Provvedimento del 17 luglio 2024 [10053224]

VEDI ANCHE Newsletter del 22 ottobre 2024

[doc. web n. 10053224]

Provvedimento del 17 luglio 2024

Registro dei provvedimenti
n. 472 del 17 luglio 2024

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 (di seguito, "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTO il reclamo presentato dal sig. XX ai sensi dell'art. 77 del Regolamento, con cui veniva lamentato l'illecito trattamento di dati personali da parte di Seletra S.p.A.;

ESAMINATA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. Il reclamo presentato all'Autorità e l'avvio dell'istruttoria.

Con il reclamo presentato in data 28/12/2021, il sig. XX lamentava una violazione della disciplina in materia di protezione dei dati personali posta in essere da Selectra S.p.A. (di seguito "la Società"), con cui aveva intrattenuto un rapporto di collaborazione in qualità di agente di commercio.

In particolare, il reclamante rappresentava che, a seguito dell'interruzione del rapporto di collaborazione avvenuta in data 24/02/2021, la Società aveva mantenuto attivo l'account di posta elettronica aziendale di tipo individualizzato, a lui assegnato in costanza del rapporto di collaborazione ("XX"), accedendo al contenuto di tutta la corrispondenza in transito sul predetto account che, infatti, veniva prodotta nel corso di un giudizio instaurato dinanzi al Tribunale di

Venezia.

Con nota del 14/03/2022, l'Ufficio formulava nei confronti della Società una richiesta di informazioni, ai sensi dell'art. 157 del Codice, al fine di acquisire utili elementi di valutazione in ordine a quanto rappresentato nel reclamo.

La Società forniva riscontro con nota del 13/04/2022 e, in tale occasione, precisava che:

- "Selectra non ha mai acceduto alla casella [di posta elettronica] in uso al reclamante durante la vigenza del rapporto lavorativo";

- "Selectra esegue periodicamente un backup delle caselle di posta elettronica aziendali, mediante il software MailStore. L'esecuzione del backup in parola non richiede alcun accesso da parte del personale aziendale, poiché è eseguito con modalità automatiche dal software MailStore. Il backup di ciascuna casella di posta elettronica aziendale è conservato per un periodo massimo di tre anni, dopo la cessazione di ogni rapporto lavorativo o di collaborazione";

- "ha avviato un'azione giudiziaria nei confronti dell'odierno reclamante e di altri soggetti, […], a seguito di fondati sospetti di sottrazione di segreti aziendali e di ulteriori illeciti perpetrati dal [reclamante]";

- "al fine di tutelare i propri segreti aziendali, Selectra ha dato mandato allo studio di ingegneria forense XX […] per eseguire una perizia con la finalità, tra le altre cose, di accertare eventuali fenomeni di esfiltrazione di dati aziendali segreti da parte del [reclamante], nel periodo di vigenza del rapporto lavorativo";

- "in seno a tale mandato, lo studio XX ha acquisito una copia forense del backup della casella di posta elettronica aziendale [assegnata al reclamante], direttamente dall'applicativo MailStore";

- "l'account di posta elettronica aziendale [assegnato al reclamante] è stato disattivato entro i tre giorni successivi al 05 marzo 2021, data in cui Selectra ha inviato una specifica direttiva al reparto IT";

- "lo stato attuale dell'account è […] non attivo";

- "Selectra ha fornito al [reclamante] una copia dell'informativa Privacy e del regolamento aziendale in data 15 marzo 2019";

Veniva prodotta in atti copia dell'"Informativa per i collaboratori esterni/rappresentanti, anche per dati sensibili/particolari ex art. 13 Reg. Europeo 679/2016", e del documento avente ad oggetto "Attrezzatura utilizzata dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze", entrambi consegnati al reclamante e da questi sottoscritti in data 15/03/2019.

In particolare, il documento "Attrezzatura utilizzata dal lavoratore per rendere la prestazione lavorativa e gli strumenti di registrazione degli accessi e delle presenze" specificava che:

- "nell'ipotesi di cessazione dell'attività lavorativa o di assenza, [la Società si riserva di] accedere alla casella di posta utilizzata in pendenza del rapporto lavorativo, per consentire la continuità lavorativa (…)";

- "il sistema informatico registra i suoi accessi alle caselle di posta elettronica e al gestionale, elaborando costantemente dei report di log che vengono conservati dal sistema per una

durata di almeno 6 mesi";

- "Ai fini della tutela di riservatezza, la scrivente informa ex art. 13 reg. Eur. 679/2016 e art. 4 L. 300/1970 (Statuto dei lavoratori) che gli strumenti sopra descritti sono tutti potenzialmente idonei ad attuare il controllo a distanza della sua prestazione lavorativa";

- "nell'ipotesi in cui lo ritenesse strettamente utile e/o strettamente necessario, potrà effettuare verifiche a campione finalizzate ad accertare la correttezza della prestazione, nonché potrà effettuare controlli tesi alla verifica del regolare utilizzo degli strumenti in dotazione e dei relativi sistemi e del loro regolare funzionamento, anche mediante test con l'avvertimento di cui all'art. 4 Legge 300/1970 (…) e che le informazioni raccolte ai sensi dei commi 1 e 2, art. 4, legge 300 del 20 maggio 1970, derivanti dagli strumenti per rendere la prestazione, saranno utilizzati a tutti i fini connessi al rapporto di lavoro (ivi comprese le procedure sanzionatorie)".

- "il trattamento eseguito da Selectra [è] avvenuto nel rispetto dei principi di pertinenza e non eccedenza dei dati. La base giuridica del trattamento è data dal diritto di Selectra di tutelare i propri diritti a fronte di un fondato sospetto di sottrazione massiva dei propri dati (inclusi segreti commerciali e banche dati) […]";

- la Società ha "disattivato tempestivamente la casella di posta elettronica del reclamante, senza mai accedervi direttamente, ed ha eseguito la conservazione dei dati e ne [ha] permesso l'esame ad una società di consulenza esterna, esattamente nei limiti dell'informativa resa al reclamante, con le modalità […] indicate nel regolamento aziendale".

2. L'avvio del procedimento per l'adozione dei provvedimenti correttivi dell'Autorità.

Sulla base delle dichiarazioni rese e della documentazione prodotta nel corso dell'attività istruttoria, l'Ufficio provvedeva a notificare alla Società l'atto di avvio del procedimento sanzionatorio, ai sensi dell'art. 166, comma 5, del Codice per la violazione degli artt. 5, par. 1, lett. a), c) ed e), 13 e 88 del Regolamento, art. 114 del Codice (nota del 07/09/2022).

Con le memorie difensive inviate il 05/10/2022, ai sensi dell'art. 18 della legge n. 689/1981 e dell'art. 166 comma 6 del Codice, la Società rappresentava che:

- "Il sig. XX non è mai stato lavoratore dipendente della Selectra, né quest'ultima ne è mai stata datore di lavoro, essendo intercorso tra le parti esclusivamente un contratto di agenzia ai sensi degli artt. 1742 ss. c.c.";

- pertanto, "risulta non pertinente l'intero impianto accusatorio di asserita violazione del Codice (…) siccome fondato da codesta Autorità sulla contestazione a Selectra di aver eseguito un trattamento di dati personali posto in essere in violazione dell'art. 114 del Codice (che richiama l'art. 4 della l. 300/1970 quale condizione di liceità del trattamento) (…)";

- "Si precisa altresì che l'agente di commercio era del pari estraneo all'apparato aziendale di Selectra a Bolzano o altrove; tra l'altro non era munito neppure di un suo ufficio o di personal computer (…), operando solo al di fuori e presso la sua autonoma azienda (…). Si vuole inoltre precisare che l'agente di commercio ha utilizzato la casella che Selectra gli aveva messo a disposizione esclusivamente per l'uso strettamente aziendale-professionale (…) per utilizzi diversi e personali del tutto avulsi dalla sua attività di agente di commercio. Salvo poi dolersi se Selectra, dopo avere scoperto le attività di concorrenza sleale ex art. 2589 n. 3 c.c. e di sottrazione di dati segreti (…), ha lamentato l'emersione di e-mail sue personali da egli fatte transitare illegittimamente attraverso la casella di posta elettronica di Selectra (…);

- "la Selectra ha interesse a precisare che tutti i trattamenti eseguiti anche persino nei

confronti dei propri dipendenti (benché il reclamante non lo fosse mai stato, essendo un agente di commercio esterno all'azienda) sono stati ispirati a principi di correttezza come indicato nel Regolamento".

Con riferimento agli specifici aspetti di illiceità contestati, la Società osservava che:

- il back up sulle caselle e-mail, eseguito mediante l'applicativo Mail Store, "è una misura tecnica di sicurezza" disposta in ottemperanza all'art. 5, par. 1, lett. f) del Regolamento "per garantire la sicurezza e l'integrità dei dati personali trattati da attacchi informatici (…). L'esecuzione del backup non richiede alcun accesso da parte del personale aziendale, mentre il periodo massimo di conservazione pari a tre anni, è un parametro teorico che delimita il tempo massimo di retention e, di conseguenza, il tempo massimo per cui è possibile recuperare dati e/o informazioni a ritroso in caso di disservizio o attacco informatico";

- rispetto all'informativa resa ai propri dipendenti e collaboratori, questa "specificava la possibilità per Selectra di accedere al contenuto delle caselle e-mail per eventuali e comprovate esigenze di continuità lavorativa (…). La finalità indicata nell'informativa resa al [reclamante] è del tutto legittima, perché riferibile a caselle e-mail aziendali assegnate a soggetti diversi dai dipendenti. Gli agenti di commercio della Selectra, infatti, non hanno accesso ai software gestionali aziendali (CRM, ERP, etc.) e gestiscono la loro routine esclusivamente mediante la posta elettronica";

- "l'esigenza di assicurare la continuità lavorativa costituisce la finalità per la quale la Selectra, esclusivamente mediante un soggetto incaricato, potrebbe accedere alla casella di posta elettronica";

- "occorre ribadire che la Selectra mai ha acceduto alle caselle e-mail aziendali (…). L'accesso eseguito dallo Studio XX, esclusivamente mediante l'applicativo Mail Store, è avvenuto su dati raccolti da Selectra per una finalità determinata e legittima di tutela in ambito giudiziario ai sensi dell'art. 5, par. 1, lett. b) e sono stati trattati in modo lecito, corretto e trasparente ai sensi dell'art. 5, par. 1, lett. a), poiché l'informativa resa al ricorrente era cristallina sul punto";

- "in attesa della definizione del reclamo, Selectra ha comunque deciso di sospendere l'uso di Mail Store e di intraprendere un processo di revisione delle proprie informative privacy con l'obiettivo di renderle ancora più sinottiche nei confronti degli interessati".

3. L'esito dell'istruttoria e del procedimento per l'adozione dei provvedimenti correttivi.

All'esito dell'esame delle dichiarazioni rese dalla parte nel corso del procedimento, nonché della documentazione acquisita, risulta che la Società, in qualità di titolare del trattamento, ha effettuato alcune operazioni di trattamento che non sono conformi alla disciplina in materia di protezione dei dati personali. In proposito si evidenzia che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante".

In particolare, è emerso che la Società ha incaricato uno studio di ingegneria forense di svolgere un'attività di indagine sul contenuto della posta elettronica del reclamante utilizzando l'applicativo Mail Store (installato sui pc aziendali). Le e-mail raccolte tramite l'applicativo (individuate dal reclamante in 34) sono state utilizzate nell'ambito di un procedimento giudiziario avviato nei confronti del reclamante dinanzi al Tribunale di Venezia.

È altresì emerso che la Società, in base a quanto risulta dal documento “Attrezzatura utilizzata dal lavoratore per rendere la prestazione lavorativa e strumenti di registrazione degli accessi e delle presenze-Modalità e limiti di impiego”, (allegato all’informativa consegnata al reclamante in qualità di collaboratore e rivolto anche ai dipendenti della Società), tratta i dati relativi agli account di posta elettronica aziendale individualizzati in violazione della disciplina di protezione dei dati.

3.1. Violazione degli artt. 5. par. 1, lett. a) e 13 del Regolamento.

In primo luogo, occorre precisare che, aldilà della qualificazione del rapporto intercorso tra la Società e il reclamante, il trattamento avente ad oggetto i dati personali dell’interessato è imputabile alla Società che ha agito in qualità di titolare del trattamento, secondo la definizione di cui all’art. 4, par. 1, n. 7 del Regolamento (“titolare del trattamento: la persona fisica o giuridica,… che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali”).

A fronte del trattamento svolto, che ha riguardato prevalentemente i dati contenuti nella casella di posta elettronica, è risultato che l’informativa resa dalla Società non è conforme alla disciplina di protezione dei dati, in quanto inidonea e incompleta nel rappresentare compiutamente le caratteristiche e le modalità dei trattamenti svolti, con particolare riferimento ai tempi di conservazione dei dati relativi alla posta elettronica e alle modalità e le finalità con cui sono effettuati i controlli da parte della Società in qualità di titolare del trattamento.

In particolare, dall’esame della documentazione in atti, risulta che l’informativa rilasciata al reclamante prevede, in via assai generale, la conservazione dei dati personali unicamente per consentire l’espletamento di tutti gli adempimenti connessi o derivanti dalla conclusione del rapporto di lavoro, indicando come tempo di conservazione il termine di 10 anni in conformità alle disposizioni di cui agli artt. 19 e 22 del d.P.R. 600/1973.

Analogamente, nella parte del documento denominata “Attrezzatura utilizzata dal lavoratore per rendere la prestazione lavorativa e strumenti di registrazione degli accessi e delle presenze”, l’interessato è informato della elaborazione di log degli accessi alla posta elettronica e al gestionale, che sono conservati “per una durata di almeno 6 mesi”.

Nessuna informazione viene invece fornita riguardo l’effettuazione di back up del contenuto della casella individuale di posta elettronica, in vigenza di rapporto, e la conservazione del relativo contenuto, successivamente alla cessazione del rapporto con la Società, che, in base a quanto dichiarato dalla stessa, è prevista per 3 anni (note del 13/04/2022 e del 05/10/2022).

La parte del documento contenente le istruzioni sull’utilizzo degli strumenti di lavoro prevede, inoltre, la possibilità, per la Società, di accedere alla casella di posta elettronica dei lavoratori, a seguito della cessazione del rapporto lavorativo o anche nell’ipotesi di assenza, unicamente per garantire la continuità della prestazione lavorativa.

Occorre, a tal proposito, richiamare il costante orientamento di questa Autorità che, nei propri provvedimenti, ha sempre affermato che per assicurare l’ordinario svolgimento e la continuità dell’attività aziendale, è necessario predisporre sistemi di gestione documentale in grado di archiviare e conservare i documenti “con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile”. Tali caratteristiche non possono rinvenirsi nei sistemi di posta elettronica che, infatti, rispondono ad altre finalità (si veda, tra gli altri, il provvedimento n. 53 del 01/02/2018, doc. web n. 8159221 e provvedimento n. 214 del 29/10/2020 doc. web 9518890).

In ogni caso, emerge dall’analisi sopra riportata che i documenti informativi predisposti dalla Società non forniscono nessuna informazione riguardo alle indagini che la stessa si riserva di

effettuare sui contenuti memorizzati sui dispositivi aziendali né i necessari chiarimenti sulle eventuali ragioni legittime, specifiche e non generiche alla base di tali controlli e le relative modalità, che devono essere comunque conformi ai principi di liceità, proporzionalità e gradualità (v. “Linee guida per posta elettronica e internet”, provvedimento 1° marzo 2007, n. 13, doc web n. 1387522).

In proposito, si rileva che il contenuto dell’informativa deve essere conforme alla disciplina di protezione dei dati in quanto non è sufficiente informare l’interessato delle caratteristiche essenziali del trattamento, ma è anche necessario che le informazioni fornite delineino operazioni di trattamento di per sé lecite.

Deve, pertanto, confermarsi l’illiceità del trattamento dei dati personali posto in essere dalla Società mediante l’informativa predisposta che risulta inidonea per i motivi esposti. Tra l’altro, si rammenta che l’obbligo di rendere l’informativa è espressione del principio di correttezza dei trattamenti anche nell’ambito di rapporti di collaborazione.

La condotta posta in essere, dunque, è avvenuta in violazione degli artt. 5, par. 1, lett. a) (principio di correttezza) e 13 del Regolamento.

3.2. Violazione dell’art. 5, par. 1, lett. a), c) ed e) e 88 del Regolamento e dell’art. 114 del Codice.

Un ulteriore profilo di illiceità emerso all’esito dell’attività istruttoria attiene al trattamento sul contenuto della posta elettronica che transita sugli account aziendali, effettuata dalla Società per mezzo di un dispositivo software denominato Mail Store.

Sulla base delle dichiarazioni rese, risulta che attraverso tale dispositivo la Società effettua il backup del contenuto delle caselle di posta elettronica in uso ai dipendenti e ai collaboratori, in vigenza del rapporto di lavoro/collaborazione, conservandone il contenuto in modo sistematico e automatico per un periodo di tempo pari a tre anni, dopo la cessazione dei rapporti lavorativi.

La Società ha dichiarato, nelle memorie difensive, che la finalità di tale trattamento è garantire la sicurezza dei sistemi informatici, ai sensi dell’art. 5, par. 1, lett. f), del Regolamento.

In primo luogo, si rileva che la Società, a fronte della conservazione anche del contenuto delle comunicazioni effettuate da dipendenti e collaboratori tramite la posta elettronica per un tempo così esteso (ovvero tutta la durata del rapporto di lavoro e tre anni dopo la cessazione del rapporto stesso), non ha indicato le specifiche ragioni in virtù delle quali, tenuto anche conto delle concrete caratteristiche dei sistemi utilizzati, ha ritenuto necessario individuare un siffatto periodo di conservazione (retention) per finalità di sicurezza dei predetti sistemi.

Nello stesso tempo, la Società non ha indicato le specifiche ragioni in virtù delle quali ha ritenuto necessario conservare per l’ampio tempo di conservazione pari a 6 mesi i log di accesso alla posta elettronica e al gestionale in uso ai dipendenti (al riguardo si veda anche quanto precisato dall’Autorità sui tempi di conservazione dei log della posta elettronica nel Provvedimento del 6 giugno 2024, “Documento di indirizzo. Programmi e servizi informatici di gestione della posta elettronica nel contesto lavorativo e trattamento dei metadati”, doc web. n. 10026277).

Emerge, in ogni caso, con evidenza che il software Mail Store è stato utilizzato per finalità diverse da quella di garantire la sicurezza dei sistemi informatici. Infatti, nella fattispecie oggetto di reclamo, la Società ha analizzato le e-mail presenti sull’account del reclamante, ne ha verificato il contenuto e avviato il contenzioso.

Le operazioni di trattamento realizzate per mezzo del suddetto software (quali la raccolta, la conservazione, la consultazione) che hanno consentito di ricostruire l’attività dell’interessato,

risultano in contrasto con i principi di liceità, di minimizzazione dei dati e di limitazione della conservazione (art. 5, par. 1, lett. a), c) ed e) del Regolamento).

Infatti, in base alla disciplina posta in materia di protezione dei dati personali, nell'ambito di rapporti di lavoro/collaborazione, il titolare può trattare lecitamente i dati personali, di regola, solo se il trattamento è necessario per la gestione del rapporto stesso oppure se è necessario per adempiere a specifici obblighi o compiti posti dalle discipline di settore applicabili (art. 6, par. 1, lett. a) e c) del Regolamento, con riferimento ai dati c.d. comuni), e comunque può trattare solo i dati adeguati, pertinenti e limitati a quanto necessario rispetto alle finalità per le quali sono trattate e per un arco di tempo non superiore al conseguimento delle finalità per le quali sono trattati.

Nel caso di specie, invece, la sistematica conservazione delle e-mail, effettuata per un considerevole periodo di tempo (pari a tre anni successivi alla cessazione del rapporto), nonché la sistematica conservazione dei log di accesso alla posta elettronica e al gestionale utilizzato dai lavoratori, non sono conformi alla disciplina di protezione dei dati, in quanto non proporzionata e necessaria al conseguimento delle dichiarate finalità di sicurezza della rete informatica e di continuità dell'attività aziendale.

Sotto altro profilo, emerge che il trattamento che la Società effettua in qualità di datore di lavoro sui dati contenuti nelle caselle di posta elettronica (ad esempio a seguito della conservazione delle e-mail ricevute e inviate durante l'attività lavorativa) assegnate ai propri dipendenti è idoneo a consentire un'attività di controllo sull'attività dei lavoratori in violazione di quanto previsto dall'art. 4 della legge n. 300 del 20/05/1970, norma richiamata dall'art. 114 del Codice (v. tra gli ultimi provvedimenti adottati dal Garante, provvedimento n. 255 del 21/07/2022, doc. web n. 9809466, provvedimento n. 137 del 15/04/2021, doc web n. 9670738, provvedimento n. 214 del 29/10/2020, doc. web n. 9518890 e il provvedimento n. 353 del 29/09/2021, doc. web n. 9719914).
In base all'art. 114 del Codice, infatti, il rispetto della disposizione di cui all'art. 4 della citata legge n. 300/1970 costituisce condizione di liceità dei trattamenti di dati personali effettuati in ambito lavorativo, in quanto è una delle norme del diritto nazionale "più specifiche per assicurare la protezione dei diritti e delle libertà con riguardo al trattamento dei dati personali dei dipendenti nell'ambito dei rapporti di lavoro" individuate dall'art. 88 del Regolamento (v. artt. 5, par. 1, lett. a) e 88 del Regolamento).

Proprio con riferimento ai profili di violazione dell'art. 114 del Codice, si osserva che il software utilizzato dalla Società (fino alla dichiarata sospensione del suo utilizzo), proprio per le sue caratteristiche (così come descritte dalla parte e vista l'informativa rilasciata ai lavoratori), è idoneo a realizzare un controllo dell'attività lavorativa (su questo punto, si veda tra gli altri il provvedimento n. 303 del 13/07/2016, doc web n. 5408460).

In particolare, la Società, attraverso il citato software, ha effettuato trattamenti che consentono di ricostruire minuziosamente, anche a distanza di tempo, l'attività dei dipendenti, sia attraverso le comunicazioni scambiate via e-mail, sia attraverso i log del gestionale utilizzato per svolgere l'attività lavorativa.

Peraltro anche se, in ipotesi, tali trattamenti fossero preordinati a realizzare una delle finalità tassativamente indicate dall'art. 4, comma 1, legge n. 300/1970 cit., non risulta che la Società abbia attivato la procedura di garanzia ivi prevista (accordo con le rappresentanze dei lavoratori o, in assenza, autorizzazione dell'Ispettorato del lavoro).

In ultimo, si osserva che con riferimento all'accesso sulla posta elettronica, delegato allo studio di ingegneria forense ed effettuato secondo la Società per la "finalità determinata e legittima di tutela in ambito giudiziario" (così come indicato nell'informativa), l'Autorità ha avuto modo di precisare che il trattamento dei dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi già in atto o a situazioni precontenziose, non ad astratte e indeterminate

ipotesi di possibile difesa o tutela dei diritti (si veda il provvedimento n. 53 del 01/02/2018, doc web n. 8159221 e il provvedimento n. 255 del 21/07/2022, doc web n. 9809466).
Alla luce delle considerazioni esposte, deve quindi confermarsi l'illiceità della condotta posta in essere che è avvenuta in violazione dei principi di liceità, di minimizzazione e di limitazione della conservazione (art. 5, par. 1, lett. a), c) ed e) del Regolamento) e della disciplina di settore in materia di controlli a distanza (art. 88 del Regolamento e art. 114 del Codice).

4. Conclusioni: illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, Regolamento.

Per i suesposti motivi, l'Autorità ritiene che le dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento con riferimento agli artt. 5, par. 1, lett. a), c) ed e), 13 e 88 del Regolamento, art. 114 del Codice che risultano pertanto inidonee a consentire l'archiviazione del presente procedimento, non ricorrendo peraltro, con riferimento a tali profili, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Si rammenta che, ai sensi dell'art. 160-bis del Codice "La validità, l'efficacia e l'utilizzabilità nel procedimento giudiziario di atti, documenti e provvedimenti basati sul trattamento di dati personali non conforme a disposizioni di legge o di Regolamento restano disciplinate dalle pertinenti disposizioni processuali".

Visti i poteri correttivi attribuiti dall'art. 58, par. 2, del Regolamento, alla luce delle circostanze del caso concreto:

- si dispone il divieto dell'ulteriore trattamento dei dati estratti attraverso il software Mail Store (art. 58, par. 2, lett. f) del Regolamento);

- si dispone l'applicazione di una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i), del Regolamento).

5. 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).

All'esito del procedimento risulta che Selectra S.p.A. ha violato gli artt. 5, par. 1, lett. a), c) ed e), 13 e 88 del Regolamento, art. 114 del Codice.

Per la violazione delle predette disposizioni è prevista l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. a) e d) del Regolamento mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689).

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento che prevede che "Se, in relazione allo stesso trattamento o a trattamenti collegati, un titolare del trattamento […] viola, con dolo o colpa, varie disposizioni del presente regolamento, l'importo totale della sanzione amministrativa pecuniaria non supera l'importo specificato per la violazione più grave", l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto dal medesimo art. 83, par. 5, del Regolamento.

Con riferimento agli elementi elencati dall'art. 83, par. 2 del Regolamento ai fini della applicazione della sanzione amministrativa pecuniaria e della relativa quantificazione, tenuto conto che la sanzione deve "in ogni caso [essere] effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state considerate le seguenti circostanze:

a) in relazione alla natura, gravità e durata della violazione è stata considerata rilevante la natura della violazione che ha riguardato i principi generali del trattamento e l'obbligo dell'informativa; in particolare le violazioni hanno riguardato anche la disciplina di settore in materia di controlli a distanza nei confronti di un numero rilevante di interessati considerato che 31/12/2023 risultano 151 dipendenti in forza presso la Società;

b) con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare è stata presa in considerazione la condotta della Società e il grado di responsabilità della stessa che non si è conformata alla disciplina in materia di protezione dei dati relativamente ad una pluralità di disposizioni;

c) la Società ha cooperato con l'Autorità nel corso del procedimento dichiarando di aver sospeso l'utilizzo del software al fine di conformarsi alle indicazioni che saranno fornite dall'Autorità;

d) l'assenza di precedenti specifici a carico della Società.

Si ritiene inoltre che assumano rilevanza nel caso di specie, tenuto conto dei richiamati principi di effettività, proporzionalità e dissuasività ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione (art. 83, par. 1, del Regolamento), in primo luogo le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti dalla società con riferimento al bilancio d'esercizio per l'anno 2022.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Selectra S.p.A. la sanzione amministrativa del pagamento di una somma pari ad euro 80.000,00 (ottantamila).

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate che hanno riguardato i principi generali del trattamento 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 provvedimento sul sito internet del Garante.

Si ritiene, altresì, 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 da Selectra S.p.A. in persona del legale rappresentante, con sede legale in Bolzano, Via Antonio Pacinotti n. 11, P.I. 00123700213 ai sensi dell'art. 143 del Codice, per la violazione degli artt. 5, par. 1, lett. a), c) ed e), 13 e 88 del Regolamento e art. 114 del Codice;

DISPONE

ai sensi dell'art. 58, par. 2, lett, f) del Regolamento a Selectra S.p.A. il divieto dell'ulteriore trattamento dei dati estratti attraverso il software Mail Store;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i), del Regolamento di pagare la somma di euro 80.000,00 (ottantamila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

altresì alla medesima Società di pagare la predetta somma di euro 80.000,00 (ottantamila),

secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dell'art. 27 della legge n. 689/1981.

Si ricorda che resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato - di un importo pari alla metà della sanzione irrogata, entro il termine di cui all'art. 10, comma 3, del d. lgs. n. 150 dell'1.9.2011 previsto per la proposizione del ricorso come sotto indicato (art. 166, comma 8, del Codice);

DISPONE

la pubblicazione del presente provvedimento sul sito web del Garante ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/20129, e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

Richiede alla Società di comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto disposto con il presente provvedimento e di fornire comunque riscontro adeguatamente documentato ai sensi dell'art. 157 del Codice, entro il termine di 90 giorni dalla data di notifica del presente provvedimento; l'eventuale mancato riscontro può comportare l'applicazione della sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento.

Ai sensi dell'art. 78 del Regolamento, nonché degli articoli 152 del Codice e 10 del d.lg. n. 150/2011, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo individuato nel medesimo art. 10, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 17 luglio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei