Ordinanza ingiunzione nei confronti di Comune di Bolzano - 13 maggio 2021 [9669974]

VEDI ANCHE NEWSLETTER DEL 22 GIUGNO 2021

[doc. web n. 9669974]

Provvedimento del 13 maggio 2021

Registro dei provvedimenti
n. 190 del 13 maggio 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (di seguito, "Regolamento");

VISTO il d.lgs. 30 giugno 2003, n. 196 recante "Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la Direttiva 95/46/CE (di seguito "Codice");

VISTO il Regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione del n. 98 del 4/4/2019, pubblicato in G.U. n. 106 dell'8/5/2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

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

Relatore il prof. Pasquale Stanzione;

PREMESSO

1. Il reclamo.

Con reclamo del XX, una dipendente del Comune di Bolzano (di seguito "il reclamante") ha

lamentato presunte violazioni della disciplina di protezione di dati personali con riguardo al trattamento di dati posti in essere dall'Ente mediante il monitoraggio del traffico di rete e dei singoli accessi ad Internet effettuati dall'interessato e, in generale, dai dipendenti comunali.

In particolare, il reclamante ha lamentato che l'Ente avrebbe trattato dati personali relativi alla sua navigazione in Internet, durante l'orario di lavoro, e di aver ricevuto, in data XX, una comunicazione di avvio di procedimento disciplinare (cfr. nota del XX allegata al reclamo), nella quale gli veniva contestato che "nel periodo dal XX al XX, era […] collegat[o] con il computer del Comune, per oltre 40 minuti a facebook e per oltre 3 ore a youtube, per seguire attività non istituzionali e che […] aveva consultato pagine Internet non inerenti il suo lavoro" come risultanti dai tabulati del traffico dati del Comune di Bolzano (cfr. report allegati al reclamo). Tali dati sarebbero stati utilizzati per formulare i rilievi disciplinari, previa richiesta della Direttrice dell'Ufficio gestione del Territorio all'Ufficio servizi informatici dell'Ente (cfr. all.ti nn. 2 e 3 al reclamo). Successivamente il procedimento disciplinare sarebbe stato archiviato per ragioni inerenti all'inattendibilità dei dati raccolti (cfr. all. n. 8 al reclamo).

Con il reclamo è stata lamentata la violazione dei principi di liceità, correttezza e minimizzazione nel trattamento dei dati personali dei dipendenti del Comune, atteso che il sistema di registrazione degli accessi ad Internet impiegato dall'Ente consentirebbe di "controllare, tracciare, filtrare in maniera massiva, costante e indiscriminata […] la cronologia dei siti internet visitati e il tempo di navigazione di per ciascun sito" (cfr. reclamo, p. 6), nonché la memorizzazione e la conservazione di tali dati associati a ciascun dipendente per un lungo periodo di tempo. Ciò avrebbe, dunque, reso possibile, inoltrando specifica richiesta all'Ufficio servizi informatici dell'Ente, la verifica sui singoli siti visitati dall'interessato, mediante estrazione di reportistica (cfr. report relativi al reclamante all. n. 4 al reclamo), tradottasi in un "controllo a distanza ingiustamente lesivo della libertà e della dignità […] nonché vietato dall'art. 4 della l. 300 del 1970" (cfr. p. 7 reclamo).

Il trattamento sarebbe avvenuto in assenza di un'informativa ai dipendenti in merito ai possibili controlli sugli accessi ad Internet da parte del datore di lavoro, precisando che non può "a tal fine ritenersi esaustivo il contenuto dell'accordo sindacale del 25.10.2010 ove non è assolutamente indicato alcun limite con riferimento alla navigazione in internet né in che misura sia consentito utilizzare la rete per ragioni personali e in quali casi possa scattare controllo; non risulta poi alcuna informazione riguardo al trattamento dei dati acquisiti, al soggetto responsabile di siffatto trattamento e alla sua finalità" (cfr. p. 7 reclamo).

Con lo stesso reclamo l'interessato ha lamentato, altresì, la non conformità ai principi di protezione di dati personali della procedura interna per la fruizione del servizio di assistenza psicologica messo a disposizione dei dipendenti. Sotto tale profilo è stato rappresentato che la procedura prevede la compilazione del modello denominato "Richiesta di accertamento medico straordinario", da trasmettere alla società che svolge le funzioni di medico competente per conto dell'amministrazione e al "rispettivo Direttore di Ripartizione del dipendente" (cfr. p. 9 reclamo). Nel caso specifico, il dirigente del reclamante avrebbe sottoscritto "per presa visione" in data XX il modulo presentato dall'interessato al medico competente.

Il reclamante ha, quindi, chiesto al Garante di "verificare la liceità dei trattamenti" di dati posti in essere dal Comune, "di dichiarare illecito il trattamento che risulti violare la normativa e i principi in materia di protezione dei dati perianali, oltre che l'art., 4 l. 300/1970", "dichiarare l'inutilizzabilità delle informazioni reperite in violazione di legge e disporre il divieto dell'ulteriore trattamento e conservazione dei dati" e di "disporre la trasmissione degli atti all'autorità giudiziaria per le valutazioni di competenza in ordine agli illeciti penali che riterrà eventualmente configurabili" (cfr. p. 10 reclamo).

2. L'attività istruttoria.

In riscontro alle specifiche richieste dell'Ufficio in merito ai numerosi profili sollevati dal reclamo, il Comune ha trasmesso la nota del XX, con la quale è stato precisato quanto segue:

- l'"accordo sindacale decentrato per l'utilizzo di Internet/intranet e uso della posta elettronica" del XX prevede che "i dirigenti possono chiedere all'amministratore di rete controlli mirati degli accessi ad internet da parte di personale del rispettivo ufficio/ripartizione";

- di tale accordo, "pubblicato sulla pagina intranet della home page del Comune di Bolzano", il reclamante "era a perfetta conoscenza" (ciò sarebbe comprovato dalla documentazione relativa alla presa visione da parte dell'interessato in merito, cfr. all. 1B e 2C alla nota cit.);

- "l'art. 10 del Codice di comportamento dei dipendenti, pubblicato sulla pagina intranet della home page del Comune di Bolzano, […] prevede espressamente che […] l'uso di tutti gli strumenti IT, sia che si tratti di software o di hardware, messi a disposizione dall'Amministrazione è limitato alle necessità lavorative" e che "sulla pagina intranet dell'home page del Comune di Bolzano nella pagina che descrive le modalità di accesso Internet-Servizio di posta è evidenziato in rosso e in grassetto che "viene tenuto traccia dei siti visitati" (all. n. 4 nota cit.);

- "la raccolta dei log da parte del comune ha l'obiettivo primario di registrazione degli eventi degli utenti per le finalità definite dall'accordo sindacale e, in particolare, per generare evidenze per la sicurezza informatica della rete del Comune […] che rientra nell'art. 6, lett. e) del GDPR in quanto volta a preservare la rete comunale in esecuzione dei propri compiti di interesse pubblico […]"; peraltro "l'attività di raccolta di log e monitoraggio è fortemente consigliata per garantire la sicurezza informatica (per es. le ISO 27001 e 27002 e le misure Enisa del Manuale sulla sicurezza nel trattamento dei dati personali […]" (cfr. p. 6 nota cit.);

- con riguardo alle modalità del trattamento è stato dichiarato che "la traccia viene aggiornata giornalmente sovrascrivendo[la] al 30° giorno [...e] quindi viene cancellata. Sono pertanto conservate solo le tracce degli ultimi 30 giorni come previsto dall'accordo sindacale";

- inoltre, "il tracciamento dei dati, quale misura di sicurezza, permette allo stesso utente di vedere anomalie sui suoi accesi, con l'obbligo in tal caso di comunicarle immediatamente all'amministratore di rete"; "l'uso improprio degli accessi, segnalato da un responsabile di settore, comporta, se richiesto, la disabilitazione all'accesso e l'attivazione di eventuali procedimenti disciplinari nei confronti dell'inadempiente"; "i dirigenti, che hanno obbligo di controllo sui collaboratori […] possono chiedere all'amministratore di rete controlli mirati sul personale del rispettivo ufficio";

