte del datore di lavoro (artt. 113 "Raccolta dati e pertinenza" e 114 "Garanzie in materia di controllo a distanza"). Per effetto di tale rinvio, e tenuto conto dell'art. 88, par. 2, del Regolamento, l'osservanza degli artt. 4 e 8 della l. n. 300/1970 e dell'art. 10 del d.lgs. n. 297/2003 (nei casi in cui ne ricorrono i presupposti) costituisce una condizione di liceità del trattamento.

Tali norme costituiscono nell'ordinamento interno quelle disposizioni più specifiche e di maggiore garanzia di cui all'art. 88 del Regolamento - a tal fine oggetto di specifica notifica a cura del Garante alla Commissione (consultabile alla pagina: https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu/eu-countries-gdpr-specific-notifications_en.) ai sensi dell'art. 88, par. 3, del Regolamento - la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione - analogamente alle specifiche situazioni di trattamento del capo IX del Regolamento - determina anche l'applicazione di sanzioni amministrative pecuniarie ai sensi dell'art. 83, par. 5, lett. d), del Regolamento (cfr., con riguardo all'ambito lavorativo pubblico, da ultimo, provv. 28 ottobre 2021, n. 384, doc. web n. 9722661; provv. 13 maggio 2021, n. 190, doc. web n. 9669974; provv. 11 marzo 2021, n. 90, doc. web n. 9582791, nonché i provvedimenti in essi richiamati).

Il titolare del trattamento è, comunque, tenuto a rispettare i principi in materia di protezione dei dati (art. 5 del Regolamento) ed è responsabile dell'attuazione di misure tecniche e organizzative adeguate in ragione degli specifici rischi derivanti dal trattamento, dovendo essere in grado di dimostrare che lo stesso è effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento).

3.2 Il trattamento dei dati personali relativo all'utilizzo della posta elettronica da parte dei dipendenti.

Dagli elementi acquisiti nel corso dell'attività istruttoria è emerso che la Regione, al fine di verificare presunti comportamenti illeciti da parte di proprio personale in sevizio presso gli uffici dell'avvocatura regionale, in presenza del sospetto in merito alla possibile rivelazione a terzi di notizie d'ufficio, ha incaricato LazioCrea, in veste di proprio responsabile del trattamento, di effettuare un controllo sui metadati relativi all'utilizzo degli account di posta elettronica istituzionale da parte dei lavoratori in questione (giorno, ora, mittente, destinatario, oggetto e dimensione dell'email).

Tale operazione di analisi ed estrazione dei dati è stata possibile in quanto, come confermato nel corso del procedimento, i metadati, relativi all'utilizzo degli account di posta elettronica istituzionale assegnati ai dipendenti della Regione, vengono raccolti in modo preventivo e generalizzato, e successivamente conservati ordinariamente per 180 giorni.

3.3 La correttezza e la trasparenza nei confronti degli interessati: l'informativa sul trattamento dei dati personali.

Nel rispetto del principio di "liceità, correttezza e trasparenza", il titolare del trattamento deve adottare misure appropriate per fornire all'interessato tutte le informazioni di cui agli artt. 13 e 14 del Regolamento in forma concisa, trasparente, intelligibile e facilmente accessibile, con un linguaggio semplice e chiaro (art. 12 del Regolamento).

A fronte di tale obbligo, la Regione, nel fornire ai propri dipendenti l'informativa sul trattamento dei dati personali - che sarebbe stata pubblicata nell'intranet aziendale dal XX, sebbene della stessa non sia stata prodotta copia - comunicava esclusivamente la circostanza che essa "si riserva di verificare, nei limiti consentiti dalle norme di legge e contrattuali, l'integrità dei propri sistemi (informatici e di telefonia)", mentre solo nel corso dell'istruttoria ha rappresentato l'intenzione di adottare un disciplinare interno per rendere edotti i lavoratori in merito alle modalità di effettuazione dei predetti controlli in relazione all'utilizzo degli strumenti informatici da parte dei dipendenti (cfr. nota prot. n. XX del XX).

Nel corso del procedimento è poi emerso che sin dal XX la Regione avesse adottato un disciplinare per l'utilizzo delle dotazioni ICT per il personale in servizio presso gli uffici della Giunta regionale, riservandosi "per motivi organizzativi o di sicurezza […] la facoltà di effettuare, attraverso LAZIOcrea, controlli saltuari e occasionali", e in particolare di "monitorare le reti e le Dotazioni [in caso di] […] constatazione di utilizzo indebito della posta elettronica", anche in merito al "volume dei messaggi scambiati, formato e dimensione dei file allegati" (par. 8 della determinazione XX del XX della Direzione Affari Istituzionali, Personale e Sistemi Informativi).

Nel premettere che agli atti non vi è prova che i dipendenti siano stati effettivamente informati della possibilità di reperire e consultare il disciplinare in questione all'interno dell'intranet regionale (cfr. par. 10 della determinazione, ove si afferma in via generica che "viene data diffusione ai dipendenti dell'approvazione del Disciplinare tramite intranet regionale e/o posta elettronica"), si rileva che né l'originaria informativa resa ai dipendenti né tale documento contengono tutti gli elementi espressamente richiesti dalla normativa in materia di protezione dei dati – segnatamente la "base giuridica del trattamento" e il "periodo di conservazione dei dati personali" (art. 13, par. 1, lett. c) e par. 2, lett. a), del Regolamento) - e forniscono agli stessi una chiara e trasparente rappresentazione del complessivo trattamento effettuato, con particolare riguardo alla raccolta e alla conservazione per 180 giorni dei metadati relativi all'utilizzo della posta elettronica (v. le "Linee guida del Garante per posta elettronica e internet" del 1° marzo 2007, n. 13, doc. web n. 1387522 - che, ancorché riferite al previgente quadro normativo, contengono principi e indicazioni ancora validi - in particolare parr. 3.1 e 3.3).

L'osservanza dell'obbligo di fornire agli interessati tutti gli elementi informativi essenziali previsti dal Regolamento risponde all'esigenza di consentire agli stessi di essere pienamente consapevole, prima che il trattamento abbia inizio, delle caratteristiche dello stesso. Ciò anche con riguardo alla raccolta, in un quadro di liceità, di dati personali connessi all'attività lavorativa (cfr., sentenza della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 - Ricorso n. 61496/08 - Causa Barbulescu c. Romania, spec. par. n. 133 e 140).

Sul punto si evidenzia, peraltro, che l'adempimento degli obblighi informativi nei confronti dei dipendenti (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica precondizione per il lecito utilizzo dei raccolti attraverso strumenti tecnologici, da parte del datore di lavoro, anche a tutti i fini connessi al rapporto di lavoro (art. 4, co. 3, della l. n. 300/1970).

Pur dandosi atto dell'intenzione della Regione di predisporre un nuovo disciplinare in merito all'utilizzo delle risorse informatiche da parte dei dipendenti e ai trattamenti che, per esigenze

organizzative e di sicurezza informatica, comportano la raccolta e la conservazione anche dei metadati relativi all'impiego della posta elettronica da parte dei dipendenti, risulta accertato che la Regione non ha, all'atto dell'avvio del descritto trattamento, provveduto a rendere agli interessati tutti gli elementi informativi previsti dal Regolamento, avendo, pertanto, agito in maniera non conforme al "principio di liceità, correttezza e trasparenza" e in violazione degli artt. 5, par. 1, lett. a), 12 e 13 del Regolamento.

3.4 La liceità del trattamento: il mancato rispetto della disciplina in materia di controlli a distanza.

In via generale, si rileva che il tema del trattamento dei dati connesso all'attribuzione di un account di posta elettronica istituzionale o aziendale ai singoli dipendenti è da tempo all'attenzione dell'Autorità, sia con provvedimenti a carattere generale (v. le "Linee guida del Garante per posta elettronica e internet", cit.) sia con decisioni su singoli casi.

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 (artt. 2 e 15 Cost.), che proteggono il nucleo essenziale della dignità della persona e il pieno sviluppo della sua personalità nelle formazioni sociali. Ciò comporta che, anche nel contesto lavorativo, sussista una legittima aspettativa di riservatezza in relazione ai messaggi oggetto di corrispondenza (v. punto 5.2 lett. b), delle "Linee guida del Garante per posta elettronica e Internet", cit.; v., tra i tanti, provv. 4 dicembre 2019, n. 216, doc. web n. 9215890 e i precedenti in esso citati).

La conservazione dei metadati relativi all'utilizzo della posta elettronica dei dipendenti, ancorché sul presupposto della sua necessità per finalità di sicurezza informatica (invocate nel caso di specie dalla Regione), può comportare un indiretto controllo a distanza dell'attività dei lavoratori, che la legge consente esclusivamente al ricorrere di esigenze organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale, e in presenza delle garanzie procedurali previste dall'art. 4, comma 1, della l. n. 300/1970 (accordo sindacale o, in alternativa, autorizzazione pubblica).

Sebbene la gestione dei dati esteriori relativi all'utilizzo dei sistemi di posta elettronica, contenuti nella cosiddetta "envelope" del messaggio, e la conservazione degli stessi per un arco temporale limitato, di regola non superiore a sette giorni, si possano considerare necessarie ad assicurare il corretto funzionamento e il regolare utilizzo del sistema di posta elettronica, comprese le essenziali garanzie di sicurezza informatica (v. provv.ti nn. 303 del 13 luglio 2016, doc. web n. 5408460, confermato dal Tribunale di Chieti con sent. n. 672 del 24 ottobre 2019; 1° febbraio 2018, n. 53, doc. web n. 8159221; 29 ottobre 2020, n. 214, doc. web n. 9518890; 29 settembre 2021, n. 353, doc. web n. 9719914), la conservazione di tali metadati, per un lasso di tempo più esteso, non può, invece, ricondursi all'ambito di applicazione dell'art. 4, comma 2, della predetta l. n. 300/1970. Infatti, 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, 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.

In tale quadro, la generalizzata raccolta e la conservazione, per un periodo più esteso (rispetto ai predetti 7 giorni), dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti non possono, invece, essere ricondotte all'ambito di applicazione del comma 2 dell'art. 4 della l. n. 300/1970, rientrando, piuttosto, tra gli strumenti funzionali alla tutela dell'integrità del patrimonio informativo del titolare nel suo complesso, di cui al comma 1 del medesimo art. 4.

Con riguardo al caso di specie, ciò è, altresì, comprovato dalla circostanza che nel citato disciplinare del XX la Regione si è riservata di effettuare trattamenti dei predetti metadati – conservandoli, come detto, per un esteso arco temporale - "per motivi organizzativi e di sicurezza" (cfr. par. 8 delibera XX, cit.).

Pertanto, non avendo la Regione posto in essere le procedure di garanzia di cui all'art. 4, comma 1, della l. n. 300/1970, prima di dare avvio alla preventiva e sistematica raccolta dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, e alla conservazione degli stessi per un ampio arco temporale, il trattamento in questione risulta essere in contrasto con la normativa in materia di protezione dei dati personali e con la disciplina di settore in materia di controlli a distanza, in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970).

Né può essere invocato, ai fini della liceità del complessivo trattamento, come prospettato dalla Regione nella propria memoria difensiva, il perseguimento di un legittimo interesse del titolare del trattamento, non potendo lo stesso trovare applicazione "al trattamento di dati effettuati dalle autorità pubbliche" (cfr. art. 6, par.1, lett. f), del Regolamento), e più, in generale, in quanto, come sopra precisato e costantemente ribadito nei provvedimenti del Garante in materia, i trattamenti conseguenti all'impiego degli strumenti tecnologici nei luoghi di lavoro, da cui può derivare un controllo indiretto sull'attività lavorativa, trovano la propria base giuridica nella disciplina di settore di cui all'art. 4 della l. n. 300/1970. Tale disposizione perimetra, infatti, in modo uniforme a livello nazionale, l'ambito del trattamento consentito in ogni contesto lavorativo (pubblico e privato) e costituisce nell'ordinamento interno una disposizione più specifica e di maggiore garanzia di cui all'art. 88 del Regolamento, la cui osservanza è condizione di liceità del trattamento (art. 5, par.1, lett. a) e 6, par. 1, lett. c) del Regolamento; cfr., anche la giurisprudenza della Corte europea dei diritti dell'uomo, nel caso Antovic e Mirkovic v. Montenegro, application n. 70838/13 del 28.11.2017, che ha stabilito che il rispetto della "vita privata" deve essere esteso anche ai luoghi di lavoro pubblici, evidenziando che i controlli sul posto di lavoro possono essere effettuati solo nel rispetto delle garanzie previste dalla legge nazionale applicabile).

In merito alla compatibilità con i principi di protezione dei dati dell'esteso periodo di conservazione di tali metadati individuato dalla Regione (180 giorni), si veda il successivo par. 3.7.

3.5. Le verifiche effettuate sugli account di posta elettronica di alcuni dipendenti.

Come risulta dalle evidenze in atti, i dati personali relativi ai messaggi di posta elettronica, raccolti e conservati con le modalità sopra descritte, sono stati poi trattati dalla Regione anche al fine di effettuare verifiche puntuali su specifici dipendenti.

A tal riguardo, non può essere accolta la tesi difensiva prospettata dalla Regione, secondo la quale la stessa avrebbe effettuato "un accertamento ex post, ovvero dopo l'attuazione del presunto comportamento illecito, in presenza di ragionevoli sospetti di comportamenti illeciti da parte di alcuni avvocati dell'avvocatura regionale, consistenti nella rivelazione a terzi di notizie d'ufficio sottoposte al vincolo di segretezza", sul presupposto che "tale fattispecie sia estranea al campo di applicazione degli artt. 4 e 8 della l. 300/1970".

Premesso che la c.d. teoria sui controlli difensivi, di pura creazione giurisprudenziale, è oggetto di applicazioni non univoche (cfr. provv. 15 aprile 2021, n. 137, doc. web n. 9670738) e si fonda su circostanze di fatto che in ogni caso non ricorrono nel caso di specie, occorre ribadire, per i profili di protezione dei dati, quanto segue. I trattamenti di dati personali connessi all'impiego di strumenti dai quali possa derivare anche la possibilità di controllo a distanza dell'attività dei lavoratori devono essere svolti nel rigoroso rispetto dei limiti e delle condizioni previste dalla cornice legislativa di riferimento, che ne costituisce, come detto, la base giuridica (artt. 5, par. 1, lett. a), 6 , 88, par. 1, del Regolamento, nonché 114 del Codice, in riferimento all'art. 4 della l. n.

300/1970). Ciò, a maggior ragione, in quanto, a seguito delle modifiche apportate all'art. 4 della l. n. 300/1970 dal d.lgs. 14 settembre 2015, n. 151, anche le esigenze di tutela del patrimonio datoriale sono state espressamente incluse tra le sole finalità lecite perseguibili mediante sistemi che possono comportare il controllo indiretto sulla generalità dei dipendenti, subordinandone l'installazione e l'utilizzazione all'accordo sindacale o, in alternativa, all'autorizzazione pubblica (v. il precedente par. 3.4). Ne consegue che, qualora non vengano rispettate tali condizioni per il lecito impiego dei predetti sistemi, qualunque trattamento, anche ulteriore, di tali dati, inclusa la loro "estrazione, consultazione e uso" (art. 4, par. 1, n. 1), del Regolamento), debba considerarsi sprovvisto di idonea base giuridica e quindi illecito.

Conseguentemente, le forme di controllo sull'attività dei lavoratori, poste in essere in assenza delle predette garanzie, si pongono al di fuori del quadro di liceità delineato dalle disposizioni di settore e dalla disciplina in materia di protezione dei dati. Si consideri, altresì, che la predetta disciplina di settore consente di utilizzare, per ulteriori finalità nell'ambito della gestione del rapporto, solo le informazioni già lecitamente raccolte nel rispetto delle condizioni e dei limiti previsti dall'art. 4 della l. n. 300/1970 e, dunque, nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata (v. provv.ti 28 ottobre 2021, n. 384, doc. web n. 9722661, e 13 maggio 2021, n. 190, doc. web n. 9669974).

Alla luce delle considerazioni che precedono, anche il trattamento dei dati personali, consistente nella consultazione dei metadati raccolti e nell'estrazione di alcune casistiche relative a singoli lavoratori è stata effettuata in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice (in relazione all'art. 4, comma 1, della l. n. 300/1970).

3.6. La raccolta di dati non attinenti all'attività lavorativa.

Fin dal 1970, al datore di lavoro, pubblico e privato, è fatto divieto di "effettuare indagini, anche a mezzo di terzi, 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 della l. n. 300/1970 e art. 10 del d.lgs. 10 settembre 2003, n. 276, richiamati espressamente dall'art. 113 del Codice).

La generalizzata raccolta e la conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, per un periodo di tempo esteso, peraltro in assenza di idonei presupposti giuridici e di chiare indicazioni e informazioni rese ai lavoratori (v. il precedente par. 3.1), comporta, altresì, la possibilità per il datore di lavoro di acquisire, nel corso dello svolgimento del rapporto di lavoro, informazioni sulla vita privata del lavoratore o su fatti comunque non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore.

Si osserva, a tal riguardo, che dagli elementi ricavabili dai dati esteriori della corrispondenza, come l'oggetto, il mittente e il destinatario e altre informazioni che accompagnano i dati in transito, definendone profili temporali (come la data e l'ora di invio/ricezione), nonché dagli aspetti quali-quantitativi anche in ordine ai destinatari e alla frequenza di contatto (in quanto anche questi dati sono, a propria volta, suscettibili di aggregazione, elaborazione e di controllo), è possibile acquisire elementi riferiti alla sfera personale o alle opinioni dell'interessato, ove tali informazioni, come nel caso di specie, siano conservate per periodi particolarmente estesi.

A riprova di ciò, vi è la circostanza che tale ampia e prolungata raccolta ha permesso di effettuare le predette verifiche e, nell'ambito di queste, una precisa selezione degli specifici account da indagare, anche sulla base di altre informazioni già disponibili e di dati personali, comunque noti, riferiti agli interessati. In particolare, risultano essere stati esaminati i flussi di email in uscita dagli account di posta elettronica del personale dell'avvocatura regionale e, in special modo, i messaggi indirizzati a rappresentati di una specifica sigla sindacale (alla quale molti lavoratori dell'avvocatura avevano aderito o con cui erano in rapporto di sodalizio o di cui erano

simpatizzanti), nonché quelli inviati a un collega noto per essere sostenitore di tale sigla sindacale (cfr. esposto della Regione al Comando provinciale della Guardia di Finanza, in atti).

Né può essere ritenuto sufficiente, a tal fine, che il datore di lavoro, come nel caso di specie, si limiti a richiamare il corretto utilizzo della posta elettronica da parte dei propri dipendenti per soli fini istituzionali o connessi al rapporto di lavoro, facendo leva esclusivamente sulla responsabilità dei dipendenti e sul divieto di utilizzo degli strumenti informativi per fini personali (cfr. provv. 13 maggio 2021, n. 190, doc. web n. 9669974, par. 3.4). Ciò in quanto, considerato che la linea di confine tra ambito lavorativo e professionale e quello strettamente privato non può sempre essere tracciata in modo netto, non può essere prefigurato il completo annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, anche nei casi in cui il dipendente sia connesso ai servizi di rete messi a disposizione del datore di lavoro o utilizzi una risorsa aziendale, ragione per la quale la Corte europea dei diritti dell'uomo ha nel tempo confermato che la protezione della vita privata si estende anche all'ambito lavorativo, ove si svolgono le relazioni della persona che lavora (v. sentenze Niemietz c. Allemagne, 16.12.1992, ric. n. 13710/88, spec. par. 29; Copland v. UK, 03.04.2007, ric. n. 62617/00, spec. par. 41; Brbulescu v. Romania, cit., spec. parr. 70-73 e 80; Antovi and Mirkovi v. Montenegro, cit., spec. par. 41-42).

Per tali ragioni, la condotta della Regione risulta, altresì, in contrasto con le disposizioni nazionali che vietano al datore di lavoro di acquisire (e comunque "trattare") informazioni che "non [siano] rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore" o comunque relative alla sfera privata degli interessati, in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 113 del Codice (in relazione agli artt. 8 della l. n. 300/1970 e 10 del d.lgs. n. 276/2003).

3.7 La limitazione della conservazione e la protezione dei dati fin dalla progettazione e per impostazione predefinita.

In base al principio di "limitazione della conservazione", i dati personali devono essere "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" (art. 5, par. 1, lett. e), del Regolamento).

In considerazione del rischio che incombe sui diritti e le libertà degli interessati, il titolare del trattamento deve - "fin dalla progettazione" e "per impostazione predefinita" (art. 25 del Regolamento) - adottare misure tecniche e organizzative adeguate ad attuare i principi di protezione dei dati, integrando nel trattamento le necessarie garanzie per soddisfare i requisiti del Regolamento e tutelare i diritti e le libertà degli interessati (cfr. "Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", adottate dal Comitato europeo per la protezione dei dati il 20 ottobre 2020, spec. punti 42, 44 e 49).

Tale obbligo "vale [anche] per […] il periodo di conservazione […]" dei dati (art. 25, par. 2, del Regolamento).

Nel caso di specie, all'esito dell'istruttoria, è emerso che la Regione conserva i metadati relativi all'utilizzo della posta elettronica, per generiche finalità di sicurezza informativa, per un periodo di 180 giorni, che, anche alla luce dei provvedimenti adottati in materia dal Garante, non risultata giustificato per il perseguimento delle predette finalità. Ciò in quanto, ove occorra, eventuali incidenti di sicurezza possono e devono essere tempestivamente rilevati e mitigati, a tutela dell'integrità e del buon funzionamento dei sistemi informatici, attuando le opportune contromisure e, se del caso, facendo ricorso ai metadati relativi all'utilizzo della posta elettronica, in ogni caso entro limiti temporali ben più ristretti (v. provv.ti del Garante nn. 303 del 13 luglio 2016, doc. web n. 5408460; 1° febbraio 2018, n. 53, doc. web n. 8159221; 29 ottobre 2020, n. 214, doc. web n. 9518890).

Non è stato, pertanto, assicurato, sia al momento di determinare i mezzi del trattamento sia durante il trattamento stesso, che la protezione dei dati personali fosse integrata nel trattamento fin dalla sua progettazione e per impostazione predefinita durante l'intero ciclo di vita dei dati, "incorporan[d]o nel trattamento le misure e le garanzie adeguate ad assicurare l'efficacia dei principi di protezione dei dati, dei diritti e delle libertà degli interessati" e facendo in modo che "[venisse] effettuato per impostazione predefinita solo il trattamento strettamente necessario per conseguire la specifica e lecita finalità", anche con riguardo al periodo di conservazione dei dati, "in tutte le fasi della progettazione delle attività di trattamento, compresi gli appalti, le gare di appalto, l'esternalizzazione, lo sviluppo, il supporto, la manutenzione, il collaudo, la conservazione, la cancellazione ecc." ("Linee guida 4/2019 sull'articolo 25 - Protezione dei dati fin dalla progettazione e per impostazione predefinita", cit.). Ciò ha pertanto determinato la violazione dell'art. 25 del Regolamento.

Né si può ritenere rilevante, ai fini dell'esclusione della complessiva responsabilità della Regione sotto tale profilo, la circostanza che, come dichiarato, la stessa "non ha indicato il […] tempo di conservazione [dei metadati connessi all'utilizzo della posta elettronica] alla società LazioCrea" e che, invece, la determinazione di tale tempo di conservazione dei metadati, pari a 180 giorni, sarebbe stata "frutto di valutazioni della società".

Occorre, infatti, evidenziare che sul titolare del trattamento, in quanto soggetto sul quale ricadono le decisioni circa le finalità e le modalità del trattamento dei dati personali degli interessati, grava una "responsabilità generale" sui trattamenti posti in essere (cons. 74 del Regolamento; cfr., tra i tanti, provv. 10 febbraio 2022, n. 43, doc. web n. 9751498 e i precedenti provv. ivi richiamati; v. anche le "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", adottate dal Comitato europeo per la protezione dei dati il 7 luglio 2021, spec. par. 174).

In base al principio di "responsabilizzazione", il titolare è, infatti, tenuto a rispettare i principi di protezione dei dati (art. 5, par 1, del Regolamento) e deve essere in grado di comprovarlo (art. 5, par. 2, del Regolamento), anche con riguardo alle adeguate misure tecniche e organizzative messe in atto al fine di garantire il rispetto della disciplina in materia di protezione dei dati e di quella di settore eventualmente applicabile (art. 24, par. 1, del Regolamento).

Come recentemente messo in evidenza dal Garante, il titolare del trattamento, anche quando utilizza prodotti o servizi realizzati da terzi, deve verificare, anche avvalendosi del supporto del Responsabile della protezione dei dati, ove designato, la conformità ai principi applicabili al trattamento dei dati (art. 5 del Regolamento) adottando, nel rispetto del principio di responsabilizzazione, le opportune misure tecniche e organizzative e impartendo le necessarie istruzioni al fornitore del servizio (cfr. artt. 5, par. 2, 24, 25 e 32 del Regolamento; cfr., con riguardo a specifici trattamenti in ambito lavorativo, provv.ti 28 ottobre 2021, n. 384, doc. web n. 9722661, e 10 giugno 2021, n. 235, doc. web n. 9685922; ma v. anche provv. 17 dicembre 2020, n. 282, doc. web n. 9525337). In tale prospettiva, il titolare del trattamento deve accertarsi, ad esempio, che siano disattivate le funzioni che non sono compatibili con le finalità del trattamento o che si pongono in contrasto con specifiche norme di settore previste dall'ordinamento, specie in ambito lavorativo, commisurando adeguatamente anche i tempi di conservazione dei dati.

Dalla circostanza che la Regione abbia chiesto a LazioCrea di effettuare i controlli in questione su tali metadati si desume, peraltro, che la stessa fosse a conoscenza della raccolta degli stessi, che veniva effettuata per proprio conto e nel proprio esclusivo interesse da parte del responsabile del trattamento.

La necessità e le ragioni volte a giustificare tale ampia conservazione dei predetti metadati sono inoltre state prospettate dalla stessa Regione nel corso dell'istruttoria, in particolare in occasione dell'audizione, nel corso della quale è stata espressa la necessità che "al fine di garantire la

sicurezza dei sistemi informativi" gli stessi devono essere conservati "per periodi di tempo sufficientemente lunghi, di almeno sei mesi", confermando, in tal modo, che le scelte operate in proposito siano imputabili alla Regione o comunque riconducibili ad esigenze invocate dalla Regione in quanto titolare del trattamento.

Per tali ragioni, la scelta di fissare il periodo di conservazione in 180 giorni deve essere comunque imputata alla Regione. Conseguentemente, tenuto conto del quadro normativo di settore applicabile, le specifiche operazioni di trattamento consistenti nella generalizzata raccolta e memorizzazione per un arco temporale di 180 giorni dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, si pongono, altresì, in contrasto con i principi di "limitazione della conservazione dei dati" nonché di "protezione dei dati personali fin dalla progettazione e per impostazione predefinita", in violazione degli artt. 5, par. 1, lett. e), e 25 del Regolamento.

3.8 Il principio di responsabilizzazione.

Considerata la delicatezza del trattamento di dati personali posto in essere dalla Regione, idoneo a controllare a distanza l'attività dei lavoratori e a consentire al datore di lavoro di entrare in possesso anche di informazioni relative alla sfera privata degli stessi, e tenuto conto che tale trattamento, per le ragioni sopra esposte, è stato effettuato in violazione dei principi di base in materia di protezione dei dati di cui all'art. 5, par. 1, lett. a) ed e), si ritiene che la Regione abbia, altresì, agito in maniera difforme dal principio di "responsabilizzazione", in violazione dell'art. 5, par. 2, del Regolamento (v. anche l'art. 24 del Regolamento).

3.9 La valutazione d'impatto sulla protezione dei dati.

Ai sensi dell'art. 35 del Regolamento, "quando un tipo di trattamento, allorché prevede in particolare l'uso di nuove tecnologie, considerati la natura, l'oggetto, il contesto e le finalità del trattamento, può presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento effettua, prima di procedere al trattamento, una valutazione dell'impatto dei trattamenti previsti sulla protezione dei dati personali. Una singola valutazione può esaminare un insieme di trattamenti simili che presentano rischi elevati analoghi".

In attuazione del principio di "responsabilizzazione" (cfr. art. 5, par. 2, e 24 del Regolamento), spetta al titolare valutare se i trattamenti che si intendono realizzare possano presentare un rischio elevato per i diritti e le libertà delle persone fisiche - in ragione delle tecnologie impiegate e considerata la natura, l'oggetto, il contesto e le finalità perseguite - che renda necessaria una preventiva valutazione di impatto sulla protezione dei dati personali (cfr. cons. 90 del Regolamento).

Nel caso di specie, il trattamento dei metadati relativi all'utilizzo della posta elettronica è stato effettuato anche in assenza di una preliminare valutazione d'impatto sulla protezione dei dati sul presupposto che il trattamento non presentasse rischi specifici per gli stessi.

Come, infatti, dichiarato dalla Regione nella propria memoria difensiva, la Regione ha provveduto a redigere una valutazione di impatto sulla protezione dei dati personali "relativa alla gestione dei log" soltanto successivamente all'avvio dell'istruttoria, sebbene il documento in questione non sembri riferirsi espressamente alla conservazione dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti.

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si rileva, invece, che il trattamento in questione, consistente nella sistematica raccolta di tali metadati (incluse le informazioni relative al mittente/destinatario e all'oggetto di ciascuna e-mail), nella memorizzazione per 180 giorni e nella possibilità di effettuare estrazioni, elaborazioni e verifiche su tali metadati, comporta rischi specifici per i diritti e le libertà degli interessati nel contesto

lavorativo (art. 35 del Regolamento).

Tanto in considerazione della particolare “vulnerabilità” degli interessati nel contesto lavorativo (cfr. cons. 75 e art. 88 del Regolamento e le “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”, WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menzionano espressamente “i dipendenti”) e del fatto che in tale ambito l’impiego di sistemi che comportano il “monitoraggio sistematico”, inteso come “trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti” (cfr. criterio n. 3 indicato nelle Linee guida, cit., ma vedi anche criteri 4 e 7), può presentare rischi - come emerso nel caso di specie - in termini di possibile monitoraggio dell’attività dei dipendenti (cfr. artt. 35 e 88, par. 2, del Regolamento; v. anche provv. 11 ottobre 2018, n. 467, doc. web n. 9058979, all. n. 1, che espressamente menziona i “trattamenti effettuati nell’ambito del rapporto di lavoro mediante sistemi tecnologici […] dai quali derivi la possibilità di effettuare un controllo a distanza dell’attività dei dipendenti”; v., tra gli altri, provv. 13 maggio 2021, n. 190, doc. web n. 9669974, par. 3.5).

Per tali ragioni, il trattamento dei dati personali in questione è stato effettuato dalla Regione in assenza di una valutazione di impatto e quindi in violazione dell’art. 35 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento nel corso dell’istruttoria della cui veridicità si può essere chiamati a rispondere ai sensi dell’art. 168 del Codice , seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall’Ufficio con l’atto di avvio del procedimento e risultano insufficienti a consentire l’archiviazione del presente procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall’art. 11 del Regolamento del Garante n. 1/2019.

Si confermano, pertanto, le valutazioni preliminari dell’Ufficio e si rileva l’illiceità del trattamento di dati personali effettuato dalla Regione, per aver effettuato il trattamento di dati personali in questione in violazione degli artt. 5, par. 1, lett. a) ed e), e par. 2, 6, 12, 13, 25, 35, 88, par. 1, del Regolamento, nonché 113 e 114 del Codice (in relazione agli artt. 4 e 8 della l. 300/1970).

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall’art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 3, del Regolamento medesimo, come richiamato anche dall’art. 166, comma 2, del Codice.

5. Misure correttive (art. 58, par. 2, lett. d) e f), del Regolamento).

L’art. 58, par. 2, del Regolamento attribuisce al Garante il potere di “ingiungere al titolare del trattamento o al responsabile del trattamento di conformare i trattamenti alle disposizioni del presente regolamento, se del caso, in una determinata maniera ed entro un determinato termine” (lett. d)), nonché di “imporre una limitazione provvisoria o definitiva al trattamento, incluso il divieto di trattamento” (lett. f).

Prendendo atto di quanto emerso in fase di istruttoria e tenendo conto della circostanza che dalla documentazione in atti risulta che la Regione stia tutt’ora raccogliendo e conservando per un periodo di 180 giorni i metadati relativi all’utilizzo della posta elettronica da parte dei lavoratori, si rende necessario, ai sensi dell’art. 58, par. 2, lett. d) e f), del Regolamento, disporre la limitazione del trattamento, vietando alla Regione di conservare tali dati per un periodo eccedente sette giorni dalla data della loro raccolta, in assenza dell’esperimento delle procedure di garanzia di cui all’art. 4, comma 1, della l. 300/1970, nonché disporre la cancellazione dei dati già raccolti e attualmente conservati in eccedenza del termine sopra indicato.

Ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, la Regione dovrà, inoltre, provvedere a comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ordinato ai sensi del citato art. 58, par. 2, lett. f), nonché le eventuali misure poste in essere per assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali.

6. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

In relazione ai predetti elementi, è stata considerata sia la specifica natura del trattamento – avviato in modo non conforme alla disciplina di settore in materia di impiego di strumenti tecnologici sul luogo di lavoro e alle indicazioni fornite nel tempo dal Garante, per i profili di competenza - sia la prolungata durata del trattamento, che risulta, peraltro, ancora in corso, nonostante l'avvio dell'attività istruttoria e la successiva contestazione di violazione amministrativa. È stata, altresì, tenuta in considerazione la delicatezza dei dati trattati, essendo gli stessi idonei a rivelare anche informazioni inconferenti rispetto al contesto lavorativo e relative alla vita privata.

Di contro, si è tenuta in considerazione la circostanza che, ancorché il trattamento risulti attualmente in corso, la Regione ha comunque offerto un sufficiente livello di cooperazione nel corso dell'istruttoria e che le precedenti violazioni commesse dalla Regione non possono essere considerate precedenti specifici "relativamente allo stesso oggetto" (art. 83, par. 2, lett. i) del Regolamento) rispetto alla condotta in esame, la quale si riferisce a trattamenti effettuati per finalità eterogenee a quelle oggetto dei precedenti provvedimenti del Garante.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 100.000,00 (centomila) per la violazione degli artt. 5, par. 1, lett. a) ed e), e par. 2, 6, 12, 13, 25, 35, 88, par. 1, del Regolamento, nonché 113 e 114 del Codice (in relazione agli artt. 4 e 8 della l. 300/1970), quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto che la raccolta generalizzata dei dati personali relativi a lavoratori è tutt'ora in corso, in assenza dei presupposti di liceità previsti dalla disciplina di settore, si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente

provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara, ai sensi dell'art. 57, par. 1, lett. f), del Regolamento, l'illiceità del trattamento effettuato dalla Regione per violazione degli artt. 5, par. 1, lett. a) ed e), e par. 2, 6, 12, 13, 25, 35, 88, par. 1, del Regolamento, nonché 113 e 114 del Codice (in relazione agli artt. 4 e 8 della l. n. 300/1970), nei termini di cui in motivazione;

ORDINA

ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, alla Regione Lazio, con sede legale in Via Cristoforo Colombo, 212 - 00147 Roma (RM), C.F. 80143490581, di pagare la somma di euro 100.000,00 (centomila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Regione:

a) di pagare la somma di euro 100.000,00 (centomila) in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

b) ai sensi dell'art. 58, par. 2, lett. d) e f) del Regolamento, la limitazione del trattamento, vietando alla Regione ogni ulteriore operazione di trattamento con riguardo ai metadati relativi all'utilizzo della posta elettronica da parte dei lavoratori, conservati per un periodo eccedente a sette giorni dalla data della loro raccolta, in assenza dell'esperimento delle procedure di garanzia di cui all'art. 4, comma 1, della l. 300/1970, nonché la cancellazione dei dati già raccolti e attualmente conservati in eccedenza del termine sopra indicato;

c) ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, di comunicare a questa Autorità, fornendo un riscontro adeguatamente documentato, entro trenta giorni dalla notifica del presente provvedimento, le iniziative intraprese al fine di dare attuazione a quanto sopra ordinato ai sensi del citato art. 58, par. 2, lett. f), nonché le eventuali misure poste in essere per assicurare la conformità del trattamento alla normativa in materia di protezione dei dati personali.

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice (v. art. 16 del Regolamento del Garante n. 1/2019);

l'annotazione del presente provvedimento nel registro interno dell'Autorità, previsto dall'art. 57, par. 1, lett. u), del Regolamento, delle violazioni e delle misure adottate in conformità all'art. 58, par. 2, del Regolamento (v. art. 17 del Regolamento del Garante n. 1/2019).

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. n. 150/2011, avverso il presente provvedimento è possibile proporre ricorso dinnanzi all'autorità giudiziaria ordinaria, a pena di inammissibilità, entro trenta giorni dalla data di comunicazione del provvedimento stesso ovvero entro sessanta giorni se il ricorrente risiede all'estero.

Roma, 1° dicembre 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei