Provvedimento del 29 aprile 2025 [10134221]

[doc. web n. 10134221]

Provvedimento del 29 aprile 2025

Registro dei provvedimenti
n. 243 del 29 aprile 2025

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 dott. Claudio Filippi, segretario generale reggente;

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 reggente 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.

Nell'ambito di accertamenti avviati d'ufficio al fine di verificare l'osservanza delle norme in materia di protezione dei dati personali in relazione ai trattamenti posti in essere in ambito lavorativo, anche con riferimento alle modalità di svolgimento del cd. "lavoro agile", l'Autorità ha condotto un'attività ispettiva, ai sensi dell'art. 58, par. 1, del Regolamento e degli artt. 157 e 158 del Codice,

nei confronti della Regione Lombardia.

2. L'attività istruttoria.

Dagli accertamenti ispettivi effettuati (cfr. verbali del XX, XX e XX, in atti) è emerso, in particolare, che:

l'utilizzo della strumentazione informatica da parte del personale "è regolato dal "Decreto regole per l'utilizzo degli strumenti info-telematici" n. XX del XX della Giunta regionale"; con più specifico riguardo alla modalità di lavoro agile, "non sono state previste regole diverse per il trattamento da remoto rispetto a quello in presenza […]";

la navigazione in Internet effettuata dai dipendenti "è libera ad eccezione dei siti presenti in una black list costantemente aggiornata"; "sono conservati tutti i log relativi alla navigazione effettuata, compresi i tentativi falliti di accesso ai predetti siti" (v. successiva nota del XX); "in caso di richieste motivate, sono messi a disposizione della sola autorità giudiziaria. È possibile risalire alla navigazione effettuata da una particolare macchina tramite ricongiunzione delle informazioni (conservate separatamente) di utente e IP della macchina come indicato [… nel] decreto XX. Tale ricongiunzione viene effettuata anche nel caso in cui i sistemi rilevino particolari anomalie di traffico […] il predetto decreto è stato adottato a seguito di un percorso di condivisione con i sindacati e richiamato nel medesimo decreto. In ogni caso non è stato stipulato un accordo con i sindacati ai sensi dell'articolo 4 comma 1 della Legge 300/1970 atteso che […] la Regione ritiene che i trattamenti effettuati in proposito non sono riconducibili ai controlli a distanza che rientrano nell'ambito di applicazione di quella norma [… e] i sindacati non hanno richiesto l'attivazione di tavoli di contrattazione […;] i log relativi alla navigazione Internet sono conservati per 12 mesi sui server di ARIA, nominato responsabile del trattamento, nell'ambito della convenzione quadro per la gestione dell'infrastruttura tecnologica in cui sono compresi il networking, gestione servizio navigazione sicura, con specifico incarico";

il servizio di posta elettronica (Microsoft 365) "è gestito da ARIA mediante incarico specifico nell'ambito della convenzione"; "i log del servizio di posta elettronica (metadati) sono raccolti da ARIA e conservati per 90 gg per consentire l'eventuale assistenza tecnica e […] nessun dipendente ha accesso ai medesimi log"; la Regione ha successivamente "precisato che, anche alla luce del provvedimento del Garante nei confronti della regione Lazio di XX sul trattamento dei metadati relativi all'utilizzo della posta elettronica da parte dei dipendenti, la Regione ha avviato, al proprio interno, una riflessione su impulso del DPO che ha coinvolto la Giunta e il responsabile del trattamento ARIA, per gli aspetti di competenza";

la Regione ha dichiarato che "non sono mai stati utilizzati i log della navigazione Internet e posta elettronica per verificare il comportamento di un dipendente"; la Regione ha aggiunto che, nell'ultimo quinquennio, "sono stati avviati due procedimenti disciplinari nei confronti dei dipendenti uno per presunto uso dei dispositivi non conforme al [predetto] decreto [XX] e uno per presunto comportamento non adeguato alle istruzioni impartite nel trattamento dei dati";

in ordine alle modalità di gestione del servizio di assistenza tecnica per i dipendenti (in sede o in lavoro agile), all'epoca degli accertamenti ispettivi in esame era previsto "un numero telefonico dedicato all'assistenza tecnica", il quale "con il nuovo contratto [sarebbe stato] affiancato da un apposito portale accessibile da intranet e Internet"; al riguardo, la Regione ha altresì dichiarato che "poiché in tutte le direzioni c'è un referente informatico i dipendenti possono rivolgersi a tale figura per l'apertura di ticket di assistenza tecnica. Il servizio help desk, si avvale della piattaforma SDAS […]. Tale servizio è gestito da operatori da remoto che o risolvono la problematica durante la chiamata dell'utente o inoltrano il ticket al supporto da remoto o on site […]. Per ogni ticket viene inviata al dipendente richiedente una

mail di apertura e una di chiusura"; "i ticket vengono mantenuti nel sistema di gestione ticket per tutta la durata del contratto, in particolare i dati del nuovo sistema SDAS saranno conservati per 78 mesi (6 anni + ulteriori 6 mesi necessari per espletare le attività contrattuali residuali quali contabilità, pagamenti, verifica della regolare esecuzione del contratto) come previsto in atto nomina. Mensilmente si tiene una riunione fra fornitori e struttura dei sistemi informativi (SAL) per verificare l'avanzamento dei lavori e fare il punto della situazione, monitorare gli SLA, individuare eventuali criticità quali numero eccessivo di ticket, particolari e ripetute problematiche che, di regola, non prevedono il trattamento di dati personali identificativi"; "al sistema di gestione ticket, oltre al personale della società fornitrice, accedono alcuni dipendenti della struttura dei sistemi informativi, individuati in base a specifiche mansioni, con visibilità su tutti i ticket aperti dai dipendenti dell'Ente nonché i referenti informatici delle direzioni, questi ultimi con visibilità solo sugli asset della direzione";

fino al XX era in uso il sistema OTRS - Open Source Help Desk System, che, tuttavia, all'epoca degli accertamenti ispettivi, risultava essere ancora "utilizzato dal personale del nuovo fornitore subentrato nel contratto di servizio per la gestione degli asset ancora non sostituiti come da nuovo contratto e dei ticket ancora aperti prima del XX" e sarebbe stato utilizzato, altresì, "fino a completa dismissione degli asset gestiti nel vecchio contratto, [a seguito della quale] tutti i dati [sarebbero stati] cancellati".

In relazione agli aspetti sopra indicati, con successiva nota, pervenuta in data XX, la Regione, anche a scioglimento delle riserve formulate in sede ispettiva, ha rappresentato, in particolare, quanto segue:

- relativamente alla conservazione dei log generati dalla navigazione in Internet del personale dipendente, "Aria – gestore del servizio proxy – conserva i log di navigazione con la sola informazione relativa all'indirizzo IP della macchina. Il gestore della rete (Fastweb) possiede l'informazione relativa all'associazione tra l'IP della macchina e il MAC ADDRESS della macchina stessa. Il gestore delle PdL (Engineering) possiede l'informazione relativa all'associazione tra il MAC ADDRESS della macchina e il nome dell'utente assegnatario della macchina stessa. Singolarmente nessun gestore, quindi, è in grado di risalire autonomamente all'informazione completa tra la navigazione effettuata e l'utente che l'ha eseguita";

- "le tipologie di allarmi di sicurezza costantemente analizzati in modo automatico ed anonimo consistono in: attacchi DoS/DDoS; postazioni e server infette; tentativi di attacco a sistemi e/o applicazioni e/o servizi; sfruttamento di vulnerabilità; sistemi collegati a Botnet; esfiltrazione di dati; intrusioni; compromissione di sistemi e/o applicazione e/o servizi; modifica o cancellazione non autorizzata di dati; invio di e-mail di phishing; comunicazione con IP, domini, URL riconducibili ad attività malevole. Al verificarsi di una di queste tipologie viene valutata la probabilità che questo allarme possa generare un danno effettivo all'infrastruttura (e alle informazioni ivi contenute). Solo il verificarsi di questa condizione fa scattare la procedura di analisi approfondita che come estrema ratio prevede l'individuazione della postazione infetta. Negli ultimi 12 mesi non si sono verificati casi che hanno determinato un alert tale da dover attivare la procedura di ricongiunzione";

- con riguardo ai metadati generati dall'utilizzo del servizio di posta elettronica da parte del personale dipendente della Regione, "gli amministratori del tenant di posta elettronica hanno la possibilità di condurre un'operazione di tracciamento della posta transitata dal server Exchange. Le informazioni che Microsoft permette di raccogliere sulla base di questa ricerca sono disponibili per 7 giorni direttamente sul server, e comprendono: data e ora del messaggio; indirizzo del mittente; Indirizzo del destinatario; oggetto della mail; status (informazione sulla corretta consegna del messaggio o, in alternativa, sulla motivazione per

cui non è stato correttamente recapitato); dimensione del messaggio (espressa in KB o in MB, includendo la dimensione di eventuali allegati); header del messaggio (file di testo contenente identificativo univoco del messaggio e informazioni riguardo il transito)"; "per le email più vecchie di 7 giorni, Microsoft permette di raccogliere una quantità minore di informazioni attraverso un report in formato CSV. Le informazioni acquisibili in questa modalità restano disponibili agli amministratori per 90 giorni, e comprendono: timestamp del messaggio; indirizzo del mittente; indirizzo del destinatario con eventuale status (in questo report si acquisiscono solo le email ricevute dal server e indirizzate verso la destinazione, non vengono tracciate le mail che il server blocca a monte); oggetto della mail; dimensione del messaggio (espressa in bytes, includendo la dimensione di eventuali allegati); identificativo univoco del messaggio"; "il parametro dei 90 giorni di retention è impostato da Microsoft (condizioni di rilascio della licenza) e gli amministratori non hanno la possibilità di diminuirlo. Le informazioni messe a disposizione dal tracciamento servono unicamente allo scopo di offrire assistenza agli utenti nel momento in cui un messaggio non viene recapitato correttamente"; per quanto più specificamente concerne i profili di applicabilità della normativa in materia di impiego di controlli a distanza dei lavoratori, la Regione ha evidenziato che "il personal computer e la casella di posta elettronica forniti dall'Amministrazione ai dipendenti sono necessari per lo svolgimento dell'attività lavorativa quotidiana e, pertanto, devono considerarsi come gli strumenti di lavoro essenziali. L'Amministrazione, proprio sulla base della distinzione tra strumenti di controllo di cui al comma 1 e strumenti di lavoro di cui al comma 2, ha ritenuto che non fossero necessari gli adempimenti di natura sindacale di cui al comma 1. L'Amministrazione, considerato quanto emerso durante l'ispezione, sta valutando le modalità con cui affrontare la questione sui tavoli sindacali, rappresentando preliminarmente alle RSU gli aspetti vincolanti derivanti dalla licenza Microsoft";

- con riferimento alle soluzioni atte a garantire l'osservanza dei principi di minimizzazione e limitazione della conservazione dei dati trattati dal servizio di assistenza tecnica, "preliminarmente va osservato che i dati generati dal sistema di ticketing sono di natura operativa e vengono consultati ai fini dell'assistenza e della gestione amministrativa dei Service Level Agreement (SLA). In particolare, durante il tavolo tecnico immediatamente è stato richiesto al Fornitore di verificare la possibilità tecnica di conservare le informazioni relative ai ticket superiori ai 12 mesi in modalità anonima, per le finalità di amministrative legate alla gestione del contratto. In pratica, per 12 mesi potranno essere conservate le basi dati complete, comprensive dei dati identificativi dell'utente e l'oggetto della richiesta, per garantire un adeguato servizio di assistenza. Successivamente, dopo i 12 mesi, i dati identificativi degli utenti e degli operatori saranno resi anonimi, con possibilità di conservazione e utilizzo delle basi dati anonimizzate per finalità amministrative";

- con riferimento all'avvicendamento dei fornitori incaricati dell'erogazione del servizio di assistenza tecnica al personale dipendente e all'accesso ai dati contenuti nel sistema OTRS, in fase di dismissione, a scioglimento delle riserve formulate a verbale, la Regione ha dichiarato che "ritiene di adottare un addendum [… agli accordi stipulati ai sensi dell'art. 28 del Regolamento] al fine di regolamentare il trattamento dei dati pregressi contenuti nel vecchio sistema di ticketing fino a completa dismissione degli asset e alla formattazione dell'ambiente relativi alla precedente fornitura"; la Regione ha quindi trasmesso all'Autorità la bozza del suddetto addendum contrattuale in corso di formalizzazione con i fornitori del nuovo sistema SDAS.

A valle dell'attività ispettiva nonché, in particolare, dell'esame della documentazione integrativa successivamente trasmessa da parte della Regione anche a scioglimento delle riserve formulate in sede di ispezione, l'Ufficio, nel rilevare la necessità di acquisire ulteriori elementi e precisazioni ritenuti indispensabili al fine di completare il quadro istruttorio, ha rivolto alla Regione una richiesta

di ulteriori informazioni e chiarimenti, a cui è stato fornito riscontro, in tempi diversi e con successive comunicazioni, anche al fine di documentare all'Autorità le misure progressivamente adottate dalla Regione per conformare i trattamenti alla disciplina di protezione dei dati (cfr. note del XX, XX, XX e XX).

In particolare, nel dare atto con nota del XX di essere addivenuta in data XX alla stipula dell'accordo collettivo ai sensi dell'art. 4, comma 1, della l. 20 maggio 1970, n. 300, con le organizzazioni sindacali rappresentative del solo personale non dirigenziale, la Regione ha trasmesso copia del predetto accordo all'Autorità, allegando altresì evidenza dello svolgimento della valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento e dell'informativa resa ai sensi dell'art. 13 del Regolamento. Ha inoltre dichiarato che "è in fase di perfezionamento l'aggiornamento al Decreto infotelematico al fine di renderlo coerente con gli atti sottoscritti".

Successivamente, con nota del XX, la Regione, con riguardo al personale dirigenziale, ha altresì trasmesso copia di un separato accordo stipulato il XX ai sensi dell'art. 4, comma 1, della l. 20 maggio 1970, n. 300 con le organizzazioni sindacali rappresentative del personale dirigenziale nonché del predetto Decreto n. XX del XX relativo all'aggiornamento del documento "Regole per l'utilizzo dei servizi infotelematici della Giunta Regionale".

Con nota del XX, l'Ufficio, sulla base degli elementi acquisiti dalle verifiche compiute e dei fatti emersi nell'ambito dell'attività istruttoria, ha notificato alla Regione Lombardia, 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 sul presupposto che il trattamento dei dati personali in questione fosse stato posto in essere:

> in ragione dell'inosservanza della disciplina di settore in materia di controlli a distanza in riferimento alla conservazione dei metadati generati dall'attività del personale dipendente relativamente sia all'utilizzo del servizio di posta elettronica che alla navigazione in Internet, 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. 20 maggio 1970, n. 300);
>
> stante il mancato rispetto delle condizioni previste dalla disciplina di settore con riguardo all'utilizzo dei metadati raccolti per altri fini connessi alla gestione del rapporto di lavoro, in violazione degli artt. 5, par. 1, lett. a), 6 e 88 del Regolamento e 114 del Codice (in relazione all'art. 4, comma 3, della legge n. 300 del 1970);
>
> in ragione dell'eccedenza dei tempi di conservazione dei log relativi alla navigazione in Internet nonché dei dati relativi alle richieste di assistenza tecnica, in violazione degli artt. 5, par. 1, lett. e), e 25 del Regolamento;
>
> stante la raccolta di dati non attinenti all'attività lavorativa con riferimento alla conservazione dei log di navigazione in Internet, in violazione degli artt. 5, par. 1, lett. a), c), 6, 88, par. 1, del Regolamento nonché 113 del Codice (in relazione agli artt. 8 della l. 20 maggio 1970, n. 300 e 10 del d.lgs. n. 276/2003);
>
> in mancanza dello svolgimento di una valutazione d'impatto sulla protezione dei dati con riferimento al trattamento dei metadati relativi all'utilizzo della posta elettronica e dei log relativi alla navigazione in Internet, in violazione dell'art. 35 del Regolamento;
>
> stante l'inadeguata regolamentazione ai sensi dell'art. 28 del Regolamento del rapporto con i fornitori del servizio di assistenza tecnica in riferimento al trattamento dei dati personali contenuti nel sistema OTRS, in violazione dell'art. 28 del Regolamento.

Con la medesima nota, il predetto titolare è stato invitato a produrre al Garante scritti difensivi o

documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice, nonché art. 18, comma 1, della l. 24 novembre 1981, n. 689).

Con nota del XX, la Regione Lombardia ha presentato una memoria difensiva, dichiarando, in particolare, che:

> "il datore di lavoro […] ha utilizzato sistemi che determinano un trattamento di dati personali riferiti o riferibili ai lavoratori solo ed esclusivamente per finalità necessarie ad assicurare il funzionamento delle infrastrutture e di natura prettamente tecnica, come il rilevamento delle anomalie, sospetto attacco informatico o per manutenzione, nel rispetto dell'art. 4, secondo comma, dello Statuto dei lavoratori e in linea con quanto contenuto nell'art. 32 comma 1 lett. d) del GDPR";
>
> "Regione Lombardia riteneva che la conservazione dei metadati pari a 90 giorni per finalità di natura tecnica, relativo al corretto funzionamento e regolare utilizzo del sistema di posta elettronica […], insieme ad una corretta e trasparente informazione dei lavoratori, con controlli anonimi, indiretti e graduali, potesse bastare a rientrare nell'ambito applicativo del secondo comma dell'art 4 dello Statuto dei lavoratori. Solo con il provvedimento nei confronti di Regione Lazio del mese di XX, l'Autorità Garante ha [… indicato] uno specifico ambito temporale oltre al quale viene presunto che si applichi il comma 1 dell'art. 4 dello Statuto dei lavoratori. Prima di tale provvedimento, l'Autorità Garante non aveva mai indicato un termine preciso che fungesse da spartiacque per la determinazione della sfera di applicazione tra primo e secondo comma dell'art. 4 dello Statuto dei lavoratori.[…] Solo dopo la consultazione pubblica, precisamente nel mese di XX l'Autorità Garante, seppure in linea con la precedente interpretazione ha rivisto il tempo di conservazione dei metadati della posta elettronica, passando da 7 a 21 giorni, rendendo in tal modo effettivamente applicabile il documento di indirizzo nei confronti di tutti i titolari del trattamento, la cui efficacia veniva sospesa durante il periodo di consultazione pubblica";
>
> "Regione Lombardia che da sempre, anche con il supporto dell'ufficio privacy e del DPO, pone particolare attenzione ai provvedimenti del Garante, anche a seguito dell'attività ispettiva nei confronti della Regione Lazio e a fronte di questa ulteriore specifica temporale prevista dall'Autorità Garante, successivamente cristallizzata con la pubblicazione del documento di indirizzo "Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati" a XX, ha ponderato la predisposizione di un adeguamento, sottoscrivendo, all'esito di un percorso sindacale di confronto, l'accordo con le rappresentanze sindacali, raggiunto in data XX per il personale del comparto ed in data XX per il personale dirigenziale, in relazione alla conservazione dei metadati di posta elettronica e ai log della navigazione Internet, rivedendo l'impostazione precedente, anche relativamente al decreto infotelematico, condiviso con spirito di piena collaborazione con l'Autorità Garante";
>
> per quanto riguarda la conservazione dei file di log relativi alla navigazione in Internet, "Regione Lombardia non ha mai messo in atto controlli massivi, prolungati, costanti e indiscriminati in relazione ai propri dipendenti utilizzando le informazioni raccolte, senza mai utilizzare informazioni personali, anche non pertinenti o idonei a rivelare convinzioni religiose, filosofiche o di altro genere, opinioni politiche, lo stato di salute o la vita sessuale. […] Regione Lombardia attraverso le proprie Regole aveva messo in atto delle misure tecniche ed organizzative che impedivano agli operatori della stessa di risalire autonomamente all'informazione completa tra la navigazione effettuate e l'utente che l'ha eseguita. La conservazione ha sempre e solo riguardato dati anonimi e conservati in forma disgiunta presso i singoli fornitori. […] Inoltre, […] solo il verificarsi [… delle condizioni già indicate con nota del XX, concernenti talune "tipologie di allarmi di sicurezza"] faceva scattare la procedura di analisi approfondita che, come extrema ratio, prevedeva

l’individuazione della postazione infetta, anche in coerenza con quanto previsto dalle Linee Guida [… dell’]Autorità del 2007. […] La misura di sicurezza tecnica della necessità di ricongiunzione, tesa a garantire un’effettiva minimizzazione dei dati personali, esclude un controllo dei lavoratori”;

sempre con riferimento alla conservazione dei file di log relativi alla navigazione Internet, “dal punto di vista tecnico, […] nel progettare un’efficace strategia di Incident Response, l’amministrazione regionale si è basata anche su un approccio metodico, a partire innanzitutto da una corretta identificazione degli incidenti. Sempre più attacchi, infatti, non generano immediatamente un allarme di sicurezza (come, ad esempio, un picco dell’utilizzo della banda della rete) ma sono composti da tante piccole azioni che sfruttano l’utilizzo della connettività Internet (es. chiamate in orari anomali, ripetuti in più periodi ecc.) che solo analizzate complessivamente nel tempo consentono di risalire all’origine dell’attacco. Gli attacchi di tipo APT (Advanced Persistent Threat) sono noti per la loro durata estesa nel tempo. A differenza degli attacchi tradizionali, gli APT non mirano a ottenere un accesso rapido e immediato, ma piuttosto a infiltrarsi in una rete in modo discreto e rimanervi a lungo per raccogliere informazioni sensibili o causare danni su vasta scala ovvero recuperare tutte le informazioni necessarie a scatenare attacchi di tipo Ransomware che, come è noto, minano in un solo colpo, l’integrità, la disponibilità e, in caso di furto prima dell’attacco, la riservatezza dei dati trattati. L’analisi dei log della navigazione è uno dei fattori da tenere in considerazione per valutare comportamenti anomali potenzialmente pericolosi nel lungo periodo. In media, un attacco APT può durare diversi mesi o anche anni.”;

quanto alla contestazione relativa all’utilizzo dei metadati per fini disciplinari in assenza delle condizioni previste dalla disciplina di settore al riguardo, la Regione, nel fornire ulteriori elementi, ha reso precisazioni in merito alle precedenti dichiarazioni rese, specificando che “nessuno dei due procedimenti disciplinari è stato avviato per il tramite dell’utilizzo dei log della posta elettronica o della navigazione in Internet”;

con riguardo alla definizione del tempo di conservazione dei dati relativi alle richieste di assistenza tecnica del personale dipendente a seguito della chiusura dei ticket, “all’interno della organizzazione regionale anonimizzare/cancellare ogni singolo ticket al momento della chiusura dello stesso non garantirebbe un servizio di assistenza adeguato in quanto, nel caso, in cui un singolo utente segnali anomalie ricorrenti non sarebbe possibile analizzare e risolvere compiutamente la problematica”;

quanto al mancato svolgimento di una valutazione d’impatto sulla protezione dei dati ai sensi dell’art. 35 del Regolamento con riferimento al trattamento dei metadati relativi all’utilizzo della posta elettronica e dei log della navigazione in Internet, “secondo 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], nella maggior parte dei casi un titolare del trattamento può considerare che un trattamento che soddisfi due criteri debba formare oggetto di una valutazione d'impatto sulla protezione dei dati. Nel caso che ci occupa, risulta applicabile esclusivamente il criterio numero 7 in relazione ai dati relativi a interessati vulnerabili, mentre, a parere di questa Amministrazione, non risultano assolutamente applicabili i criteri numero 3 (monitoraggio sistematico) e numero 8 (uso innovativo o applicazione di nuove soluzioni tecnologiche od organizzative)”;

quanto alla rilevata carenza di taluni degli elementi essenziali dell’accordo di cui all’art. 28 del Regolamento con i fornitori incaricati dell’erogazione del servizio di assistenza tecnica, “la nomina principale a responsabile del trattamento da parte dei tre fornitori del servizio di assistenza tecnica […] descriveva […] l’attività di assistenza tecnica individuando compiutamente la materia disciplinata, la natura e la finalità del trattamento, il tipo di dati

personali e le categorie di interessati, pur senza specificare adeguatamente lo strumento a supporto e le date di riferimento. A seguito di quanto emerso durante l'ispezione del Garante, si è ritenuto opportuno prevedere un addendum alla nomina in essere per meglio chiarire che le stesse attività descritte nel trattamento [… in questione] venivano effettuate anche attraverso il sistema di ticketing OTRS ".

Infine, con successiva nota del XX, la Regione ha comunicato di non volersi avvalere della facoltà di prendere parte all'audizione ai sensi dell'art. 166, comma 6, del Codice.

3. La normativa applicabile: la disciplina in materia di protezione dei dati personali in ambito lavorativo e lo svolgimento dell'attività lavorativa in modalità agile.

In base alla disciplina in materia di protezione dei dati personali, il datore di lavoro può trattare i dati personali dei lavoratori, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1, del Regolamento), 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).

In tale quadro, ai trattamenti di dati personali effettuati nell'ambito dell'esecuzione del contratto di lavoro subordinato in modalità agile – regolato da una disciplina volta a favorire l'adozione di nuove modalità di organizzazione del lavoro basate sulla flessibilità spazio-temporale, sulla valutazione per obiettivi e sulla conciliazione della vita lavorativa con quella privata (artt. da 18 a 23 della legge 22 maggio 2017, n. 81) - trovano applicazione le medesime basi giuridiche sopra richiamate che ricorrono tipicamente in ambito lavorativo.

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. 20 maggio 1970, n. 300 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/dataprotection/data-protection-eu/eu-countries-gdpr-specific-notifications_en) ai sensi dell'art. 88, par. 3, del Regolamento - 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.

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).

4. L’esito dell’attività istruttoria.

4.1. Il trattamento dei metadati di posta elettronica.

Dagli elementi acquisiti nell’ambito della complessa attività istruttoria risulta accertato, in particolare, che, in virtù dell’adozione del decreto n. XX del XX(recante “Regole per l’utilizzo degli strumenti infotelematici della giunta regionale”), i metadati di posta elettronica venivano conservati dalla Regione, in assenza della previa stipulazione di un accordo collettivo con le rappresentanze sindacali (cfr. art. 4, comma 1, della l. 20 maggio 1970, n. 300), per un ampio periodo temporale, complessivamente pari a 90 giorni, per finalità di sicurezza informatica e assistenza tecnica nonché “allo scopo di offrire assistenza agli utenti nel momento in cui un messaggio non viene recapitato correttamente” (v. nota del XX; v. anche, in senso analogo, nota del XX).

Risulta, tuttavia, che, nel corso dell’istruttoria, la Regione, anche tenuto conto delle indicazioni del proprio Responsabile della protezione dei dati, ha dato atto di essere addivenuta alla stipula, in relazione ai trattamenti in questione, di un accordo collettivo con le competenti parti sindacali in data XX per quanto concerne il personale non dirigenziale e in data XX per quanto invece riguarda il personale dirigenziale.

Al riguardo, si rappresenta in via generale che, sin dal 2007, il Garante si è nel tempo occupato dei trattamenti posti in essere dal datore di lavoro e aventi ad oggetto i dati personali relativi all’utilizzo da parte dei dipendenti dei servizi di rete, con particolare riguardo al servizio di posta elettronica e alla navigazione in Internet, anche con provvedimenti a carattere generale (v. “Linee guida del Garante per posta elettronica e Internet” del 1° marzo 2007, n. 13, doc. web n. 1387522, le quali, ancorché riferite al previgente quadro normativo, contengono principi e indicazioni ancora validi). Più di recente, anche sulla base di specifiche decisioni su singoli casi concreti (provv. 1° dicembre 2022, n. 409, doc. web n. 9833530, e provv. 13 luglio 2016, n. 303, doc. web n. 5408460, quest’ultimo confermato dal Tribunale di Chieti con sent. n. 672 del 24 ottobre 2019), il Garante ha affrontato il delicato tema della conservazione dei metadati di posta elettronica, fornendo, da ultimo, indicazioni e chiarimenti volti ad orientare le scelte organizzative e tecniche dei datori di lavori con il “Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”, adottato, a seguito di consultazione pubblica, con provv. del 6 giugno 2024, n. 364, doc. web n. 10026277.

In particolare, i metadati di posta elettronica, che corrispondono tecnicamente alle informazioni registrate nei log generati dai sistemi server di gestione e smistamento della posta elettronica e dalle postazioni nell’interazione che avviene tra i diversi server interagenti e, se del caso, tra questi e i client, comprendono generalmente gli indirizzi email del mittente e del destinatario, gli indirizzi IP dei server o dei client coinvolti nell’instradamento del messaggio, gli orari di invio, di ritrasmissione o di ricezione, la dimensione del messaggio, la presenza e la dimensione di eventuali allegati e, in certi casi, a seconda del sistema di gestione del servizio di posta elettronica utilizzato, anche l’oggetto del messaggio spedito o ricevuto.

I metadati di posta elettronica risultano assistiti da garanzie di segretezza, tutelate anche costituzionalmente (artt. 2 e 15 Cost.), intese ad assicurare protezione al nucleo essenziale della dignità della persona e al pieno sviluppo della sua personalità nelle formazioni sociali.

Ciò comporta che, anche nel contesto lavorativo, sussista una legittima aspettativa di riservatezza in relazione alla corrispondenza e, analogamente, agli elementi ricavabili dai dati esteriori della stessa, che ne definiscono i profili temporali (come la data e l’ora di invio/ricezione) nonché gli 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 (v. punto 2 del predetto Documento di indirizzo; punto 5.2 lett. b), delle Linee guida citate; v. anche provv. 1° dicembre 2022, n. 409, doc. web n. 9833530 e provv. 13 luglio 2016, n. 303, doc. web n.

5408460).

La disciplina nazionale più specifica ai sensi dell'art. 88 del Regolamento individua tassativamente le finalità (ovvero quelle organizzative, produttive, di sicurezza del lavoro e di tutela del patrimonio aziendale) per le quali gli strumenti, dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori, possono essere impiegati nel contesto lavorativo, stabilendo precise garanzie procedurali (accordo sindacale o autorizzazione pubblica; cfr. art. 114 del Codice, che richiama l'art. 4, comma 1, l. 20 maggio 1970, n. 300, come modificato dal d.lgs. 14 settembre 2015, n. 151).

Sebbene la Regione abbia dichiarato in un primo momento che la posta elettronica venga utilizzata dal personale dipendente per rendere la prestazione lavorativa, tuttavia, alla luce del quadro normativo nazionale di settore, nella nozione di "strumenti utilizzati dal lavoratore per rendere la prestazione lavorativa" (ai sensi e per gli effetti dell´art. 4, comma 2, della l. n. 300/1970) - che costituisce un'eccezione, rispetto al comma 1 e come tale deve essere oggetto di stretta interpretazione, stante altresì le responsabilità anche sul piano penale che ne conseguono - possono ricomprendersi solo servizi, software o applicativi strettamente funzionali alla prestazione lavorativa.

Tali principi hanno trovato applicazione in numerosi provvedimenti del Garante, con riferimento ai contesti di lavoro pubblici e privati, nei quali è stato affrontato il tema del discrimine tra il comma 1 e il comma 2 dell'art. 4 della l. n. 300/1970 e del diverso regime giuridico che ne discende, valutando, di volta in volta, la specificità dei trattamenti e dei sistemi utilizzati in concreto dal datore di lavoro. Ciò, anche alla luce degli orientamenti della giurisprudenza, del Ministero del lavoro e dell'Ispettorato Nazionale del lavoro, che applicano tale disciplina nell'ambito delle proprie funzioni istituzionali di controllo, ritenendo non applicabile l'eccezione del comma 2 e trovando invece applicazione il comma 1, nei casi in cui, ad esempio, il sistema agisca con modalità non percepibili dal lavoratore e in modo del tutto indipendente rispetto alla normale attività dello stesso oppure in presenza di sistemi che non sono solo funzionali alla prestazione ma consentono anche ulteriori elaborazioni da parte del datore di lavoro per il perseguimento di proprie finalità e specie nei casi in cui tali funzionalità non possano essere disabilitate dal dipendente (cfr., tra i numerosi provvedimenti in ambito pubblico, in particolare, provv. 28 ottobre 2021, n. 384, doc. web n. 9722661 nonché INL, circolare n. 4 del 26 luglio 2017; provv. 13 maggio 2021, n. 190, doc. web n. 9669974; provv. 16 novembre 2017, n. 479, doc. web n. 7355533; provv. 13 luglio 2016, n. 303, doc. web 5408460; v. anche i numerosi provvedimenti citati, nel contesto pubblico e privato, nelle Relazioni annuali del Garante 2017-2023).

Tali caratteristiche ricorrono nel caso del trattamento dei metadati di posta elettronica, qualora gli stessi siano raccolti e conservati, in modo preventivo e generalizzato, per un esteso arco temporale dai programmi e servizi informatici per la gestione della posta elettronica. Ciò in quanto tali operazioni di trattamento sono effettuate, per esigenze proprie del datore di lavoro, automaticamente e indipendentemente dalla percezione e dalla volontà del lavoratore; inoltre, i predetti metadati rimangono nella disponibilità esclusiva del datore di lavoro e, per suo conto, del fornitore del servizio, documentando il traffico anche dopo l'eventuale cancellazione del messaggio da parte del lavoratore, il quale, invece, mantiene la disponibilità dei messaggi che, in qualità di mittente o destinatario, scambia all'interno della casella di posta assegnatagli dal datore di lavoro, con la conseguenza che in tali casi sussiste il rischio di un indiretto controllo a distanza dell'attività dei lavoratori. Per tali ragioni, in tali casi non può essere generalmente invocata l'eccezione di cui al comma 2 dell'art. 4, trovando invece di regola applicazione il comma 1 (v. anche Documento di indirizzo, par. 3, cit., e provv.ti ivi citati).

In tale quadro, affinché sia ritenuto applicabile il comma 2 dell'art. 4 della l. 20 maggio 1970, n. 300, l'attività di raccolta e conservazione dei soli metadati necessari ad assicurare il funzionamento delle infrastrutture del sistema della posta elettronica e il soddisfacimento delle più

essenziali garanzie di sicurezza informatica, all'esito di valutazioni tecniche e nel rispetto del principio di responsabilizzazione, si ritiene che possa essere effettuata, di norma, per un periodo limitato a pochi giorni, comunque non superiore ai 21 giorni, salvo che il titolare, sempre nel perseguimento della predetta finalità riconducibile all'alveo del comma 2 dell'art. 4 della l. 20 maggio 1970, n. 300, comprovi adeguatamente la ricorrenza in concreto di particolari condizioni che ne rendano necessaria l'estensione in ragione delle specificità della propria realtà tecnica e organizzativa.

Diversamente, la generalizzata raccolta e la conservazione dei metadati di posta elettronica, per un lasso di tempo più esteso, in presenza di esigenze comunque riconducibili alla sicurezza e alla tutela del patrimonio anche informativo del datore di lavoro, potendo comportare un indiretto controllo a distanza dell'attività dei lavoratori, richiede l'esperimento delle garanzie previste dall'art. 4, comma 1, della predetta l. 20 maggio 1970, n. 300 (v. provv. 1° dicembre 2022, n. 409, doc. web n. 9833530 e provv. 13 luglio 2016, n. 303, doc. web n. 5408460; tali principi sono stati da ultimo ribaditi nel punto 3 del predetto Documento di indirizzo).

Preso atto, dunque, che, nel caso di specie, i predetti metadati di posta elettronica, relativi ai messaggi scambiati dai lavoratori tramite gli account individualmente assegnati, venivano – e vengono tuttora - conservati dalla Regione per 90 giorni, deve ritenersi, come peraltro confermato dalla stessa Regione, che entro i margini di tale ampio intervallo temporale, la finalità di trattamento in concreto perseguita non possa essere ricondotta soltanto all'ambito del mero funzionamento delle infrastrutture del sistema della posta elettronica e del suo regolare utilizzo, comprese le più essenziali garanzie di sicurezza del servizio (comma 2 dell'art. 4), configurandosi piuttosto, come un'attività funzionale alla tutela dell'integrità del patrimonio informativo e della sicurezza informatica, finalità riconducibile al comma 1 dell'art. 4 (cfr. accordi collettivi del XX e del XX4, ove si dà conto anche della finalità di "garantire la sicurezza degli strumenti assegnati al personale, e più in generale tutelare il patrimonio informativo dell'Ente").

In tale contesto, con riguardo al periodo anteriore alla sottoscrizione dei predetti accordi, non può essere ritenuta sufficiente per escludere la responsabilità della Regione la circostanza che la stessa conservasse i metadati relativi alle e-mail più risalenti di 7 giorni "attraverso un report in formato CSV" (v. nota del XX) e che dunque, in tal caso, "l'operatore non accede[sse] direttamente ai metadati ma d[ovesse] necessariamente scaricare un report csv dal quale andare a ricostruire le indicazioni utili per l'assistenza richiesta" (v. nota del XX). Ciò in quanto, come dichiarato dalla Regione, "gli elementi che differenziano i metadati conservati per l'intervallo più breve rispetto a quelli conservati per l'intervallo più lungo, riguardano esclusivamente la velocità/facilità con cui poter recuperare le informazioni necessarie alla risoluzione della problematica di assistenza" e che, quindi, decorsi i primi 7 giorni dalla raccolta dei metadati, per i successivi 83 giorni gli stessi possono essere comunque acceduti da ciascun operatore preposto al servizio di assistenza tecnica, previo download del predetto report (v. nota del XX). Tale misura, che pure risulta apprezzabile sotto il profilo della minimizzazione dei dati, non risulta, infatti, idonea a colmare, anteriormente alla stipula dei predetti accordi collettivi nel rispetto delle procedure di garanzia di cui all'art. 4, comma 1, della l. 20 maggio 1970, n. 300, il difetto di base giuridica, diversamente da quanto sostenuto dalla Regione nell'ambito dell'istruttoria e, da ultimo, con le proprie memorie difensive del XX.

Né può essere invocato, ai fini della liceità del complessivo trattamento, che l'individuazione, da parte della Regione, del termine di 90 giorni per la conservazione dei metadati di posta elettronica sia avvenuta prima della pubblicazione del Documento di indirizzo sui metadati sopra citato o che "solo dopo la consultazione pubblica, precisamente nel mese di XX l'Autorità Garante, […] ha rivisto il tempo di conservazione dei metadati della posta elettronica, passando da 7 a 21 giorni". Ciò in quanto, come affermato anche dalla stessa Regione, i chiarimenti forniti per il tramite del predetto Documento, anche all'esito della consultazione pubblica cui lo stesso è stato sottoposto, si pongono "in linea con la precedente interpretazione" sostenuta dall'Autorità, nel solco di un

consolidato orientamento, sin dal 2016 (cfr. provv. 13 luglio 2016, n. 303, doc. web n. 5408460, confermato dal Tribunale di Chieti con sent. n. 672 del 24 ottobre 2019; v. anche, successivamente, provv. 1° dicembre 2022, n. 409, doc. web n. 9833530). La stessa Regione, peraltro, nel periodo immediatamente successivo agli accertamenti ispettivi (XX) - e dunque ancor prima della pubblicazione delle indicazioni orientative contenute nella prima versione del Documento di indirizzo sui metadati, del dicembre 2023 - aveva già intrapreso al proprio interno le attività finalizzate a conformare i predetti trattamenti alla disciplina di protezione dei dati, anche avviando specifiche interlocuzioni con i tavoli sindacali in vista della sottoscrizione dei relativi accordi (cfr. nota del XX, "l'Amministrazione, considerato quanto emerso durante l'ispezione, sta valutando le modalità con cui affrontare la questione sui tavoli sindacali, rappresentando preliminarmente alle RSU gli aspetti vincolanti derivanti dalla licenza Microsoft"; v. anche nota del XX, "il tema dell'accordo collettivo sul corretto utilizzo degli strumenti infotelematici ed in modo particolare per quanto riguarda l'utilizzo della posta elettronica e dei possibili controlli a distanza dei lavoratori, sarà oggetto di discussione nei prossimi tavoli sindacali, d'intesa con il Responsabile della Protezione dei Dati").

Né, ancora, può assumere rilevanza, per i profili di protezione dei dati, la circostanza per cui, nel caso di specie, "i sindacati non hanno richiesto l'attivazione di tavoli di contrattazione" (v. verbale del XX), posto che, ai sensi della disciplina normativa in materia di controlli a distanza, l'obbligo di attivarsi per addivenire alla stipulazione dell'accordo collettivo spetta in ogni caso al datore di lavoro, in qualità di titolare del trattamento, non potendo l'inerzia delle rappresentanze sindacali al riguardo essere invocata per escludere la responsabilità che l'art. 4 della l. 20 maggio 1970, n. 300 pone in capo al datore di lavoro.

Deve quindi concludersi che il trattamento in questione è stato effettuato in assenza delle garanzie procedurali previste dall'art. 4, comma 1, della l. 20 maggio 1970, n. 300, in violazione degli artt. 5, par. 1, lett. a), 6 e 88, par. 1, del Regolamento, nonché 114 del Codice, sino al XX per quanto concerne il personale non dirigenziale e sino al XX per quanto invece riguarda il personale dirigenziale, essendo la Regione in tali date addivenuta alla stipula dei citati accordi collettivi con le competenti parti sindacali.

4.2. Il trattamento dei log di navigazione in Internet.

Dagli elementi acquisiti nell'ambito della complessa attività istruttoria risulta accertato, in particolare, che, in virtù dell'adozione del decreto n. XX del XX (recante "Regole per l'utilizzo degli strumenti infotelematici della giunta regionale"), i log di navigazione in Internet - consistenti in informazioni inerenti ai siti web visitati dai dipendenti, inclusi quelli relativi ai tentativi falliti di accesso ai siti già censiti all'interno di una apposita black list, cui è comunque inibito l'accesso dal sistema - venivano raccolti e conservati dalla Regione in assenza della previa stipulazione di un accordo collettivo con le rappresentanze sindacali (cfr. art. 4, comma 1, della l. 20 maggio 1970, n. 300).

Nel corso dell'istruttoria, la Regione, anche tenuto conto delle indicazioni del proprio Responsabile della protezione dei dati, ha dato atto di essere addivenuta alla stipula, in relazione ai trattamenti in questione, di un accordo collettivo con le competenti parti sindacali in data XX per quanto concerne il personale non dirigenziale e in data XX per quanto invece riguarda il personale dirigenziale.

Quanto ai profili di rilevanza ai fini della sopra richiamata normativa in materia di controllo a distanza dell'attività dei lavoratori, tanto la raccolta quanto la successiva conservazione dei log di navigazione in Internet richiedono il rispetto dell'art. 4, comma 1, della l. 20 maggio 1970, n. 300, posto che i sistemi che consentono la tracciatura degli accessi ad Internet non possono essere, in generale, ricompresi nell'ambito di applicabilità dell'art. 4, comma 2, diversamente dai sistemi di inibizione automatica di consultazione in rete (senza conservazione dei tentativi di accesso), da

parte dei dipendenti, di specifici contenuti vietati dall'organizzazione di appartenenza.

La raccolta e la conservazione sistematica di tutti i file di log generati dall'utilizzo della rete Internet nell'ambito del rapporto di lavoro - inclusi quelli relativi ai tentativi falliti di accesso ai siti già censiti all'interno di una apposita black list, cui è comunque inibito l'accesso dal sistema - dando luogo, infatti, a un trattamento generalizzato dei dati relativi all'attività e all'utilizzo dei servizi di rete da parte di dipendenti comunque identificabili, comportano, in presenza di un collegamento univoco con il dipendente e con la sua specifica postazione di lavoro, la possibilità di ricostruirne l'attività mediante l'impiego di sistemi tecnologici, con la conseguenza che, in tali casi, al datore di lavoro è richiesto di assicurare il rispetto delle garanzie procedurali previste dall'art. 4, comma 1, della l. 20 maggio 1970, n. 300, che costituisce, come sopra ricordato, condizione di liceità dello stesso trattamento dei dati in questione.

Tale principio è stato confermato, nel tempo, dal Garante, in molteplici casi (v., in ambito pubblico, provv. del 13 maggio 2021, n. 190, doc. web n. 9669974, e provv. del 13 luglio 2016, n. 303, doc. web n. 5408460; v. anche, con riguardo al contesto lavorativo privato, provv. del 12 dicembre 2024, n. 771, doc. web n. 10096474).

Preso atto, dunque, che la Regione, avendo adottato il decreto n. XX del XX, ha raccolto e trattato tutti i log di navigazione in Internet del personale dipendente in assenza della previa stipulazione di un accordo collettivo con le competenti parti sindacali, a cui la Regione stessa risulta essere addivenuta soltanto nei giorni XX e XX, deve ritenersi che il trattamento in questione è avvenuto, entro i limiti di tale arco temporale, 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. 20 maggio 1870, n. 300).

Tanto premesso, si osserva ulteriormente che, in via generale, il trattamento deve in ogni caso essere "necessario" rispetto alla lecita finalità perseguita (art. 6, par. 1 del Regolamento) e avere ad oggetto i soli dati "adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattati" (art. 5, par. 1, lett. c), del Regolamento).

Sotto altro ma connesso profilo, 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 quest'ottica, in considerazione del rischio che incombe sui diritti e sulle libertà degli interessati, il titolare del trattamento deve altresì adottare - "fin dalla progettazione" e "per impostazione predefinita" (art. 25 del Regolamento) - 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).

Si evidenzia, inoltre, che fin dal 1970 al datore di lavoro pubblico e privato è fatto divieto di raccogliere o comunque trattare "anche a mezzo di terzi" dati personali relativi alle "opinioni politiche, religiose o sindacali del lavoratore, nonché [… a] fatti non rilevanti ai fini della valutazione dell'attitudine professionale del lavoratore" (v. art. 8 della l. 20 maggio 1970, n. 300, e art. 10 del d.lgs. 10 settembre 2003, n. 276, richiamati espressamente dall'art. 113 del Codice).

Come messo in evidenza in numerose circostanze dal Garante e dalla giurisprudenza anche a livello sovranazionale, i log di navigazione in Internet, tanto più se tra essi sono ricompresi i file di log relativi ai tentativi falliti di accesso ai siti già censiti all'interno di una apposita black list, cui è comunque inibito l'accesso dal sistema, possono riguardare aspetti della sfera personale e della

vita privata dei dipendenti (artt. 8 della Convenzione europea dei diritti dell'uomo e 7 della Carta dei diritti fondamentali dell'Unione europea). Ciò considerato che la linea di confine tra l'ambito lavorativo e professionale e quello strettamente privato non può sempre essere tracciata in modo netto. Nei casi in cui il dipendente sia connesso ai servizi di rete messi a disposizione del datore di lavoro o utilizzi una risorsa aziendale anche attraverso dispositivi personali e, in special modo, allorquando operi in modalità agile, sussiste per lo stesso una legittima aspettativa di riservatezza (v., al riguardo, le sentenze della Corte Europea dei Diritti dell'Uomo 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 [GC], 5.9.2017, ric. n. 61496/08, spec. parr. 70-73 e 80; Antovi and Mirkovi v. Montenegro, 28.11. 2017, ric. n. 70838/13, spec. par. 41-42; v. inoltre, per quanto attiene alla casistica esplorata dal Garante negli anni, in particolare provv. del 13 maggio 2021, n. 190, doc. web n. 9669974, e provv. del 13 luglio 2016, n. 303, doc. web n. 5408460).

Il trattamento di tali dati, effettuato mediante tecnologie informatiche nell'ambito del rapporto di lavoro, deve pertanto conformarsi al rispetto dei diritti e delle libertà fondamentali nonché della dignità dell'interessato, a tutela di lavoratori e di terzi (v. Raccomandazione CM/Rec(2015)5 del Comitato dei Ministri agli Stati Membri sul trattamento di dati personali nel contesto occupazionale, spec. punto 3; Gruppo "Articolo 29", Parere n. 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, par. 5).

In tale quadro, l'esigenza di ridurre il rischio di usi impropri della navigazione in Internet, da parte dei dipendenti, consistenti in attività non correlate alla prestazione lavorativa (ad esempio, la visione di siti web non pertinenti, l'upload o il download di file, l'uso di servizi di rete con finalità ludiche o estranee all'attività lavorativa) non può, infatti, giustificare ogni forma di interferenza nella vita privata, ma, come tradizionalmente affermato dal Garante, può essere in generale soddisfatta mediante la predisposizione di misure tecniche e organizzative idonee a prevenire in radice che le eventuali informazioni relative alla sfera extralavorativa vengano raccolte, dando luogo a trattamenti di informazioni personali "non pertinenti" che ricadono nell'ambito di applicazione dell'art. 113 del Codice (v., al riguardo, "Linee guida su posta elettronica e Internet", provv. 1° marzo 2007, n. 13, doc. web n. 1387522 in particolare, punto 5.2., lett. a), i cui principi possono ritenersi tuttora validi; cfr., inoltre, provv. del 13 maggio 2021, n. 190, doc. web n. 9669974, provv. del 13 luglio 2016, n. 303, doc. web n. 5408460, e provv. del 21 luglio 2011, n. 308, doc. web n. 1829641, confermato da Corte di Cassazione, sent. n. 18302 del 19 settembre 2016).

Quanto al caso di specie, il sistema adottato dalla Regione per finalità di sicurezza della rete, nella sua configurazione attuale, consente operazioni di tracciatura delle connessioni e dei collegamenti ai siti Internet visitati dai dipendenti, compresi i tentativi falliti di accesso ai siti web indicati nell'apposita black list, la memorizzazione di tali dati e la loro conservazione per 365 giorni, e comporta il trattamento di informazioni anche estranee all'attività professionale.

In particolare, quanto alla profondità temporale della conservazione dei predetti dati, la Regione, nella prospettiva del principio di "responsabilizzazione" (art. 5, par. 2, del Regolamento), ha determinato il termine di 365 giorni anche tenendo conto delle indicazioni fornite da altre autorità per i profili di relativa competenza nonché, più in generale, alla luce di studi e osservazioni sistematiche delle dinamiche proprie degli incidenti di sicurezza che possono essere occasionati dalla navigazione sul web, in special modo negli scenari che più di recente tendono a concretizzarsi nel contesto attuale.

Alla luce di una valutazione globale delle caratteristiche del sistema e delle conseguenti operazioni di trattamento consentite (raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti, memorizzazione per un prolungato periodo temporale e possibilità di risalire alla navigazione dei singoli dipendenti), deve ritenersi che, pur in presenza di alcune misure sul piano tecnico ed organizzativo, il trattamento in questione non

possa ancora ritenersi complessivamente proporzionato rispetto alla finalità perseguita dalla Regione, ossia quella di sicurezza della rete.

Al riguardo, si prende tuttavia favorevolmente atto delle procedure interne alla Regione, per cui i log di navigazione in Internet possono essere acceduti al ricorrere di due specifici ordini di casistiche, ossia in caso di richiesta dell'autorità giudiziaria ovvero in caso di rilevazione di particolari, motivate e predeterminate anomalie di traffico, oggetto di puntuale ricognizione e catalogazione da parte della Regione.

Analogamente, si prende atto anche della circostanza per cui la Regione, non disponendo di sufficienti informazioni per risalire, autonomamente, all'identità del dipendente che ha effettuato la navigazione in Internet, può identificare gli interessati mettendo in relazione le informazioni separatamente conservate dai tre fornitori di cui si avvale in tale ambito, disponendo l'uno del solo indirizzo IP della macchina utilizzata dai dipendenti, l'altro della sola informazione relativa all'associazione tra l'IP della macchina e il rispettivo MAC address e l'altro ancora del dato concernente la mera associazione tra il MAC address della macchina e il nome del dipendente che ne è assegnatario. Detta misura organizzativa, dando luogo ad una forma di separazione dei dati in questione, non preclude infatti al titolare del trattamento, datore di lavoro, la possibilità di risalire all'identità del dipendente che ha effettuato la navigazione in Internet, con la cooperazione dei tre fornitori e mettendo in relazione le informazioni che ciascuno di essi conserva, per conto e nell'interesse della Regione, in qualità di responsabile del trattamento.

Per tali ragioni, al fine di assicurare la piena conformità alla normativa in materia di protezione dei dati e nella prospettiva di prevenire possibili effetti pregiudizievoli per gli interessati nel delicato contesto lavorativo e professionale, la natura delle operazioni di trattamento in essere e, in generale, la delicatezza dei dati raccolti e conservati per un ampio arco temporale, come sopra descritto, richiedono, nel contesto di riferimento, la necessaria adozione delle specifiche misure supplementari indicate al par. 6 del presente provvedimento. La metodologia individuata dalla Regione e, in generale, le misure tecniche ed organizzative messe in atto, anche sul piano della minimizzazione, non possono, infatti, ritenersi ancora sufficienti, allo stato attuale, a superare del tutto le criticità sopra evidenziate e a rendere proporzionato il complessivo trattamento, non assicurando l'efficace attuazione dei principi di protezione dei dati e l'integrazione di tutte le necessarie garanzie al fine di tutelare i diritti e le libertà degli interessati.

Alla luce delle considerazioni che precedono, deve concludersi che, in base a una complessiva valutazione degli elementi emersi nel corso dell'istruttoria, il sistema attualmente impiegato dalla Regione, che consente di registrare dati di dettaglio in ordine alla risorsa Internet visitata dal personale dipendente, dia luogo, allo stato degli atti, ad una raccolta sistematica di numerosi dati personali, anche non attinenti allo svolgimento della prestazione lavorativa, e a una conservazione prolungata degli stessi, non risultando conforme alla disciplina di protezione dei dati e ponendosi in violazione degli artt. 5, par. 1, lett. a), c) ed e), e 25 del Regolamento, e 113 del Codice, in riferimento all'art. 8 della l. 20 maggio 1970, n. 300 e all'art. 10 del d.lgs. 10 settembre 2003, n. 276.

4.3. Il mancato svolgimento di una valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento.

Nel caso di specie, il trattamento dei metadati di posta elettronica e di navigazione in Internet è stato altresì effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento.

In attuazione del principio di responsabilizzazione (cfr. art. 5, par. 2, 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).

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si rileva, invece, che sia il trattamento dei metadati relativi all'utilizzo del servizio di posta elettronica - consistente nella sistematica raccolta dei dati esteriori afferenti alla corrispondenza e-mail (incluse le informazioni relative al mittente/destinatario e all'oggetto di ciascuna e-mail) e nella relativa memorizzazione per 90 giorni – sia il trattamento dei log relativi alla navigazione in Internet - consistente nella raccolta preventiva e generalizzata dei dati concernenti le connessioni ai siti web dei singoli dipendenti e nella relativa memorizzazione per 365 giorni - comportano rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo (art. 35 del Regolamento).

Tanto in considerazione sia della particolare "vulnerabilità" degli interessati nel contesto lavorativo (cfr. cons. 75 e art. 88 del Regolamento e criterio n. 3 indicato nelle "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menzionano espressamente "i dipendenti") sia del fatto che in tale ambito, diversamente da quanto sostenuto dalla Regione, 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) può presentare rischi - come nel caso di specie - in termini di possibile monitoraggio dell'attività dei dipendenti (cfr. artt. 35 e 88, par. 2, del Regolamento). Come sopra già rilevato, infatti, in presenza di talune specifiche caratteristiche o funzionalità, tali strumenti possono comportare un controllo preterintenzionale dell'attività del dipendente.

Tali principi sono stati ribaditi dal Garante, oltre che, da ultimo, nel predetto Documento di indirizzo (v. punto 2), anche nel 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", nonché in diverse decisioni su singoli casi concreti (v., tra gli altri, anche provv. 13 maggio 2021, n. 190, doc. web n. 9669974, par. 3.5).

Per tali ragioni, nel prendere atto che, seppur tardivamente e nel corso dell'istruttoria, la Regione ha da ultimo fornito evidenza dello svolgimento delle valutazioni d'impatto dei trattamenti suindicati (v. nota del XX), si rileva che, anteriormente a tale adempimento, gli stessi sono stati effettuati in assenza di una valutazione di impatto e quindi in violazione dell'art. 35 del Regolamento.

4.4. Ulteriori considerazioni sui trattamenti dei metadati di posta elettronica e dei log di navigazione in Internet.

Quanto alla contestazione relativa all'utilizzo a fini disciplinari, in due specifici casi, dei log relativi alla navigazione in Internet e all'utilizzo del servizio di posta elettronica da parte dei dipendenti, raccolti e trattati in assenza dei presupposti di cui all'art. 4, comma 1, della l. 20 maggio 1970, n. 300, si prende atto delle precisazioni rese con nota del XX. In particolare, con tale nota, la Regione, nel far pervenire nuovi e più specifici elementi, ha chiarito che "nessuno dei due procedimenti disciplinari è stato avviato per il tramite dell'utilizzo dei log della posta elettronica o della navigazione in Internet", dovendosi per l'effetto concludere che, per i profili di competenza dell'Autorità, non ricorrono nel caso di specie i presupposti per far valere responsabilità della Regione in ordine all'utilizzo ai fini connessi al rapporto di lavoro di dati raccolti e trattati in violazione della disciplina di cui all'art. 4, comma 1, della l. 20 maggio 1970, n. 300 (cfr. artt. 5, par. 1, lett. a), 6 e 88 del Regolamento e 114 del Codice, in relazione all'art. 4, comma 3, della l. 20 maggio 1970, n. 300).

4.5. Il trattamento dei dati relativi alle richieste di assistenza tecnica.

Dall'attività istruttoria è emerso che i dati relativi alle richieste di assistenza tecnica presenti nel sistema di ticketing "OTRS", successivamente dismesso, sono stati conservati dalla Regione per tutta la durata del rapporto contrattuale intercorso con il fornitore del servizio, in ragione di esigenze connesse alla gestione amministrativa del servizio stesso. Al riguardo, la Regione, nel rilevare che "la fattibilità di interventi tecnici volti a minimizzare la visibilità dei ticket non più aperti prevedeva tempi di realizzazione superiori al momento programmato per la dismissione", si è determinata nel senso "di intervenire organizzativamente accelerando la dismissione del [sistema di ticketing "OTRS"]" (v. nota del XX) e ha evidenziato che in data XX "il fornitore ha comunicato via PEC di aver proceduto alla cancellazione in modalità irreversibile della base dati dello strumento ITSM OTRS […]" (v. nota del XX).

Alla luce dell'attività istruttoria, risulta altresì che, inizialmente, la Regione intendeva conservare i dati relativi alle richieste di assistenza tecnica per il tramite del nuovo sistema di ticketing "SDAS" per un periodo massimo complessivo di 78 mesi (72 mesi in ragione di esigenze connesse alla gestione del servizio e ulteriori 6 mesi al fine di "espletare le attività contrattuali residuali quali contabilità, pagamenti, verifica della regolare esecuzione del contratto"; v. verbale del XX).

Anche tenuto conto che la Regione aveva dichiarato di tenere con cadenza mensile una riunione tra i fornitori del servizio di assistenza tecnica e la "struttura dei sistemi informativi (SAL) per verificare l'avanzamento dei lavori e fare il punto della situazione, monitorare gli SLA, individuare eventuali criticità quali numero eccessivo di ticket, particolari e ripetute problematiche" (v. verbale del XX) e che la regolare programmazione di tali incontri non consentiva di giustificare una tanto prolungata conservazione dei dati in questione, la Regione, nel quadro delle iniziative progressivamente intraprese nel corso dell'istruttoria per assicurare la conformità di tale trattamento alla disciplina di protezione dei dati, ha stabilito, anche a fronte di specifiche interlocuzioni con il fornitore del servizio, di ridurre il predetto periodo a 12 mesi.

Benché, in generale, le esigenze di consuntivazione, contabilizzazione, fatturazione e remunerazione dei servizi possano essere soddisfatte, normalmente, anche senza fare ricorso al trattamento di dati personali ovvero, se del caso, anonimizzando quelli presenti e dunque conservando le sole informazioni strettamente necessarie a consentire il raffronto tra il servizio effettivamente reso e quello previsto contrattualmente (cfr., al riguardo, ancorché in riferimento ad altra tipologia di servizio, provv. del 24 maggio 2017, n. 247, doc. web n. 6495708; v. anche provv. 2 ottobre 2014, doc. web n. 3534543, e provv. n. 427 del 19 luglio 2018), si osserva quanto segue.

Preso atto delle valutazioni svolte dalla Regione, nella prospettiva del principio di responsabilizzazione (cfr. art. 5, par. 2, del Regolamento), con riferimento al nuovo sistema di ticketing "SDAS" nonché, in particolare, delle dichiarate esigenze di conservazione dei predetti dati in chiaro per un arco temporale pari ad un anno alla luce delle specificità proprie della complessa realtà organizzativa della Regione, occorre comunque rilevare che, invece, la conservazione dei dati relativi alle richieste di assistenza tecnica di cui al dismesso sistema "OTRS" risulta essersi protratta per un periodo temporale particolarmente esteso. In particolare, dalla documentazione acquisita in sede ispettiva è emerso che le richieste di assistenza tecnica del personale dipendente di cui la Regione conservava ancora traccia risalivano al 2016; tali informazioni sono state conservate fino al XX, data in cui il fornitore di tale servizio ha comunicato "di aver proceduto alla cancellazione in modalità irreversibile della base dati dello strumento ITSM OTRS" (cfr. nota del XX).

Non rinvenendosi adeguate ragioni che potessero giustificare una conservazione tanto prolungata dei dati in questione, deve pertanto concludersi che il trattamento dei dati relativi alle richieste di assistenza tecnica di cui al dismesso sistema "OTRS" è stato effettuato in contrasto con i principi di limitazione della conservazione e 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.

4.5.1. Il rapporto con i fornitori incaricati dell'erogazione del servizio di assistenza tecnica con riferimento al sistema "OTRS" in fase di dismissione.

Alla luce di quanto emerso dagli atti, risulta accertato altresì che l'accordo ai sensi dell'art. 28 del Regolamento stipulato con i tre fornitori, di cui la Regione attualmente si avvale ai fini dell'erogazione del servizio di assistenza tecnica, non riguardava - sino alla data della stipulazione dell'addendum contrattuale, intervenuta in corso di istruttoria - il trattamento dei dati personali contenuti nel sistema "OTRS" effettuato dai predetti fornitori nel corso della fase transitoria di dismissione del sistema in questione.

Al riguardo, si evidenzia che, nell'ambito della predisposizione delle misure tecniche e organizzative che soddisfino i requisiti stabiliti dal Regolamento, anche sotto il profilo della sicurezza (artt. 4, n. 7), 24 e 32 del Regolamento), il titolare del trattamento può avvalersi di un responsabile per lo svolgimento di alcune attività di trattamento, cui impartisce specifiche istruzioni (cfr. artt. 4, n. 8), 28 e considerando 81 del Regolamento).

In tale quadro, il rapporto tra titolare e responsabile deve essere regolamentato con un contratto o un altro atto giuridico, avente forma scritta, che, nel vincolare il responsabile al titolare, rechi, tra le altre cose, anche l'indicazione della "materia disciplinata" (ossia l'oggetto del trattamento, che "deve essere formulato con specifiche sufficienti affinché […] sia chiaro" - cfr. Comitato europeo per la protezione dei dati, "Linee guida 07/2020 sui concetti di titolare del trattamento e di responsabile del trattamento ai sensi del GDPR", v. 2.0, adottate il 7 luglio 2021), del "tipo di dati personali" e delle "categorie di interessati" nonché delle necessarie istruzioni documentate in merito al trattamento (art. 28, parr. 3 e 9, del Regolamento).

Posto che, nel caso in esame, l'efficacia dell'accordo ai sensi dell'art. 28 del Regolamento in essere tra la Regione e i nuovi fornitori del servizio non risultava essere stata estesa anche al trattamento dei dati contenuti nel sistema "OTRS", non può ritenersi che, limitatamente a tale specifico ambito oggettivo di trattamento, lo stesso soddisfi i requisiti analiticamente individuati dall'art. 28, par. 3, del Regolamento (cfr., in particolare, la materia disciplinata, la durata, la natura e la finalità di tale specifico trattamento, il tipo di dati personali e le categorie di interessati nonché le specifiche istruzioni documentate impartite dalla Regione al riguardo).

Per le ragioni che precedono, pur prendendosi atto dell'avvenuta sottoscrizione con i tre predetti fornitori dell'addendum contrattuale nel corso del XX, con il quale le parti hanno pattuito che le attività di trattamento previste dall'accordo ai sensi dell'art. 28 del Regolamento già stipulato "venivano effettuate anche attraverso il sistema di ticketing OTRS" (cfr. nota del XX), risulta che, anteriormente alla sottoscrizione del predetto addendum, il trattamento dei dati personali contenuti nel sistema "OTRS" è avvenuto in violazione dell'art. 28 del Regolamento.

5. 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 tutti 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 conferma l'illiceità del trattamento di dati personali effettuato dalla Regione Lombardia sul presupposto che, nei termini esplicitati in motivazione:

- il trattamento dei metadati di posta elettronica è stato effettuato in violazione degli artt. 5, par. 1, lett. a), 6, 35 e 88 del Regolamento, nonché 114 del Codice;

il trattamento dei log di navigazione in Internet è stato effettuato in violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 25, 35 e 88 del Regolamento, nonché 113 e 114 del Codice;

il trattamento dei dati personali contenuti nel sistema OTRS è stato effettuato in violazione degli artt. 5, par. 1, lett. e), 25 e 28 del Regolamento.

La violazione delle predette disposizioni comporta, ai sensi dell'art. 2-decies del Codice e "salvo quanto previsto dall'articolo 160-bis", l'inutilizzabilità dei dati personali trattati. La violazione delle predette disposizioni rende inoltre applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 2, del Codice.

6. Misure correttive (art. 58, par. 2, lett. d), del Regolamento).

Con riferimento ai profili di illiceità del trattamento dei log di navigazione web associati ai dipendenti, tuttora persistenti (v., in particolare, par. 4.2 del presente provvedimento), ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, si ritiene necessario ingiungere alla Regione Lombardia l'adozione - entro novanta giorni dalla notifica del presente provvedimento - di ulteriori misure tecniche e organizzative idonee ad assicurare che l'effettiva possibilità di risalire all'identità del singolo dipendente che ha effettuato la navigazione web risulti in concreto estremamente improbabile.

In particolare, in aggiunta alle misure già adottate dalla Regione e consistenti, nel dettaglio:

- nella separazione dei dati in questione, posto che, dei tre fornitori – responsabili del trattamento - di cui la Regione si avvale in tale ambito, l'uno dispone del solo indirizzo IP della macchina utilizzata dai dipendenti, l'altro della sola informazione relativa all'associazione tra l'IP della macchina e il rispettivo MAC address e l'altro ancora del dato concernente la mera associazione tra il MAC address della macchina e il nome del dipendente che ne è assegnatario;

- nella puntuale individuazione dei presupposti al ricorrere dei quali la Regione procede all'elaborazione che le permette di risalire all'identità dei singoli dipendenti che hanno effettuato la navigazione web (particolari, motivate e predeterminate anomalie di sicurezza e specifiche richieste da parte dell'autorità giudiziaria);

si ritiene necessario che - anche tenuto conto dell'esperienza applicativa riscontrata dal Garante in diverse istruttorie che hanno coinvolto altre pubbliche amministrazioni aventi caratteristiche analoghe a quelle della Regione in termini di estensione territoriale, ambiti di competenza e numerosità del personale dipendente impiegato - la Regione assicuri l'adozione, nello specifico contesto di riferimento, delle seguenti misure supplementari:

- l'anonimizzazione dei log relativi ai tentativi di accesso falliti ai siti web censiti nella apposita black list, ivi compresi quelli allo stato presenti nei sistemi;

- la riduzione a 90 giorni del termine di conservazione dei log di navigazione in Internet, con possibilità di conservazione per un periodo ulteriore previa anonimizzazione degli stessi, in modo da non consentire l'identificabilità del dipendente (cfr. art. 5, par. 1, lett. e), del Regolamento), e ferma restando la cancellazione dei dati personali presenti nei log di navigazione web registrati nei sistemi da oltre 90 giorni;

- che, in presenza di una delle predette anomalie di sicurezza, le attività di verifica vengano di regola svolte dalla Regione, in un'ottica di gradualità e progressività, a livello di singole strutture organizzative e non invece a livello individuale, limitando la possibilità di interventi granulari e puntuali sulla singola postazione di lavoro ai soli casi di previo e infruttuoso

esperimento di verifiche a livello aggregato (cfr. artt. 5, par. 1, lett. c), e 25 del Regolamento);

- la cifratura del dato concernente i nomi dei dipendenti assegnatari della macchina (cfr. art. 32, par. 1, lett. a), del Regolamento), fornendo a tal riguardo specifiche istruzioni documentate al fornitore che, in qualità di responsabile del trattamento, tratta tali dati per conto e nell'interesse della Regione medesima (art. 28 del Regolamento);

- che il trattamento dei dati in questione venga in ogni caso effettuato da un numero strettamente limitato di persone fisiche autorizzate e a tal fine appositamente selezionate, che dovranno essere destinatarie di designazione espressa e istruzioni specifiche in relazione ai rischi connessi al trattamento in questione (cfr. artt. 2-quaterdecies del Codice e 28, 29 e 32, par. 4, del Regolamento), secondo quanto potrà essere previsto dalle procedure interne della Regione e dalle istruzioni documentate che la stessa Regione deve impartire ai fornitori ai sensi dell'art. 28 del Regolamento, che a tal fine dovranno quindi essere opportunamente aggiornate nonché periodicamente rivalutate al fine di verificarne l'adeguatezza e l'efficacia (artt. 5, par. 2, 24 e 32 del Regolamento);

- l'aggiornamento degli accordi già stipulati ai sensi dell'art. 4 della l. 20 maggio 1970, n. 300, con le rappresentanze sindacali alla luce delle misure sopra indicate.

Ai sensi dell'art. 157 del Codice, la Regione dovrà, inoltre, provvedere a comunicare a questa Autorità le iniziative che intende intraprendere per assicurare che i trattamenti siano conformi alla disciplina di protezione dei dati, entro trenta giorni dalla notifica del presente provvedimento.

7. 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).

Nel caso di specie, si ravvisano tre condotte distinte imputabili alla Regione Lombardia (la prima in relazione al trattamento dei metadati di posta elettronica; la seconda relativa al trattamento dei log di navigazione in Internet; infine, la terza inerente al trattamento dei dati personali relativi alle richieste di assistenza tecnica del personale dipendente di cui al dismesso sistema "OTRS"), le quali devono, pertanto, essere considerate separatamente ai fini della quantificazione delle sanzioni amministrative da applicarsi.

7.1. Il trattamento dei metadati di posta elettronica (parr. 4.1 e 4.3 del presente provvedimento).

Tenuto conto che la violazione delle disposizioni citate nei precedenti paragrafi 4.1 e 4.3 del presente provvedimento ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, la violazione più grave riguarda gli artt. 5, 6 e 88 del Regolamento e 114 del Codice, soggetta alla sanzione amministrativa prevista

dall'83, par. 5, del Regolamento, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

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.

Tenuto conto che:

- il trattamento dei metadati di posta elettronica riguarda forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente (artt. 2 e 15 Cost.) (art. 83, par. 2, lett. a) e g), del Regolamento);

- malgrado, anche su indicazione del responsabile della protezione dei dati, la Regione, a seguito della pubblicazione del provv. 1° dicembre 2022, n. 409, doc. web n. 9833530, avesse già avviato una riflessione interna in merito alla necessità di addivenire alla stipulazione di un accordo collettivo con le rappresentanze sindacali in merito a tale trattamento, e nonostante la stessa abbia infine sottoscritto il predetto accordo in conformità a quanto previsto dall'art. 4 della l. 20 maggio 1970, n. 300 e ancor prima della pubblicazione della versione aggiornata del Documenti di indirizzo in materia, il trattamento è stato in precedenza avviato ed effettuato per lungo tempo 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 (art. 83, par. 2, lett. a) e b), del Regolamento).

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze attenuanti:

- la Regione ha offerto una piena cooperazione con l'Autorità nel corso dell'istruttoria, attivandosi prontamente - già a seguito dello svolgimento, da parte dell'Autorità stessa, delle attività ispettive - per assicurare la conformità delle proprie politiche di trattamento dei dati personali alla normativa in materia di protezione dei dati personali, nonché avendo cura di comprovare nel tempo le misure progressivamente adottate in tale quadro; in particolare, la Regione ha documentato di essere addivenuta alla stipula di un accordo collettivo con le competenti parti sindacali per quanto concerne il personale non dirigenziale già in data XX e, dunque, prima ancora e indipendentemente dall'esito della consultazione pubblica cui il Documento di indirizzo sui metadati è stato sottoposto nel mese di XX, con ciò testimoniando, anche grazie al virtuoso contributo del proprio Responsabile della protezione dei dati, un'apprezzabile attenzione per la disciplina per la protezione dei dati personali e per gli orientamenti dell'Autorità, espressi in maniera costante sin dalla pubblicazione, nel 2007, delle "Linee guida su posta elettronica e Internet"; la Regione ha, inoltre, documentato di aver stipulato un ulteriore accordo collettivo in data XX per quanto invece attiene al personale dirigenziale nonché di aver svolto, al riguardo, valutazioni d'impatto sulla protezione dei dati ai sensi dell'art. 35 del Regolamento (art. 83, par. 2, lett. c) e f), del Regolamento);

- non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento, aventi la medesima natura di quelle accertate in relazione alla condotta in esame, o precedenti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 20.000 (ventimila/00) per la violazione degli artt. 5, par. 1, lett. a), 6, 35 e 88 del Regolamento, nonché 114 del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che i metadati di posta elettronica, i quali sono stati trattati per lungo tempo in assenza delle garanzie procedurali previste dalla disciplina di settore in materia di controlli a distanza, riguardano forme di corrispondenza assistite da garanzie di segretezza tutelate anche costituzionalmente.

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

7.2. Il trattamento dei log di navigazione in Internet (parr. 4.2 e 4.3 del presente provvedimento).

Tenuto conto che la violazione delle disposizioni citate nei precedenti paragrafi 4.2 e 4.3 del presente provvedimento ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, la violazione più grave riguarda gli artt. 5, 6 e 88 del Regolamento e 113 e 114 del Codice, soggetta alla sanzione amministrativa prevista dall'83, par. 5, del Regolamento, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

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.

Tenuto conto che:

- il trattamento dei log relativi alla navigazione in Internet del personale dipendente della Regione riguarda anche aspetti della sfera personale e della vita privata dei dipendenti, quali beni giuridici tutelati altresì dalla cornice normativa sovranazionale (artt. 8 della Convenzione europea dei diritti dell'uomo e 7 della Carta dei diritti fondamentali dell'Unione europea; art. 83, par. 2, lett. a) e g), del Regolamento);

- la Regione ha comunque dato atto di aver adottato, nel caso di specie, specifiche misure tecniche ed organizzative per limitare il rischio per i diritti e le libertà degli interessati, ancorché le stesse non risultino ancora del tutto sufficienti ad assicurare una piena conformità alla normativa in materia di protezione dei dati personali (art. 83, par. 2, lett. a) e b), del Regolamento);

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, "Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR" del 24 maggio 2023, punto 60).

Ciò premesso, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

- la Regione ha offerto una piena cooperazione con l'Autorità nel corso dell'istruttoria,

attivandosi prontamente - già a seguito dello svolgimento, da parte dell'Autorità stessa, delle attività ispettive - per assicurare la conformità delle proprie politiche di trattamento dei dati personali alla normativa in materia di protezione dei dati personali, nonché avendo cura di comprovare nel tempo le misure progressivamente adottate in tale quadro (art. 83, par. 2, lett. c) e f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento, aventi la medesima natura di quelle accertate in relazione alla condotta in esame, o precedenti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 25.000 (venticinquemila/00) per la violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 25, 35 e 88 del Regolamento, nonché 113 e 114 del Codice, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che i log di navigazione in Internet, i quali sono stati trattati per lungo tempo in assenza delle garanzie procedurali previste dalla disciplina di settore in materia di controlli a distanza, riguardano anche aspetti della sfera personale e della vita privata dei dipendenti e vengono tuttora conservati dalla Regione per un periodo temporale comunque esteso in assenza di misure tecniche ed organizzative sufficienti ad assicurare la complessiva liceità del trattamento.

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

7.3. Il trattamento dei dati relativi alle richieste di assistenza tecnica del personale dipendente di cui al dismesso sistema "OTRS" (parr. 4.5 e 4.5.1).

Tenuto conto che la violazione delle disposizioni citate nei precedenti paragrafi 4.5 e 4.5.1 del presente provvedimento ha avuto luogo in conseguenza di un'unica condotta (stesso trattamento o trattamenti tra loro collegati), trova applicazione l'art. 83, par. 3, del Regolamento, ai sensi del quale l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave. Considerato che, nel caso di specie, la violazione più grave riguarda l'art. 5, par. 1, lett. e), del Regolamento, soggetta alla sanzione amministrativa prevista dall'83, par. 5, del Regolamento, l'importo totale della sanzione è da quantificarsi fino a euro 20.000.000.

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.

Tenuto conto che:

la Regione non ha comprovato idonee ragioni a supporto di una conservazione tanto prolungata dei dati contenuti nel sistema di ticketing "OTRS", i quali erano relativi a richieste di assistenza tecnica risalenti nel tempo; inoltre, la Regione aveva già stipulato un accordo ai sensi dell'art. 28 del Regolamento con i fornitori incaricati di erogare il servizio di assistenza tecnica, ancorché tale disciplina contrattuale, come sopra rilevato, non era stata espressamente estesa dalle parti anche al trattamento dei dati personali effettuato nell'ambito del sistema "OTRS", il quale peraltro risultava in fase di dismissione all'epoca dei fatti in questione (cfr. art. 83, par. 2, lett. a), del Regolamento);

la violazione non ha riguardato particolari categorie di dati (cfr. art. 83, par. 2, lett. g), del Regolamento);

si ritiene che, nel caso di specie, il livello di gravità della violazione commessa dal titolare del trattamento sia medio (cfr. Comitato europeo per la protezione dei dati, “Linee guida 4/2022 sul calcolo delle sanzioni amministrative pecuniarie ai sensi del GDPR” del 24 maggio 2023, punto 60).

Ciò premesso, si ritiene che, ai fini della quantificazione della sanzione, debbano essere prese in considerazione le seguenti circostanze:

la Regione ha offerto una piena cooperazione con l’Autorità nel corso dell’istruttoria, altresì dando atto di essere addivenuta, nel corso del XX, alla stipulazione di un addendum contrattuale con i tre predetti fornitori, con il quale le parti hanno regolato, sotto il profilo della protezione dei dati, il trattamento effettuato nell’ambito del sistema “OTRS” sino alla data della sua completa dismissione (art. 83, par. 2, lett. c) e f), del Regolamento);

non risultano precedenti violazioni pertinenti commesse dal titolare del trattamento, aventi la medesima natura di quelle accertate in relazione alla condotta in esame, o precedenti provvedimenti di cui all’art. 58 del Regolamento (art. 83, par. 2, lett. e), del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l’ammontare della sanzione pecuniaria nella misura di euro 5.000,00 (cinquemila/00) per la violazione degli artt. 5, par. 1, lett. e), 25 e 28 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell’art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che, ai sensi dell’art. 166, comma 7, del Codice e dell’art. 16, comma 1, del Regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente capo contenente l'ordinanza ingiunzione sul sito Internet del Garante. Ciò in considerazione del fatto che, in particolare, la Regione non ha comprovato idonee ragioni a supporto di una conservazione tanto prolungata dei dati contenuti nel sistema di ticketing “OTRS”, che concernevano, infatti, richieste di assistenza tecnica risalenti fino al 2016.

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

TUTTO CIÒ PREMESSO IL GARANTE

a) dichiara, ai sensi dell’art. 57, par. 1, lett. a) e h), del Regolamento, l’illiceità del trattamento effettuato dalla Regione Lombardia per violazione degli artt. 5, par. 1, lett. a), c) ed e), 6, 25, 28, 35 e 88 del Regolamento, nonché 113 e114 del Codice, nei termini di cui in motivazione;

b) prescrive alla predetta Regione, ai sensi dell’art. 58, par. 2, lett. d) del Regolamento, di conformarsi, entro 90 giorni dalla data della notifica del presente provvedimento, alle prescrizioni formulate al paragrafo 6 del presente provvedimento;

c) prescrive alla predetta Regione, ai sensi dell’art. 58, par. 1, lett. a), del Regolamento, e dell’art. 157 del Codice, di comunicare, fornendo un riscontro adeguatamente documentato, entro 30 giorni dalla notifica del presente provvedimento, le iniziative che intende intraprendere in relazione a quanto indicato alla precedente lettera b); il mancato riscontro a una richiesta formulata ai sensi dell’art. 157 del Codice è punito con la sanzione amministrativa, ai sensi del combinato disposto di cui agli artt. 83, par. 5, del Regolamento e 166 del Codice;

ORDINA

alla Regione Lombardia, in persona del legale rappresentante pro-tempore, con sede legale in Piazza Città Di Lombardia, 1 - 20124 Milano (MI), C.F. 80050050154, di pagare la somma di euro 50.000,00 (cinquantamila/00) 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, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 50.000,00 (cinquantamila/00) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

DISPONE

- ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione dell'ordinanza ingiunzione sul sito Internet del Garante;

- ai sensi dell'art. 154-bis, comma 3 del Codice e dell'art. 37 del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito Internet dell'Autorità;

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

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, 29 aprile 2025

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE REGGENTE
Filippi