- il Comune ha ritenuto di aver assolto all'obbligo di informare i dipendenti mediante i seguenti documenti: l'informativa generale (resa anteriormente all'entrata in vigore del Regolamento e quella successiva, "pubblicata sul sito istituzionale"), l'accordo sindacale citato, il modulo che ogni dipendente deve firmare quando fa richiesta di accedere ad Internet (in base a due diversi livelli di accesso per l'uso di Internet da parte dei dipendenti stabiliti dall'amministrazione: quello c.d. "esteso" e quello c.d. "limitato"); il codice di comportamento e le circolari interne dell'Ufficio del personale (cfr. p. 7 nota cit.); a seguito della richiesta di informazioni, il Comune si è impegnato, per il futuro, a redigere un'unica "informativa dedicata ai trattamenti che per esigenze organizzative e/o misure di sicurezza informatica comportano il tracciamento delle attività dei dipendenti" e, in generale "unificare le informative che riguardano i dati personali dei dipendenti o collaboratori, informative oggi reperibili internet sotto le singole strutture organizzative sulla base delle specifiche competenze" (cfr. p. 11, nota cit.);

- il responsabile della protezione dei dati dell'Ente si è espresso "sull'analisi dei rischi effettuata dai responsabili interni sui trattamenti censiti per competenza, validandoli o facendo osservazioni relative ad eventuali misure migliorative da adottare"; tale analisi "non ha fatto emergere alcun rischio elevato per i diritti e le libertà delle persone fisiche e pertanto ai sensi dell'art. 35 del GDPR non è stata necessaria alcuna valutazione d'impatto" (cfr. p. 10, nota cit.);

- i dati relativi alla navigazione a gli accessi di rete sarebbero stati trattati per "funzioni istituzionali" dalla Direttrice dell'Ufficio gestione del territorio, dall'amministratore di rete e dalla Direttrice dell'Ufficio personale e non sarebbero stati "né diffusi né comunicati a terzi non legittimati" (cfr. p. 3 nota cit.);

- i dati personali del reclamante, trattati in tale ambito, sono "giorno, ora, nome utente, pc utilizzato e sito consultato"; "la richiesta circa il controllo è stata fatta dalla dirigente" competente e "i dati sono stati estratti da persona nominata come amministratore di sistema";

- "i dati sono stati trattati dall'ufficio e organo competente in materia di procedimento disciplinare (capo II del contratto intercomparto; art. 21 D.p.Reg. 01.02.2005 n. 2/L e ss.mm. oggi art. 107 del "codice degli enti locali" di cui alla L. R. 03.05.2018, n. 2; Titolo IV del D.lgs. 30.03.2001, n. 165 e ss.mm.; art. 42-bis del regolamento organico e organizzazione del Comune di Bolzano)";

- "le informazioni relative all'avvio dei procedimenti disciplinari e loro esito a carico del [reclamante] sono stati forniti al legale della Direttrice dell'ufficio gestione del territorio con nota del XX", in riscontro a un'istanza di accesso agli atti ai sensi degli art. 22 e ss. della l. 241/1990. Non sarebbe comunque "mai stata data copia dei documenti inerenti ai suddetti procedimenti disciplinari ma solo le informazioni risultanti dalla nota del XX";

- "la presa visione da parte del direttore di Ripartizione della richiesta di visita straordinaria presso il medico competente è avvenuta per legge ai fini degli adempimenti di sorveglianza sanitaria in quanto nel Comune di Bolzano, il datore di lavoro è il Direttore di ripartizione - giuste delibere di Giunta comunale n. 85/12 e n. 532/13";

- "il modulo della richiesta di accertamento medico straordinario è peraltro liberamente compilato da chi fa domanda e non richiede indicazione della patologia sofferta"; […] "viene trasmesso direttamente da chi fa la richiesta alla segreteria del medico competente" e "all'esito della visita, il medico competente trasmette il certificato di idoneità alla mansione specifica […] all'ufficio del personale del comune che a sua volta lo trasmette per posta elettronica al datore di lavoro/Direttore di ripartizione, affinché vengano eseguite le eventuali prescrizioni"; "copia del predetto certificato è archiviato in autonomo fascicolo personale del dipendente, come previsto dalle misure organizzative adottate, per garantire la protezione ei dati particolari" (cfr. p. 4 nota cit.); per il futuro il Comune intende revisionare il modulo mediante "ulteriore minimizzazione dei dati ai sensi dell'art. 5 del GDPR"(cfr. p. 11, nota cit.).

Con nota del XX (prot. n. XX), l'Ufficio, sulla base degli elementi acquisiti, ha notificato al Comune, 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, invitando il predetto titolare 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, dalla legge n. 689 del 24/11/1981).

Con la nota sopra menzionata, l'Ufficio ha rilevato che il Comune ha posto in essere trattamenti di dati personali dei dipendenti relativi alla navigazione in internet, anche estranei all'attività lavorativa degli interessati, in assenza di un idoneo presupposto di liceità del trattamento, di

un'idonea informativa e di una valutazione d'impatto sulla protezione dei dati, in modo non conforme ai principi di liceità, correttezza e trasparenza e di minimizzazione, in violazione degli artt. 5, par. 1, lett. a) e c), nonché in violazione degli artt. 6, 9,13, 88 e 35 del Regolamento e degli artt. 113 e114 del Codice, anche in riferimento alle prescrizioni di cui all'allegato 1 del Provvedimento n. 146 del 5 giugno 2019, doc. web n. 9124510. Inoltre, con riguardo al trattamento dei dati personali dei dipendenti in occasione della richiesta di accertamento medico straordinario, l'Ufficio ha rilevato la violazione art. 5, par. 1, lett. a) nonché in violazione dell'art. 9, par.2, lett. b) del Regolamento.

Con nota del XX il Comune ha fatto pervenire le proprie memorie difensive, "manifestando la […] volontà di cooperare con codesta Autorità al fine di rimuovere i vizi contestati", allegando la documentazione necessaria a comprovare le misure a tal fine adottate con riguardo ai trattamenti in corso nei confronti della generalità dei dipendenti, e precisando, tra l'altro, che:

- "sin dal XX è stato dato ordine di sospendere il trattamento dei log di navigazione di cui all'accordo sindacale d.d. 25.10.2000 e ss.mm., da parte dei dirigenti" (cfr. all. n. 1);

- "è stata redatta la valutazione d'impatto sulla protezione dei dati personali in relazione al trattamento dei "log di navigazione" individuando, rispetto alla situazione attuale, una serie di misure tecniche ed organizzative migliorative";

- "all'interno dei file di log di navigazione lo userid, che riportava iniziale del nome e primi caratteri del cognome degli utenti, è stato sostituito dal XX da un numero. Tale misura si configura come pseudonimizzazione finalizzata alla minimizzazione dei dati trattati" (cfr. all. n. 2);

- "è stato stipulato un nuovo accordo decentrato con le organizzazioni sindacali, in relazione alla possibilità di utilizzo dei log di navigazione ai fini dei cosiddetti "controlli preterintenzionali" nell'osservanza delle linee guida di cui alla deliberazione 13 d.d. 01.03.2007 di codesta Autorità e delle prescrizioni emerse dai successivi Provvedimenti, tra cui il n. 303 d.d. 13.07.2016, come pure delle salvaguardie di cui alla raccomandazione CM/Rec(2015)5 del Comitato dei Ministri degli Stati membri sul trattamento di dati personali nel contesto occupazionale, e dei concetti emersi nel corso dell'audizione del presidente Antonello Soro sugli schemi di decreti legislativo attuativi del Jobs Act d.d. 9 e 14 luglio 2015";

- tale accordo, "limitando le ipotesi di attivazione della procedura di controllo ad anomalie in relazione ad incidenti informatici e graduando il monitoraggio, migliora notevolmente la tutela dei diritti e delle libertà dei lavoratori" (cfr. all. n. 3);

- "sono state redatte e pubblicate nel sito intranet comunale, previo avviso al singolo utente, le informazioni per gli utenti di internet" (cfr. all. nn. 4 e 5) e rese le informazioni ai sensi dell'art. 13 del Regolamento "per il dipendente e collaboratore comunale" (cfr. all. n. 44);

- "è stato immediatamente sostituito […]il modulo di richiesta [di visita straordinaria], con l'eliminazione del visto del dirigente "datore di lavoro" (cfr. all. n. 6);

- con riguardo allo specifico trattamento dei dati del reclamante, "gli episodi di cui al reclamo in riferimento ai log di navigazione riguardavano il controllo dei log di navigazione di un dipendente per un periodo di gg. 30, in presenza di gradualità nei controlli attraverso gli strumenti di lavoro non pienamente conforme alle prescrizioni di codesta Autorità. Infatti, il Comune ha posto in essere misure di prevenzione dei controlli (accessi internet differenziati, filtri e blacklist, e 2 circolari dirette a tutto il personale, rispettivamente d.d. 15/03/2017 e 12/05/2017 – allegati 7, 8, 9 -), che già si configuravano graduali; il controllo solo nella fase

finale, all'atto della richiesta da parte della dirigente di acquisire i report della navigazione in internet [dell'interessato], non ha soddisfatto la gradualità";

- "le informazioni sul trattamento erano contenute in diversi documenti, in parte disponibili nell'intranet comunale, in parte contenute nell'informativa generale per il personale, disponibile non nel sito internet comunale, bensì affisso dal 2004 all'interno di ciascun ufficio, in ottemperanza alla circolare d.d. 12.08.2004" (cfr. all. nn. 10, 11, 12, 13, 14 in atti);

- "sussisteva un accordo stipulato ai sensi dell'art. 4 della L. 20.05.1970, n. 300 e ss.mm., con le organizzazioni sindacali in data 25.10.2000, integrato con successivo accordo d.d. 25.03.2010 […che prevedeva] un sommario bilanciamento tra la necessità crescente di utilizzare internet, e gli svantaggi che potevano conseguirne […anche se] successivamente non risultarono perfettamente allineate alla deliberazione del Garante n. 13 d.d. 01.03.2007 "Linee guida per posta elettronica e internet", ed ai successivi provvedimenti" (cfr. all. n. 10);

- "la finalità del trattamento dei log di navigazione all'epoca dei fatti contestati, ai sensi dell'art. 22 del D.lgs. 30.06.2003, n. 196 era individuata nelle misure tecniche da impiegarsi a salvaguardia dei dati trattati, rispettivamente dagli artt. 14bis e 71 del CAD "Codice dell'Amministrazione digitale", approvato con D.lgs. 07.03.2005, n. 82 e ss.mm., e dalla Direttiva del Presidente del Consiglio dei ministri 01.08.2015 "Misure minime di sicurezza ICT per le pubbliche amministrazioni"; "la finalità ulteriore del trattamento di controllo del lavoratore da parte del dirigente trovava fondamento negli artt. 54 e 55 sexies, comma 3 e del D.lgs. 30.03.2001, n. 165 e ss.mm.";

- "dall'entrata in vigore del GDPR 2016/679 al 03.02.2020, la base giuridica del trattamento di controllo "preterintenzionale" era costituita, ai sensi dell'art. 9, paragrafo 2, lettera b), del GDPR, dall'accordo decentrato con le organizzazioni sindacali maggiormente rappresentative in seno al Comune di Bolzano d.d. 25.10.2000, come integrato dal successivo accordo d.d. 25.03.2010" (cfr. all. nn. 10 e 15);

- "il Codice di comportamento del Comune di Bolzano, approvato con deliberazione della Giunta comunale 608 d.d. 30.10.2015, che all'art. 10 tratta della sicurezza informatica, è richiamato quale strumento fondamentale della prevenzione della corruzione dal punto 8.3 del Piano triennale di prevenzione della corruzione e per la trasparenza 2020-2022 approvato con deliberazione della Giunta comunale 27.12.2019, n. 827" (cfr. all. nn. 16,17, 18);

- "dall'anno 2010 ad oggi sono state 15 le richieste di controllo evase, […] che hanno coinvolto 27 utenti degli strumenti informatici comunali, di cui una sfociata nell'irrogazione di una sanzione disciplinare, ed una nell'avvio di un procedimento disciplinare, tuttavia archiviato" (relativa al reclamante);

- "dal XX, invariato il resto, la base giuridica del trattamento di controllo "preterintenzionale" è costituita, ai sensi dell'art. 9, paragrafo 2, lettera b), del GDPR, dal nuovo accordo decentrato d.d. 04.02.2020, stipulato a seguito di confronto con le organizzazioni sindacali";

- "l'episodio di cui al reclamo ha comportato la presa di conoscenza della richiesta di essere sottopost[o] ad accertamento medico straordinario formulata dal dipendente da parte del suo dirigente, "datore di lavoro" in base all'organigramma comunale della sicurezza sul lavoro […] La procedura specifica di richiesta peraltro era stata progettata in relazione alle funzioni di sorveglianza sanitaria preventiva attribuite al dirigente […per] individuare, in via cautelare e di concerto con i dipendenti, laddove richiesta dagli interessati, migliore o diversa modalità lavorativa compatibile con i disagi in attesa delle eventuali prescrizioni del medico competente";

- “il datore di lavoro de[ve] in ogni caso essere messo a conoscenza di un accertamento medico sanitario, ancorché d’iniziativa del dipendente, in ragione delle regole di contabilità pubblica, laddove, nell’attività di liquidazione dei corrispettivi al medico competente, debba verificare la correttezza e la congruità degli importi fatturati al Comune”; “dal 2014 ad oggi le richieste inoltrate dai dipendenti comunali sono state n. 19” (cfr. all. n. 20).
In data XX si è, inoltre, svolta l’audizione richiesta dal Comune, ai sensi dell’art. 166, comma 6, del Codice, in occasione della quale, nel confermare quanto già dichiarato in sede di memorie difensive, è stato rappresentato, tra l’altro, che:

- “il Comune da lungo tempo ha prestato attenzione al rispetto della normativa in materia di protezione dei dati personali […], adottando specifiche misure organizzative e procedurali, anche per assicurare la tutela degli interessati, operando sempre in piena trasparenza nei confronti di questi ultimi”;

- “al momento in cui si sono verificati i fatti oggetto di reclamo il Comune si è trovato ad affrontare diversi cambiamenti normativi in vari ambiti […] contestualmente a problemi nell’organico dirigenziale” nonché “difficoltà interpretative del quadro normativo vigente in materia di protezione dei dati”;

- “ora il Comune ha raggiunto un migliore livello di conformità alla normativa in materia di protezione dei dati personali, anche per quanto riguarda il rispetto dei principi di protezione dei dati fin dalla progettazione e per impostazione predefinita e l’esecuzione di analisi di impatto del trattamento”

- “se c’è stata violazione, deve comunque ritenersi lieve. Il Comune aveva infatti raggiunto un accordo sindacale ai sensi dell’art. 4 dello Statuto dei Lavoratori, in cui era espressamente previsto il divieto per i lavoratori di utilizzare gli strumenti informatici per finalità personali. Ciò anche in considerazione della natura pubblica del datore di lavoro. […] Se l’uso personale era precluso, non c’era, dunque, a monte un problema di protezione dei dati personali, poiché non era prevista la presenza di dati estranei all’attività lavorativa. Inoltre, in termini di numero di log e di numero di lavoratori interessati, la violazione, se c’è stata, è di lieve entità anche in termini quantitativi”;

- “i log non hanno portato all’applicazione di sanzioni disciplinari, poiché non erano attendibili, riportando anche una serie di siti (es. collegati a banner) che non erano stati necessariamente visitati dal lavoratore, senza possibilità di distinzione tra il sito effettivamente visitato e quelli a navigazione indiretta/involontaria. Per lo stesso motivo, anche il tempo di navigazione su tali siti non era un’informazione attendibile ai fini disciplinari”;

- “il Comune ha fornito ulteriori informazioni e istruzioni ai lavoratori in merito alle modalità di utilizzo degli strumenti informatici, migliorando complessivamente il livello di conformità alla normativa vigente con riguardo alla raccolta dei file di log della navigazione. In particolare, i log, che precedentemente riportavano l’“user id” in maniera esplicita, ora non riportano più tale informazione ma solo un “id macchina”, che consente di risalire all’identità dell’utente solo con una successiva elaborazione, effettuando l’abbinamento tra “id macchina” e lavoratore a cui tale macchina è assegnata. In questo modo sono stati pseudonimizzati i dati personali raccolti. Peraltro, i log sono conservati per soli 30 giorni e sono trattati, abbinandoli all’identità dell’utente, solo qualora ci siano anomalie tali da far sospettare una minaccia alla sicurezza informatica (ad esempio, un eccessivo traffico superiore alla norma, che può far pensare a un attacco alla macchina; un ripetitivo accesso a un singolo sito, che può far ritenere che la macchina stia operando indipendentemente dalla volontà dell’utente). È dunque l’ufficio responsabile della sicurezza informatica che rileva le anomalie e richiede gli approfondimenti. […]. I log sono comunque inutili ai fini del controllo preterintenzionale,

perché considerano complessivamente i tempi di navigazione e non distinguono tra navigazione intenzionale e involontaria. Inoltre, si evidenza che tutte le attività propedeutiche ad evitare che i dipendenti potessero visitare siti non sicuri erano state già poste in essere";

- per quanto riguarda il profilo del reclamo attinente alla richiesta di visita medica per supporto psicologico "[…] era fondamentale che i dipendenti informassero i propri dirigenti di eventuali situazioni di disagio personale in relazione a salute o sicurezza, anche per prevenire eventuali infortuni e/o malattie nelle more dell'effettuazione della visita medica, modificando l'assegnazione dei compiti e delle attività assegnati al dipendente che effettua la richiesta di visita o le modalità di prestazione dell'attività lavorativa. La richiesta di visita, peraltro, non entra nel merito della specifica presunta patologia, perché essa non è motivata da parte del lavoratore, non essendoci, pertanto, un trattamento di dati personali relativi alla salute. In ogni caso, il Comune ha ora previsto nella nuova modulistica che il dirigente non debba più essere informato della richiesta di visita straordinaria";

- "quanto alla contestazione della mancata effettuazione della valutazione d'impatto del trattamento, si ritiene che essa non fosse obbligatoria, atteso che non sussistono almeno due dei criteri che ha indicato il Comitato europeo per la protezione dei dati per individuare i casi in cui essa è obbligatoria. Inoltre, quando il Garante ha indicato nel provvedimento del 2018 i casi in cui la valutazione è obbligatoria, esso, richiamando i criteri di cui ai punti 3,7 e 8 delle Linee guida del Comitato, ha implicitamente escluso dall'obbligo i casi di trattamento connessi all'uso degli strumenti di lavoro. La valutazione non può, pertanto, ritenersi obbligatoria in relazione ai trattamenti connessi all'uso di strumenti necessari per la prestazione lavorativa. Si rileva, peraltro, che il provvedimento del Garante è di difficile interpretazione e che la sua applicazione pratica risulta problematica nei diversi contesti, essendo, peraltro, stato emanato successivamente ai fatti oggetto di reclamo".

3. Esito dell'attività istruttoria.

La disciplina di protezione dei dati personali consente che il datore di lavoro tratti i dati personali, anche relativi a categorie particolari di dati (cfr. art. 9, par. 1, del Regolamento), dei lavoratori nel rispetto dei principi generali del trattamento (art. 5 del Regolamento) e se il trattamento è necessario per adempiere a specifici obblighi o compiti previsti dalla normativa nazionale o dell'Unione, in particolare per finalità di gestione del rapporto di lavoro (artt. 6, par. 1, lett. c), 9, parr. 2, lett. b), e 4, e 88 del Regolamento) oppure "per l'esecuzione di un compito di interesse pubblico o connesso all'esercizio di pubblici poteri di cui è investito il titolare del trattamento" (art. 6, par. 1, lett. c) ed e), del Regolamento e 2-ter del Codice).

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 […l'impiego di] 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"). In particolare, l'art. 114 del Codice prevede che "Resta fermo quanto disposto dall'articolo 4 della l. 20 maggio 1970, n. 300", analogamente all'art. 113 che rinvia all'art. 8 della l. 20 maggio 1970, n. 300, e all'art. 10 del d.lgs. 10 settembre 2003, n. 276.

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 dal Garante alla Commissione, ai sensi dell'art. 88, par. 3, del Regolamento - , la cui osservanza costituisce una condizione di liceità del trattamento e la cui violazione - analogamente alle specifiche situazioni di

trattamento del capo IX del Regolamento - determina anche l'applicazione di sanzioni amministrative pecuniarie ai sensi dell'art. 83, par. 5, lett. d), del Regolamento (cfr., con riguardo all'ambito lavorativo pubblico, provv. 11 marzo 2021, n. 90, in corso di pubblicazione; provv. 5 marzo 2020, n. 53, doc. web n. 9433080; ma v. anche provv. 19 settembre 2019, n. 167; cfr., anche la giurisprudenza della Corte europea dei diritti dell'uomo, nel caso Antovic e Mirkovic v. Montenegro (Application n. 70838/13 del 28.11.2017), che ha stabilito che il rispetto della "vita privata" deve essere esteso anche ai luoghi di lavoro pubblici, evidenziando che i controlli sul posto di lavoro possono essere effettuati solo nel rispetto delle garanzie previste dalla legge nazionale applicabile).

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 delle misure tecniche e organizzative adeguate a garantire e essere in grado di dimostrare che il trattamento è effettuato in conformità al Regolamento (artt. 5, par. 2, e 24 del Regolamento).

3.1. Il principio di liceità correttezza e trasparenza del trattamento dei dati relativi alla navigazione in Internet dei dipendenti: l'informativa agli interessati.

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

Alla luce degli elementi in atti, il Comune ha adottato, fin dal 2000 (cfr. accordo sindacale del 20.10.2000 per l'utilizzo dei servizi di rete, integrato il 25.3.2010, limitatamente ad alcuni aspetti), un sistema che consente il tracciamento generalizzato (ed ex ante) degli accessi ad Internet da parte dei dipendenti e la memorizzazione, per trenta giorni, di informazioni di natura personale ("giorno, ora, nome utente, PC utilizzato e sito consultato").

In origine, all'interno dei file di log di navigazione "lo userid […] riportava iniziale del nome e primi caratteri del cognome degli utenti" poi sostituito ("dal XX") "con un numero corrispondente all'id macchina" (cfr. nota XX e verbale audizione XX, cit.). Il sistema consentiva, quindi, attraverso la possibilità di ricondurre la navigazione a uno specifico nome utente ("id utente"), di effettuare un controllo individualizzato della navigazione in Internet dei singoli dipendenti, mediante estrazione di dati, ad opera dell'amministratore di rete, su richiesta dei dirigenti competenti. Tanto, al fine di "generare evidenze per la sicurezza informatica della rete del Comune", la cui integrità dovrebbe essere assicurata per consentire l'esecuzione dei compiti di interesse pubblico propri dell'Ente (art. 6, par. 1, lett. e), del Regolamento).

Nel corso dell'istruttoria il Comune ha dichiarato di aver fornito ai dipendenti, anteriormente all'entrata in vigore del Regolamento, l'informativa generale sul trattamento dei dati personali e di averne predisposta un'altra, aggiornata al nuovo quadro normativo, "pubblicata sul sito istituzionale". Tuttavia, nel corso delle verifiche è emerso che, sul sito web dell'Ente, non era presente alcuna specifica informativa relativa ai trattamenti dei dati personali dei dipendenti né, in quelle rese disponibili, vi era alcun riferimento al trattamento dei dati personali relativi alla navigazione in Internet da parte degli stessi.

Un riferimento alle operazioni di tracciamento delle connessioni ad Internet era invece presente in altri documenti messi a disposizione dei dipendenti, alcuni dei quali pubblicati nella intranet, quali, l'accordo sindacale, il codice di comportamento, alcune circolari interne dell'Ufficio del personale, nonché il modulo che ogni dipendente doveva firmare all'atto della richiesta per l'accesso ad Internet e agli altri servizi di rete. Tali atti, che non contenevano tuttavia tutti gli elementi informativi essenziali richiesti dall'art. 13 del Regolamento, essendo stati redatti per assolvere ad obblighi diversi rispetto a quelli derivanti dalla disciplina in materia di protezione dei dati, non possono

quindi sostituire l'informativa che il titolare deve rendere, prima di iniziare il trattamento, agli interessati in merito alle caratteristiche essenziali dello stesso; ciò allo scopo di consentire all'interessato di esser pienamente consapevole della tipologia di operazioni di trattamento che potranno essere svolte anche attingendo, in un quadro di liceità, ai dati raccolti nel corso dell'attività lavorativa (cfr., Sentenze della Corte Europea dei Diritti dell'Uomo del 5 settembre 2017 - Ricorso n. 61496/08 - Causa Barbulescu c. Romania, spec. par. n.133 e 140 e sentenza del 9 gennaio 2018- ricorso n. 1874/13 e 8567/13- Causa López Ribalda e altri v. Spagna, spec. par. n. 115). Sul punto si evidenzia, altresì, che l'adempimento degli obblighi informativi nei confronti del dipendente (consistenti nella "adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli") costituisce una specifica condizione per il lecito utilizzo di tutti i dati raccolti nel corso del rapporto di lavoro, attraverso strumenti tecnologici e/o strumenti di lavoro, per tutti i fini connessi al relativo rapporto, ivi compresi i rilievi disciplinari, unitamente al rispetto della disciplina in materia di protezione dei dati personali (v. art. 4, comma 3, l. 20 maggio 1970, n. 300).

Si dà tuttavia atto che, dopo l'avvio del procedimento, il Comune ha provveduto a redigere una specifica informativa dedicata ai trattamenti che, per esigenze organizzative e di sicurezza informatica, comportano il tracciamento delle attività dei dipendenti come documentato in occasione delle memorie difensive (cfr. all. n. 12 alla nota del XX).

Pertanto, fino all'adozione del nuovo documento informativo per i dipendenti (datato XX), il trattamento risulta essere stato effettuato in violazione dell'obbligo previsto dall'art. 13 del Regolamento, nonché - attesa la frammentarietà delle informazioni contenute in molteplici atti, diversi per natura e funzione, stratificatisi nel tempo dall'amministrazione - non in conformità al principio di correttezza e trasparenza e dunque in violazione degli artt. 5, par. 1, lett. a), e 13 del Regolamento.

3.2. Il principio di minimizzazione dei dati e la raccolta di dati non attinenti all'attività lavorativa.

In base al Regolamento, il trattamento deve 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).

Come emerge dagli atti, il sistema adottato dal Comune per finalità di sicurezza della rete, nella configurazione originaria, consentiva operazioni di filtraggio e tracciatura delle connessioni e dei collegamenti ai siti Internet esterni, la memorizzazione di tali dati e la loro conservazione, per trenta giorni, nonché l'estrazione di report, anche su base individuale. In base a una complessiva valutazione degli elementi emersi nel corso dell'istruttoria, risulta che il trattamento dei dati personali raccolti e trattati dal Comune tramite il personale autorizzato e gli amministratori di sistema ("giorno, ora, sito consultato"), in presenza di un collegamento diretto e univoco con il dipendente e con la sua specifica postazione di lavoro (in quanto tra i dati raccolti figuravano anche "nome utente e PC utilizzato"), abbia dato luogo a una raccolta sistematica di dati relativi all'attività e all'utilizzo dei servizi di rete da parte dipendenti direttamente identificabili.

In tale contesto, l'amministrazione ha stipulato un accordo con le organizzazioni sindacali - dapprima nel 2000, poi aggiornato nel 2010 e, da ultimo, in data XX 2020 (cfr. all. n. 11, alla nota del XX, in atti) - come prescritto dalla disciplina in materia di impiego di sistemi tecnologici sul posto di lavoro (art. 4 della legge n. 300 del 1970) che, anche a seguito delle modifiche disposte dal decreto legislativo 14 settembre 2015, n. 151, consente l'impiego di "impianti audiovisivi e [di] altri strumenti dai quali derivi anche la possibilità di controllo a distanza dell'attività dei lavoratori […] esclusivamente per esigenze organizzative e produttive, per la sicurezza del lavoro e per la tutela del patrimonio aziendale", nel rispetto di specifiche condizioni, quali il previo accordo con la rappresentanza sindacale unitaria o le rappresentanze sindacali aziendali, ovvero, in alternativa,

previa autorizzazione delle sedi territoriali dell'Ispettorato nazionale del lavoro (comma 1). Peraltro anche il Garante, dopo le modifiche apportate nel 2015 a tale quadro di settore, si è espresso, proprio in merito all'utilizzo di sistemi che comportano la tracciatura degli accessi a Internet (cfr., provvedimento del 13 luglio 2016, n. 303, doc. web n. 5408460, confermato dal Tribunale di Chieti con sentenza n. 672 del 24 ottobre 2019) precisando, tra l'altro, che tali sistemi richiedono le garanzie di cui all'art. 4, comma 1 della l. 300 del 1970, non potendo essere ricompresi nel novero degli "strumenti di lavoro", ai sensi dell'art. 4, comma 2, diversamente dai sistemi di inibizione automatica di consultazione di contenuti in rete

In ogni caso, il titolare del trattamento deve sempre rispettare i principi di protezione dei dati (art. 5 del Regolamento). Ciò comporta che l'ambito dei controlli (indiretti o preterintenzionali), entro i limiti stabiliti dalla disciplina di settore, e i trattamenti di dati personali che possono essere lecitamente effettuati dal datore di lavoro, debbano essere comunque non massivi, graduali e ammissibili solo previo esperimento di misure meno limitative dei diritti lavoratori (cfr. Audizione del Garante sul Jobs Act presso Commissione lavoro Camera deputati 9 luglio 2015, doc. web n. 4119045; nonché "Dichiarazione di Antonello Soro, Presidente del Garante per la privacy, su sentenza Corte di Strasburgo" - CEDU, sentenza 17 ottobre 2019, López Ribalda and others v. Spain-, doc. web n. 9164334, "il requisito essenziale perché i controlli sul lavoro, anche quelli difensivi, siano legittimi resta dunque, per la Corte, la loro rigorosa proporzionalità e non eccedenza: capisaldi della disciplina di protezione dati la cui "funzione sociale" si conferma, anche sotto questo profilo, sempre più centrale perché capace di coniugare dignità e iniziativa economica, libertà e tecnica, garanzie e doveri").

Considerato che la linea di confine tra ambito l'lavorativo e professionale e quello strettamente privato non può sempre essere tracciata in modo netto, non può essere prefigurato l'annullamento di ogni aspettativa di riservatezza dell'interessato sul luogo di lavoro, anche nei casi in cui il dipendente sia connesso ai servizi di rete messi a disposizione del datore di lavoro o utilizzi una risorsa aziendale anche attraverso dispositivi personali, ragione per la quale la Corte europea dei diritti dell'uomo, ha nel tempo confermato che la protezione della vita privata (art. 8 Convenzione europea dei diritti dell'Uomo) si estende anche all'ambito lavorativo, ove si esplicano la personalità e le relazioni della persona che lavora (v. 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). Pertanto il trattamento dei dati effettuato mediante tecnologie informatiche, nell'ambito del rapporto di lavoro, deve 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).

Con riguardo al caso di specie, secondo quanto emerge dagli atti e confermato dal titolare del trattamento, risulta invece che le caratteristiche originarie del sistema e le conseguenti operazioni di trattamento (raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti, memorizzazione per trenta giorni e possibilità di estrazione di reportistica relativa alla navigazione di singoli dipendenti) non fossero necessarie e proporzionate rispetto alla finalità di protezione e sicurezza della rete interna invocata dall'Ente (cfr. considerando 49 e art. 6, par.1, lett. e) del Regolamento), avendo riguardato peraltro dati non "adeguati, pertinenti e limitati" a quanto necessario a garantire la sicurezza della rete, in violazione dei principi di liceità e di minimizzazione di cui all'art. 5, par. 1, lett. a) e c), e dell'art. 6 del Regolamento (cfr. provv. 13 luglio 2016, n. 303, doc. web n. 5408460, par. 5, cit.; sul punto, cfr. anche Consiglio di Europa, Raccomandazione del 1° aprile 2015, CM/Rec(2015)5, spec. princ. 15; Gruppo "Articolo 29", Parere n. 2/2017 sul trattamento dei dati sul posto di lavoro, WP 249, par. 5).

Sotto tale profilo, peraltro, il sistema impiegato dall'Ente consentiva di registrare dati di dettaglio in

ordine alla risorsa internet visitata (URL), che proprio in ragione del collegamento univoco con il nominativo del dipendente dava luogo alla raccolta sistematica di numerosi dati personali, anche non attinenti allo svolgimento della prestazione lavorativa, e informazioni relative alla vita privata dell'interessato.

Il sistema utilizzato dal Comune effettuando una raccolta sistematica dei dati di navigazione dei dipendenti comportava inevitabilmente il trattamento di informazioni anche estranee all'attività professionale, desumibili dagli URL visitati , e risultava, pertanto, in contrasto con il divieto per il datore di lavoro di trattare dati "non attinenti alla valutazione dell'attitudine professionale del lavoratore" e dunque con l'art. 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 (cfr., sul punto Provv. del Garante n. 308 del 21 luglio 2011, doc. web n. 1829641, confermato da Corte di Cassazione, sent. n. 18302 del 19 settembre 2016, ove si legge che "l'acquisizione e conservazione dei dati relativi alla navigazione Internet dei dipendenti mediante […] registrazione dei file log importa la violazione anche del disposto di cui alla legge n. 300 del 1970, art. 8" e che "acquisire e conservare dati che contengono (o possono contenere) simili informazioni comporta già l'integrazione della condotta vietata […] anche se i dati non sono successivamente utilizzati. Non è necessario sottoporre i dati raccolti ad alcun particolare trattamento per incorrere nell'illecito, poiché la mera acquisizione e conservazione della disponibilità di essi comporta la violazione della prescrizione legislativa").

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 può essere soddisfatta mediante la predisposizione di misure tecniche e organizzative idonee a prevenire che 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 (con riguardo ai rischi per gli interessati e alle responsabilità per il titolare in ordine all'acquisizione di informazioni afferenti alla sfera privata dei dipendenti, v. da ultimo, provv. del 15 aprile 2021 n. 137 in corso di pubblicazione; ma v. pure, provv. del 26 marzo 2020, n. 64 - "Didattica a distanza: prime indicazioni" -, doc. web n. 9300784, par. 5 e, già, 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 tutt'ora validi).

Sotto altro aspetto, invece, non risulta specificamente comprovato dagli atti che, nel caso di specie, siano stati effettivamente trattati dati relativi a categorie particolari in violazione delle prescrizioni di cui al Provvedimento del Garante n. 146 del 5 giugno 2019 (recante le prescrizioni relative al trattamento di categorie particolari di dati, ai sensi dell'art. 21, comma 1, del d.lgs. 10 agosto 2018, n. 101, doc. web n. 9124510 e in G. U., 29.7.2019, n. 176), dovendosi pertanto archiviare sul punto il rilievo con riguardo a tale specifico profilo.

3.3. Il principio di limitazione della finalità e il mancato rispetto delle condizioni previste dalla disciplina di settore con riguardo all'utilizzo dei dati raccolti per altri fini connessi alla gestione del rapporto di lavoro.

Stante il principio in base al quale i dati devono essere "raccolti per finalità determinate, esplicite legittime, e successivamente trattati in modo che non sia incompatibile con tali finalità" (art. 5, par. 1, lett. b), del Regolamento) si osserva che il Comune si è riservato, fin dal 2000, la possibilità di consultare i dati relativi alla navigazione web dei propri dipendenti, su richiesta del dirigente competente e per il tramite dell'amministratore di sistema, per eventuali esigenze legate a procedimenti disciplinari. Ciò è in concreto avvenuto nei confronti di taluni dipendenti (indicati dal Comune nel numero di 27 lavoratori), tra i quali il reclamante, con conseguente utilizzo dei dati raccolti dal sistema nell'ambito del procedimento disciplinare a carico dello stesso.

Nel premettere che, solo dal 2015, il quadro normativo vigente consente che i dati raccolti ai sensi dell'art. 4, commi 1 e 2 della legge n. 300/1970 possano essere utilizzati dal datore di lavoro "a tutti i fini connessi al rapporto di lavoro" a condizione che "sia data al lavoratore adeguata informazione delle modalità d'uso degli strumenti e di effettuazione dei controlli e nel rispetto di quanto disposto dal decreto legislativo 30 giugno 2003, n.196" (art. 4, comma 3 l. n. 300/1970), si osserva quanto segue.

Il richiamato quadro normativo consente quindi al titolare (datore di lavoro) di utilizzare, per ulteriori trattamenti necessari alla gestione del rapporto di lavoro, solo le informazioni raccolte nel rispetto delle condizioni e dei limiti previsti dall'art. 4, commi 1 o 2, della l. n. 300/70 e della disciplina di protezione dati. Tali successive ed eventuali operazioni di trattamento presuppongono quindi la necessità di fornire agli interessati un'adeguata informativa sui trattamenti che il datore di lavoro si riserva di effettuare e l'opportuna configurazione dei sistemi in modo che siano poste in essere le sole operazioni necessarie e raccolti i soli dati pertinenti in relazione alla finalità principale per la quale i dati sono originariamente trattati (sul punto, v. Provv. 24 maggio 2017, n. 247, doc. web n. 6495708, spec. punto 5.3 e lett. e) del dispositivo). In altre parole, il quadro normativo vigente consente al datore di lavoro di utilizzare i dati personali dei lavoratori per ulteriori finalità riconducibili all'ambito della gestione del rapporto (cfr., l'esemplificazione contenuta nell'art. 88 del Regolamento) nei limiti in cui l'originaria raccolta sia stata lecitamente effettuata, avuto riguardo alla finalità principale e nel rispetto dei principi generali della protezione dei dati.

Nel caso di specie risulta, invece, che i dati relativi alla navigazione web del reclamante, originariamente raccolti e trattati tramite il citato sistema in modo non proporzionato e non conforme alla disciplina in materia di protezione dei dati personali, in violazione dell'art. 5, par. 1, lett. a) e c), 6 del Regolamento e dell'art. 113 del Codice, e senza un'adeguata informativa ai sensi dell'art. 13 del Regolamento, siano stati successivamente impiegati per contestare addebiti disciplinari allo stesso, non rispettando quindi i presupposti e le condizioni previste dalla richiamata disciplina di settore all'art. 4, comma 3, della legge n. 300 del 1970.

Nel corso dell'istruttoria il titolare ha dichiarato che l'analisi dei log relativi alla navigazione dell'interessato "non ha portato all'applicazione di sanzioni disciplinari, poiché non erano attendibili, riportando anche una serie di siti (es. collegati a banner) che non erano stati necessariamente visitati dal lavoratore, senza possibilità di distinzione tra il sito effettivamente visitato e quelli a navigazione indiretta/involontaria. Per lo stesso motivo, anche il tempo di navigazione su tali siti non era un'informazione attendibile ai fini disciplinari" (cfr., verbale audizione XX). Contrariamente a quanto sostenuto dal titolare del trattamento, tuttavia, si ritiene che non possa essere ritenuta rilevante, al fine di escludere la responsabilità dello stesso, la circostanza in base alla quale, data la scarsa qualità dei dati raccolti e la loro accertata inattendibilità, il procedimento disciplinare sia stato successivamente archiviato, posto che, in ogni caso, i dati relativi alla navigazione web del reclamante (analogamente a quanto accaduto nei precedenti 27 casi come confermato dal Comune) sono stati comunque utilizzati per avviare il predetto procedimento disciplinare e trattati nell'ambito dello stesso, non rispettando i presupposti e le condizioni previste dalla richiamata disciplina di settore all'art. 4, comma 3, della legge n. 300 del 1970, dunque, in violazione degli artt. 5, par. 1, lett. a), 6 e 88 del Regolamento e in violazione dell'art. 114 del Codice in riferimento all'art. 4, comma 3, della legge n. 300 del 1970.

3.4. L'attuale trattamento dei dati relativi alla navigazione in internet dei dipendenti.

Nel prendere atto del fatto che il titolare, a seguito dell'interlocuzione con l'Autorità, ha provveduto stipulare un nuovo accordo sindacale e a modificare la tipologia di dati di navigazione web raccolti, prevedendo nuove procedure per l'attivazione delle verifiche sul traffico dei dipendenti solo in presenza di anomalie rilevabili dagli amministratori di rete (cfr., nota del XX relativi allegati nonché verbale audizione dell'XX), si formulano di seguito ulteriori osservazioni in merito.

La metodologia individuata dall'Ente, finalizzata alla minimizzazione dei dati trattati ("i log, che precedentemente riportavano l'"user id" in maniera esplicita, ora non riportano più tale informazione ma solo un "id macchina", che consente di risalire all'identità dell'utente solo con una successiva elaborazione, effettuando l'abbinamento tra "id macchina" e lavoratore a cui tale macchina è assegnata. In questo modo sono stati pseudonimizzati i dati personali raccolti" – cfr. verbale audizione dell'XX), non può ritenersi ancora sufficiente a rendere proporzionato il complessivo trattamento e a minimizzare i dati personali raccolti, trattandosi, invece, di una mera pseudonimizzazione, come definita all'art. 4, punto n. 5, del Regolamento, dei dati personali in questione. Le misure introdotte dall'amministrazione consentono ancora all'amministrazione la raccolta dei dati di navigazione individualmente effettuata e l'associazione fra questi dati e l'interessato, ancorché attraverso un'indiretta e peraltro semplice elaborazione, dal momento che la postazione di lavoro è assegnata in via pressoché esclusiva al dipendente, che la presenza di eventuali postazioni condivise fra più persone è da considerarsi circostanza residuale e che, anche in tale limitata ipotesi, è sempre possibile individuare l'utilizzatore della postazione in un determinato lasso di tempo. Ciò è, peraltro, confermato da quanto riportato nell'accordo stipulato il 4 febbraio 2020, secondo cui "tali log, pur pseudonimizzati nello user id, consentono in via secondaria il controllo".

La misura introdotta, non garantendo quindi un'adeguata separazione fra i dati di navigazione in Internet (fra cui in particolare l'URL visitato) e le identità dei dipendenti, non può pertanto essere ritenuta adeguata ad assicurare il rispetto della disciplina di protezione dei dati, con particolare riguardo alla ai principi di liceità, correttezza e trasparenza, e minimizzazione, nonché delle specifiche disposizioni che vietano al datore di lavoro di acquisire, anche incidentalmente, dati relativi alla sfera extra lavorativa del dipendente (art. 113 del Codice).

Né può essere ritenuto sufficiente, a tal fine, che il datore di lavoro si limiti a richiamare il corretto utilizzo degli strumenti di rete da parte de propri dipendenti, come riportato nell'accordo sindacale e nell'informativa (cfr. all. nn. 11 e 12 alla nota del XX), facendo leva esclusivamente sulla responsabilità dei dipendenti e sul divieto di utilizzo degli strumenti informativi per fini personali ("è di fondamentale importanza che il lavoratore si attenga rigorosamente alle istruzioni per l'utilizzo degli strumenti informatici ed al Codice di comportamento approvato con deliberazione della Giunta d.d. 30.10.2015, n. 608, affinché i log oggetto di trattamento non rivelino informazioni che attengono alla Sua sfera privata extraprofessionale, e/o alle categorie di dati di cui agli artt. 9 e 10 del GDPR 2016/679").

Per tali ragioni, si ritiene che gli adeguamenti proposti non consentano di superare del tutto, allo stato attuale, le criticità evidenziate e che, quindi, il trattamento in corso debba ritenersi, tutt'ora, non pienamente conforme alla disciplina in materia di protezione dei dati.

3.5. Mancata esecuzione di una valutazione d'impatto sulla protezione dei dati.

In attuazione del principio di responsabilizzazione (che impone l'adozione di adeguate misure tecniche e organizzative atte a garantire che il trattamento avvenga in conformità alla normativa vigente; cfr. artt. 24 e 25 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.

Il trattamento dei dati personali degli interessati è stato effettuato in assenza di una preliminare valutazione d'impatto sulla protezione dei dati sul presupposto che il trattamento non presentasse rischi specifici per gli stessi.

Tenuto conto delle indicazioni fornite anche a livello europeo sul punto, si rileva, invece, che il

trattamento reso possibile dal descritto sistema, per come configurato, consistente nella raccolta preventiva e generalizzata di dati relativi alle connessioni ai siti web dei singoli dipendenti (originariamente associati in via diretta al nominativo, ad oggi, attraverso l'id macchina), nella memorizzazione per trenta giorni e nella possibilità di estrarre una reportistica relativa alla navigazione di singoli dipendenti, comporta rischi specifici per i diritti e le libertà degli interessati nel contesto lavorativo (art. 35 del Regolamento).

Tanto in considerazione della particolare "vulnerabilità" degli interessati nel contesto lavorativo (cfr. considerando 75 e art. 88 del Regolamento e le "Linee guida concernenti la valutazione di impatto sulla protezione dei dati nonché i criteri per stabilire se un trattamento "possa presentare un rischio elevato" ai sensi del Regolamento 2016/679", WP 248 del 4 aprile 2017, che, tra le categorie di interessati vulnerabili, menziona espressamente "i dipendenti") e del fatto che in tale ambito l'impiego di sistemi che comportano il "monitoraggio sistematico", inteso come "trattamento utilizzato per osservare, monitorare o controllare gli interessati, ivi inclusi i dati raccolti tramite reti" (cfr. criterio n. 3 indicato nelle Linee guida, cit., ma vedi anche criteri 4 e 7), può presentare rischi, come emerso nel caso di specie, in termini di possibile monitoraggio dell'attività dei dipendenti (cfr. artt. 35 e 88, par. 2, del Regolamento v. anche Provv. del Garante dell'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").

Per tali ragioni, nel prendere atto che, seppur tardivamente e nel corso dell'istruttoria, il titolare ha provveduto a effettuare la valutazione d'impatto sulla protezione dei dati personali in relazione al trattamento dei "log di navigazione", individuando una serie di misure tecniche ed organizzative con l'intento di attenuare i rischi per gli interessati derivanti dal trattamento (cfr. allegato recante data XX, alla nota XX), si ritiene che, quantomeno con riguardo ai trattamenti anteriori al mese di XX, il trattamento sia stato effettuato in assenza di una valutazione di impatto e quindi in violazione dell'art. 35 del Regolamento.

3.6. I trattamenti di dati personali connessi alla richiesta di accertamento medico straordinario nell'ambito della c.d. "sorveglianza sanitaria" (d.lgs. 9 aprile 2008, n. 81).

Con riguardo al trattamento dei dati del reclamante effettuato mediante il modulo della richiesta di accertamento medico straordinario, si rileva quanto segue.

La finalità di sicurezza e salute sui luoghi di lavoro afferisce, tipicamente, all'adempimento degli obblighi in materia di "diritto del lavoro", che legittimano il trattamento di dati personali dei dipendenti da parte del datore di lavoro (artt. 5, 6, par. 1, lett. c), 9, par. 2, lett. b), e 88 Regolamento) e del medico competente (art. 9, parr. 2, lett. h), e 3, del Regolamento; cfr. anche art. 2-sexies, comma 2, lett. u), del Codice), ciascuno nell'ambito dei differenti compiti ed entro i precisi limiti fissati dalla legge. Ciò anche nel quadro delle disposizioni nazionali più specifiche e di maggior tutela che garantiscono la dignità e la libertà del dipendente nel contesto lavorativo (artt. 88 del Regolamento e 113 del Codice).

Pertanto, mentre il datore di lavoro "vigila affinché i lavoratori […] non siano adibiti alla mansione lavorativa specifica senza il prescritto giudizio di idoneità" (es. art. 18 del d.lgs. n. 81/2008), il medico competente, nell'ambito delle proprie attività di sorveglianza sanitaria ("la sorveglianza sanitaria è effettuata dal medico competente"), è l'unico soggetto legittimato a trattare i dati relativi alla salute dei lavoratori e a verificare l'idoneità alla "mansione specifica" (artt. 25, 39, comma 5, e 41, comma 4, del d.lgs. n. 81/2008), potendo, "in funzione della valutazione del rischio" e delle "condizioni di salute" dei lavoratori, stabilire la necessità di sottoporre i lavoratori a ulteriori indagini diagnostiche; è, altresì, previsto che il lavoratore possa rivolgersi direttamente al medico competente per ottenere una visita straordinaria correlata alle proprie specifiche o sopravvenute condizioni di salute (art. 41, commi 2 e 4, del d.lgs. 81/2008).

In base al richiamato quadro normativo, il datore di lavoro può conoscere il mero giudizio di idoneità alla mansione specifica corredato dalle eventuali prescrizioni che il professionista fissa come condizioni di lavoro (cfr. art. 41, comma 6-bis, del d.lgs. n. 81/2008). Pertanto, solo una volta effettuata la visita, il datore di lavoro dovrà, in base al quadro normativo sopra delineato, attuare le misure eventualmente indicate dal medico competente e adibire il lavoratore alle corrispondenti mansioni (art. 42 del d.lgs. n. 81/2008).

Non è invece previsto che, come prospettato dal Comune, "nelle more dell'effettuazione della visita medica" il dipendente informi il proprio dirigente di "eventuali situazioni di disagio personale" al fine di ottenere la "modifica […del] l'assegnazione dei compiti e delle attività assegnati al dipendente che effettua la richiesta di visita o le modalità di prestazione dell'attività lavorativa" (cfr. verbale audizione in atti).

Né tale trattamento può risultare giustificato dalla necessità che si "debba verificare la correttezza e la congruità degli importi fatturati al Comune" (cfr. verbale audizione in atti), essendo previsto che il medico "comuni[chi] al datore di lavoro […] i risultati anonimi collettivi della sorveglianza sanitaria" (cfr., art. 25, comma 1, lett. i), del d.lgs. n. 81/2008), che potranno eventualmente essere utilizzati, in assenza di altri elementi, in sede di contabilizzazione dell'attività svolta e di liquidazione dei corrispettivi al medico competente.

Ciò premesso, si ritiene che il modulo originariamente in uso presso l'amministrazione, che il dipendente doveva compilare per richiedere al medico competente un accertamento straordinario sulle proprie condizioni di salute, nella parte in cui presupponeva la necessaria presa visione del Direttore di Ripartizione, non fosse conforme al richiamato quadro normativo di settore comportando - indipendentemente dall'espressa indicazione della patologia da parte del lavoratore - che soggetti delegati allo svolgimento delle funzioni datoriali all'interno dell'amministrazione, venissero a conoscenza di dati personali relativi allo stato di salute, diversi e ulteriori rispetto a quelli consentiti dalla legge, essendo, pertanto, il trattamento dei dati personali dei lavoratori che hanno compilato detto modulo avvenuto in violazione degli artt. 5, 9, par. 2, lett. b), e 88 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, si rileva che le dichiarazioni rese dal titolare del trattamento negli scritti difensivi della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice seppure meritevoli di considerazione e indicative della piena collaborazione del titolare al fine di attenuare i rischi del trattamento, rispetto alla situazione presente all'atto dell'avvio dell'istruttoria, non consentono tuttavia di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano quindi 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.

Dalle verifiche compiute sulla base degli elementi acquisiti, anche attraverso la documentazione inviata dal titolare del trattamento, nonché dalle successive valutazioni, è stata accertata la non conformità di taluni trattamenti aventi ad oggetto dati personali dei dipendenti. Tanto, con riguardo sia alla disciplina previgente (ovvero al Codice, nel testo precedente alle modifiche apportate dal d.lgs. 10 agosto 2018, n. 101), sia all'attuale disciplina in materia di protezione dei dati.

Per la determinazione della norma applicabile, sotto il profilo temporale, deve essere richiamato, in particolare, il principio di legalità di cui all'art. 1, comma 2, della l. n. 689/1981, ai sensi del quale le leggi che prevedono sanzioni amministrative si applicano soltanto nei casi e nei tempi in esse considerati. Ciò determina l'obbligo di prendere in considerazione le disposizioni vigenti al momento della commessa violazione, che nel caso in esame – data la natura permanente degli illeciti contestati – deve essere individuato nell'atto di cessazione della condotta illecita. Nel

prendere atto che, limitatamente ad alcune condotte, la cessazione dei trattamenti illeciti sia avvenuta successivamente alla data in cui il Regolamento è divenuto applicabile (cfr. nota del XX, nella quale si dà conto delle varie iniziative assunte dal titolare per porre rimedio alle violazione contestate), mentre, con riguardo alla raccolta dei dati di navigazione in Internet, il trattamento illecito risulta tutt'ora in corso, si ritiene che il Regolamento e il Codice costituiscano la normativa alla luce della quale valutare le condotte lamentate nel reclamo.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dal Comune di Bolzano, in quanto esso è avvenuto in maniera non conforme ai principi generali del trattamento, nonché in violazione degli artt. 5, par. 1, lett. a) e c), 6, 9, 13, 35, 88 del Regolamento, nonché degli artt. 113 e 114 del Codice.

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.

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

Tenuto conto di quanto rappresentato relativamente alla raccolta dei dati relativi alla navigazione web associati a dipendenti, seppure indirettamente identificabili, anche a seguito delle misure introdotte a decorrere dal 17 gennaio 2020, in ragione dell'illiceità del trattamento in corso, si ritiene necessario, ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di ingiungere al Comune di Bolzano, entro sessanta giorni dalla notifica del presente provvedimento, l'adozione di misure tecniche e organizzative idonee ad anonimizzare il dato relativo alla postazione di lavoro dei dipendenti rilevata nei log di navigazione web nonché di cancellare i dati personali presenti nei log di navigazione web già registrati.

Resta salva la possibilità di intraprendere rilevazioni di dati puntuali di navigazione in internet, solo a fronte di riscontrate anomalie di traffico web la cui entità sia tale da compromettere la sicurezza e l'integrità dei sistemi informativi, secondo quanto in parte previsto dalle procedure da ultimo individuate e inserite nell'accordo sindacale del 4 febbraio 2020 (punti 2-6), che a tal fine dovranno essere opportunamente aggiornate.

Ai sensi dell'art. 157 del Codice, il Comune 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.

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

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

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie – considerando anche il richiamo contenuto nell'art. 166, comma 2, del Codice – la violazione delle disposizioni

citate è soggetta all'applicazione della stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

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

Ai fini dell'applicazione della sanzione è stato considerato che il trattamento consistente nella raccolta sistematica e preventiva dei dati personali riferiti alla navigazione in internet ha interessato tutti i dipendenti del Comune (circa mille) e che, in taluni casi (n. 27 e tra questi il reclamante), i dati siano stati utilizzati per consultazioni specifiche mediante estrazione di report di dettaglio della navigazione web dei dipendenti, in violazione dei principi generali del trattamento e delle disposizioni nazionali di settore che tutelano specificamente la dignità degli interessati nei luoghi di lavoro (art. 88 del Regolamento, nonché artt. 113 e 114 del Codice). È stata altresì considerato l'ampio arco temporale del trattamento, intrapreso fin dal 2000.

Di contro è stato considerato che il Comune ha manifestato una particolarmente collaborazione nel corso dell'istruttoria provvedendo ad apportare, già a seguito della prima richiesta di elementi dell'Ufficio, taluni primi correttivi ai trattamenti oggetto di reclamo e ad avviare, in pari tempo, i necessari approfondimenti funzionali alla progressiva adozione anche delle misure tecniche e organizzative che, ancorché non sufficienti ad assicurare la piena conformità dei trattamenti alle disposizioni in materia di protezione dei dati, denotano tuttavia, un particolare impegno nell'attenuare gli effetti negativi del trattamento nei confronti dei dipendenti. Ai fini della commisurazione della complessiva sanzione è stato considerato altresì che il titolare del trattamento avesse confidato nella liceità dei trattamenti posti in essere avendo assolto agli obblighi previsti dalla disciplina di settore, stipulando, fin dal 2000 un accordo con le organizzazioni sindacali, il cui contenuto aveva a oggetto tuttavia trattamenti che sono risultati, nel corso dell'istruttoria, non conformi ai principi di protezione dei dati.

Non risultano, inoltre, precedenti violazioni commesse dal titolare del trattamento o precedenti provvedimenti di cui all'art. 58 del Regolamento.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria, nella misura di euro 84.000 (ottantaquattromila) per la violazione degli artt. 5, par. 1, lett a) e c), 6, 9, 13, 35, 88 del Regolamento, nonché degli artt. 113 e 114 del Codice.

Tenuto conto della particolare delicatezza dei dati illecitamente trattati, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e dall'art. 16 del Regolamento del Garante n. 1/2019.

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

TUTTO CIÒ PREMESSO IL GARANTE

rileva l'illiceità del trattamento effettuato dal Comune di Bolzano per violazione degli artt. 5, 6, 9, 88 e 35 del Regolamento, nonché 113 e 114 del Codice nei termini di cui in motivazione e dichiara ai sensi dell'art. 2-decies del Codice l'inutilizzabilità dei dati trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali, salvo quanto previsto dall'art. 160-bis del Codice;

ORDINA

al Comune di Bolzano, in persona del legale rappresentante pro-tempore, con sede legale in

Bolzano, Piazza Municipio, 5, C.F. 00389240219, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento e 166, comma 2, del Codice, di pagare la somma di euro 84.000,00 (ottantaquattromila) 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 trenta giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

al Comune di Bolzano:

a) di pagare la somma di euro 84.000,00 (ottantaquattromila), in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, secondo le modalità indicate in allegato, entro trenta giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della l. n. 689/1981;

b) ai sensi dell'art. 58, par. 2, lett. d), del Regolamento, di adottare, entro sessanta giorni dalla notifica del presente provvedimento, misure tecniche e organizzative idonee ad anonimizzare il dato relativo alla postazione di lavoro dei dipendenti rilevata nei log di navigazione web nonché di cancellare i dati personali presenti nei log di navigazione web registrati, aggiornando le procedure interne da ultimo individuate e inserite nell'accordo sindacale del 4 febbraio 2020;

c) 1-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 trenta giorni dalla notifica del presente provvedimento, le iniziative che intende intraprendere in relazione a quanto disposto 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;

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice;

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

Ai sensi dell'art. 78 del Regolamento, degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, 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, 13 maggio 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei