Ordinanza ingiunzione nei confronti di Gaypa s.r.l. - 29 ottobre 2020 [9518890]

[doc. web n. 9518890]

Ordinanza ingiunzione nei confronti di Gaypa s.r.l. - 29 ottobre 2020

Registro dei provvedimenti
n. 214 del 29 ottobre 2020

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il prof. Pasquale Stanzione, presidente, la prof.ssa Ginevra Cerrina Feroni, vicepresidente, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti e il dott. Claudio Filippi, vice 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");

VISTE le "Linee guida per posta elettronica e internet", adottate con provvedimento n. 13 del 1° marzo 2007 (pubblicato nella G.U. 10 marzo 2007, n. 58);

VISTO il reclamo presentato al Garante ai sensi dell'articolo 77 del Regolamento da XX concernente il trattamento di dati personali riferiti all'interessato effettuato da Gaypa s.r.l.;

ESAMINATA la documentazione in atti;

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

RELATORE l'avv. Guido Scorza;

PREMESSO

1. Il reclamo nei confronti della società e l'attività istruttoria.

1.1. Con reclamo del 5 novembre 2018 il Sig. XX (rappresentato e difeso dall'avvocato Anna Zavagnin) ha lamentato presunte violazioni del Regolamento da parte di Gaypa s.r.l. (di seguito, la società), con particolare riferimento al persistente utilizzo dell'account di posta elettronica di tipo individualizzato (XX) che sarebbe rimasto attivo anche dopo l'interruzione del rapporto di lavoro (in data 16.3.2018) ed il cui contenuto sarebbe stato accessibile alla società anche a ritroso nel tempo (fino al 2017). Il reclamante, inoltre, non sarebbe stato informato della possibilità per la società di effettuare tale accesso, ed anzi il presidente della società con lettera del 13 marzo 2018 ha comunicato che la predetta casella aziendale sarebbe stata disattivata dalla data di definitiva cessazione del rapporto di lavoro e non sarebbe più stata "destinataria di messaggi email. Inoltre, trascorsi sessanta giorni dalla data di cui sopra, tutto il contenuto della […] casella di posta verrà eliminato" (v. All. 9, reclamo 5.11.2018). Solo a seguito del deposito di alcune email pervenute sull'account aziendale in un giudizio incardinato dinnanzi all'autorità giudiziaria ordinaria il reclamante avrebbe appreso che la società, invece, non aveva disattivato l'account né aveva cancellato i messaggi ivi memorizzati. Con il reclamo è stato pertanto chiesto al Garante di voler disporre il divieto del trattamento dei dati personali riferiti al

reclamante contenuti nella predetta casella di posta elettronica, con “cancellazione dei propri dati personali e divieto di conservazione dei dati medesimi (inclusa la produzione e l’utilizzabilità degli stessi nel giudizio pendente avanti al Tribunale di Venezia – Sezione specializzata delle Imprese)”.

1.2. La società, in risposta alla richiesta di elementi (del 29.4.2019) formulata dall’Ufficio, con nota del 6.6.2019 ha dichiarato che:

a. a seguito della presentazione delle dimissioni da parte del reclamante, “con missiva del 13.3.2018 [la società] rappresentava […] che trascorsi 60 giorni dalla data di definitiva cessazione del rapporto di lavoro il contenuto della casella postale aziendale […] sarebbe stato eliminato” (v. nota 6.6.2019, p. 3);

b. posto che il rapporto di lavoro con il reclamante cessava, effettivamente, in data 21 marzo 2018, “in ossequio a quanto comunicato, seppure con lieve ritardo […], il giorno 12.6.2018, il […] Data Protection Officer […], si apprestava ad eliminare i contenuti della casella postale del reclamante, accedendo al server aziendale” (v. nota cit., p. 3);

c. “il DPO notava […] la presenza di due email ricevute in data 4.6.2018 provenienti da un fornitore [della società] recanti ad oggetto «richiesta date inizio lavori» [e] comunicava immediatamente la presenza di queste email alla società” (v. nota cit., p. 3);

d. dalla lettura delle email “emergeva […] che [il reclamante], qualificandosi come direttore operativo [di altra società] era in rapporti con un fornitore del suo precedente datore di lavoro” (v. nota cit., p. 3);

e. “ciò ha messo in allarme [la società] che a quel punto ha incaricato il DPO: (i) di sospendere le operazioni finalizzate alla cancellazione della casella di posta […]; (ii) di effettuare una ricerca nella medesima casella […] finalizzata ad individuare acquisizioni fraudolente, utilizzazione indebita o rivelazione di segreti […] appartenenti esclusivamente alla società” (v. nota cit., p. 3);

f. “all’esito della ricerca […] sono emersi una serie di auto-invii […] contenenti allegati di carattere tecnico con informazioni riservate […]” (v. nota cit., p. 4);

g. la società ha successivamente avviato nei confronti del reclamante un procedimento dinnanzi al Tribunale di Venezia (proc. RG 7642/2018) “utilizzando solo 32 delle 75 e-mail totali […] così recuperate” (v. nota cit., p. 4);

h. oltre alle 34 email (2 email del 4.6.2018 e le 32 estratte dall’account del reclamante) “al termine della ricerca sono state estratte altre 41 email [che] non sono state prodotte in giudizio perché informazioni attinenti a clienti [della società] con i quali è stato stipulato un apposito accordo di riservatezza […]. La conservazione di queste email è necessaria affinché [la società] possa in futuro tutelarsi da eventuali controversie attinenti all’utilizzo fraudolento di tali informazioni” (v. nota cit., p. 5);

i. il trattamento è stato effettuato dalla società per finalità di tutela dei propri diritti “in accordo con le lettere f) e g) dell’art. 24 del D. Lgs. 30 giugno 2003, n. 196, o anche secondo il combinato disposto dell’art. 6 (1) lett. f e dell’art. 23 (1) f del Codice” (v. nota cit., p. 6);

j. “ad oggi i contenuti della casella [del reclamante] sono stati completamente eliminati dal server della società, al pari dell’indirizzo aziendale […], per il quale è stato attivato un sistema di risposta automatica che informa chi scrive della disattivazione della casella” (v. nota cit., p. 6); in particolare “la definitiva eliminazione della casella e dei suoi contenuti [è] avvenuta in data 14.12.2018” (v. nota cit., p. 10);

k. “resta inteso che le e-mail estratte in precedenza e sottoposte all’esame del Tribunale di Venezia sono ancora nella disponibilità [della società]” (v. nota cit., p. 12);

l. in relazione all’obbligo di fornire l’informativa all’interessato la società “il 30 marzo 2010 […] redigeva e distribuiva tra i dipendenti un «Documento programmatico sulla sicurezza per il trattamento dei dati personali»”; sempre nel 2010 la società “effettuava una integrazione del regolamento intitolato «Privacy verifiche e correzioni» […] che veniva affisso in bacheca in posizione facilmente visibile ai lavoratori” (v. nota cit., p. 7);

m. in data 1° settembre 2018 la società “ha aggiornato le proprie policy in ambito di protezione dei dati tramite un nuovo regolamento aziendale” (v. nota cit., p. 9 e All. C “Regolamento aziendale”).

1.3. Con nota del 7 ottobre 2019 il reclamante, nel confermare le richieste già avanzate con il reclamo, ha sostenuto, tra l’altro, che:

a. i fatti oggetto di reclamo “si collocano nel giugno 2018 e sono comunque successivi all’entrata in vigore del Regolamento”;

b. la società non ha fornito al reclamante alcuna informativa relativa all’utilizzo della posta elettronica, considerato anche che l’integrazione al regolamento interno denominata “Privacy verifiche e correzioni” è privo di data certa né la società “ha provato di aver nel 2010 effettivamente affisso in bacheca una integrazione informativa completa e dettagliata”;

c. la società ha “mantenuto la casella di posta attiva oltre i 60 giorni e fino al 14.12.18 e detiene tuttora 75 e-mails”;

d. le email estratte dalla società dall’account aziendale del reclamante hanno, in parte, “per oggetto dati appartenenti a terzi” e d’altra parte il reclamante “neppure conosce quali e-mails […] Gaypa abbia illegittimamente acquisito e conservato”.

1.4. Con nota del 22 ottobre 2019 la società, in riscontro ad una richiesta di ulteriori chiarimenti formulata da questo ufficio, ha chiarito che:

a. a rettifica di quanto affermato nel precedente riscontro non è stato designato alcun “Responsabile della protezione dei dati” ai sensi dell’art. 37 del Regolamento;

b.pertanto il dipendente di 7Bridges s.r.l. “erroneamente indicato quale “Data protection officer” è in realtà […] l’amministratore di sistema incaricato dalla società”;

c. la società, in data 7.12.2015, ha stipulato con 7Bridges s.r.l. un “Contratto di manutenzione ed assistenza tecnica” relativo allo svolgimento di servizi di assistenza e manutenzione delle apparecchiature informatiche, con il quale ha proceduto a designare la medesima 7Bridges s.r.l. quale responsabile del trattamento; un dipendente di 7Bridges s.r.l. è stato designato, in particolare, amministratore di sistema con lettera datata 11.1.2016;

d. anche alla luce delle decisioni assunte dall’autorità giudiziaria nel procedimento avviato dalla società nei confronti del reclamante (R.G. 7642/2018 Tribunale di Venezia) si evince che “l’accesso da parte dell’amministratore di sistema sia avvenuto su incarico del titolare del trattamento dei dati, per tutelare un legittimo interesse di Gaypa s.r.l. quale quello di ottenere tutela in sede giudiziaria nei confronti del proprio (ex) dipendente infedele”.

1.5. Il 2 marzo 2020 l’Ufficio ha effettuato, ai sensi dell’art. 166, comma 5, del Codice, la notificazione alla società delle presunte violazioni riscontrate, con riferimento agli artt. art. 5, par. 1, lett. a), 12, 13, 88 del Regolamento e 113 e 114 del Codice. Con nota del 1° aprile 2020 la società, rappresentata e difesa dall’avvocato Vincenzo Palmisano, ha dichiarato che:

a. dopo la ricezione della notifica di violazione la società “ha preso atto delle criticità riscontrate con riferimento al proprio regolamento aziendale e si è immediatamente attivata per porvi rimedio […] nonostante si trovasse ad operare in un contesto […] tuttora complicatissimo a causa dell’esplosione dell’emergenza legata alla diffusione del Covid-19”; in proposito è stato predisposto un nuovo regolamento aziendale “che entrerà in vigore a far data dal 1° maggio 2020 […] già comunicato a tutti i dipendenti via email in data 1° aprile 2020” (v. nota 1.4.2020, p. 3-4 e All. J);

b. il nuovo regolamento aziendale fornisce ai dipendenti indicazioni sulle condizioni d’uso degli account aziendali di posta elettronica e le modalità di conservazione dei dati ivi contenuti; sono altresì individuati “i limitati e specifici casi in cui un accesso è possibile […] solo in virtù di una collaborazione […] tra il titolare del trattamento e l’amministratore di sistema […]” (v. nota cit., p. 4);

c. con specifico riferimento ai trattamenti sugli account aziendali dopo la cessazione del rapporto di lavoro, il regolamento prevede “l’immediata disattivazione dell’account […] dell’ex dipendente (entro tre giorni dall’ultimo giorno lavorativo) e la conservazione del suo contenuto per un periodo di tempo limitato (sei mesi)”, con contestuale individuazione di “una serie limitata di casi in cui tale accesso è possibile” (v. nota cit., p. 4-5);

d. in ogni caso la società dichiara la propria disponibilità “a recepire ulteriori indicazioni che dovessero pervenire dal Garante” (v. nota cit., p. 5);

e. su 52 dipendenti “soltanto 36 […] risultano assegnatari di un account di posta elettronica aziendale nominativo” (v. nota cit., p. 5);

f. nel presente procedimento non si può non tenere in considerazione la condotta del reclamante posto che “tanto nel provvedimento cautelare concesso [alla società] quanto nel provvedimento di rigetto del reclamo” proposto dinnanzi all’autorità giudiziaria competente, il reclamante è “stato ritenuto inequivocabilmente responsabile di una condotta reiterata finalizzata a sottrarre fraudolentemente [alla società] informazioni riservate” (v. nota cit., p. 5);

g. pertanto le attività di “accesso alla casella di posta elettronica dell’ex dipendente, pur integranti violazione della normativa preposta a tutela della privacy del dipendente, non sono state compiute al fine di conseguire benefici finanziari o profitti di alcun tipo, ma […] sono stati unicamente finalizzati a tutelare il proprio patrimonio ed i propri diritti in sede giurisdizionale” (v. nota cit., p. 6);

h. la società chiede all’Autorità, di conseguenza, di tenere in considerazione tali elementi in relazione alla decisione sui provvedimenti da adottare e, in particolare, di non adottare “alcuna sanzione di carattere pecuniario”, fermo restando che “l’eventuale esercizio da parte del Garante del potere di richiedere correttivi […] troverebbe pieno ed immediato riscontro” da parte della società; in subordine la società chiede di tenere in considerazione tutti gli elementi attenuanti già esposti, nonché “la circostanza attenuante «aperta» di cui alla lett. k), par. 2, dell’art. 83 del Regolamento” considerato che la società “[è] stata e [è] tuttora pesantemente penalizzata dalla crisi legata all’epidemia di Covid-19” (v. nota cit., p. 6-7).

2. L’esito dell’istruttoria e del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori.

2.1. All’esito dell’esame delle dichiarazioni rese all’Autorità nel corso del procedimento nonché della documentazione acquisita, risulta che la società, in qualità di titolare, ha effettuato alcune operazioni di trattamento di dati personali riferiti al reclamante che risultano non conformi alla disciplina in materia di protezione dei dati personali, nei termini di seguito descritti.

Si rileva preliminarmente che, conformemente al costante orientamento della Corte europea dei diritti dell’uomo, la protezione della vita privata si estende anche all’ambito lavorativo, considerato che proprio in occasione dello svolgimento di attività lavorative e/o professionali si sviluppano relazioni dove si esplica la personalità del lavoratore (v. artt. 2 e 41, comma 2, Cost). Tenuto anche conto che la linea di confine tra ambito lavorativo/professionale e ambito strettamente privato non sempre può essere tracciata con chiarezza, la Corte ritiene applicabile l’art. 8 della Convenzione europea dei diritti dell’uomo posto a tutela della vita privata senza distinguere tra sfera privata e sfera professionale (v. 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. par. 70-73; 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).]

2.2. Premesso 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”, nel merito è emerso che la società, in data 12 giugno 2018, dopo aver preannunciato al reclamante (con lettera del 13.3.2018, v. precedente punto 1.2., lett. a) che il contenuto della casella aziendale sarebbe stato eliminato decorsi 60 giorni dalla cessazione del rapporto di lavoro, ha effettuato, avvalendosi dell’amministratore di sistema dopo che quest’ultimo aveva segnalato due comunicazioni ritenute anomale, una “ricerca” sulle email contenute nel predetto account e conservate sul server aziendale quantomeno a partire dal 12 aprile 2017, data della email più risalente nel tempo. Delle email così recuperate, 32 sono state utilizzate per avviare un procedimento in sede giurisdizionale, mentre le altre 41 sono tutt’ora conservate dalla società in vista di futuri possibili contenziosi. L’account, secondo quanto dichiarato, è stato “eliminato” in data 14.12.2018, mentre sarebbe ancora attivo un sistema automatico di messaggistica in caso di ricezione di messaggi (v. precedente punto 1.2., lett. j).

Non risulta, in proposito, che il reclamante sia stato previamente informato dalla società che tutte le email in transito sull’account

aziendale fossero conservate sul server aziendale e che la società stessa si riservasse la possibilità di effettuare un controllo sulle stesse. Infatti all'interno del «Documento programmatico sulla sicurezza per il trattamento dei dati personali» del 30 marzo 2010 (v. nota riscontro 6.6.2019, All. A), non vi è alcun riferimento a tale procedura di controllo, e peraltro la società non ha prodotto documentazione dalla quale emerga che tale documento sia stato reso noto ai dipendenti.

Anche con riferimento al documento «Privacy verifiche e correzioni» (v. nota riscontro cit., All. B), adottato – secondo quanto dichiarato nel 2010, non è stato fornito alcun elemento dal quale emerga l'avvenuta adozione di modalità idonee a garantire l'effettiva conoscibilità del testo da parte dei dipendenti interessati. In ogni caso, nel merito di quanto ivi indicato, si osserva da un lato che nel predetto ultimo documento, sezione "Condizioni per l'utilizzo della posta elettronica" si afferma, tra l'altro, che "le condizioni di utilizzo della posta sono documentate in un documento consegnato al momento del rilascio della casella", tuttavia nessun modello di tale documento è stato prodotto in atti dalla società. Inoltre, e ad ogni buon conto, le formulazioni utilizzate non sono idonee a rappresentare con chiarezza agli interessati finalità e modalità della prospettata conservazione delle email nonché le ipotesi nelle quali il datore di lavoro "si riserva di effettuare controlli in conformità alla legge indicando le ragioni legittime – specifiche e non generiche per cui verrebbero effettuati e le relative modalità" (v. "Linee guida per posta elettronica e internet", provv. 1° marzo 2007, n. 13, (G.U. 10.3.2007, n. 58). Infatti, da un lato, nella parte del documento in cui si sottolinea l'importanza di effettuare "regolari operazioni di backup" al fine di "proteggere i dati", si rappresenta che "I data base di posta sono archiviati su di un server protetto ed è possibile accedere alle versioni precedenti dei database che possono contenere anche le email eliminate". D'altro lato si rappresenta che "gli amministratori di sistema possono accedere a qualunque casella di posta elettronica. Gli accessi alla casella di posta verranno fatti esclusivamente per: configurarla, manutenzione, operazioni di inoltro automatico […] e su richiesta della direzione".

La società ha pertanto omesso di informare il reclamante relativamente alla specifica modalità di trattamento in concreto effettuata, in violazione di quanto previsto dagli artt. 12 e 13 del Regolamento, già vigente all'epoca dell'accesso al contenuto dell'account (12.6.2018), in base al quale il titolare è tenuto a fornire all'interessato - prima dell'inizio dei trattamenti - tutte le informazioni relative alle caratteristiche essenziali del trattamento. Nell'ambito del rapporto di lavoro l'obbligo di informare il dipendente è altresì espressione del principio generale di correttezza dei trattamenti (v. art. 5, par. 1, lett. a) del Regolamento).

2.3. E' emerso, altresì, che la sistematica conservazione delle email in entrata e in uscita (sia dei dati esterni che del loro contenuto) sul server aziendale per un termine che non è stato reso noto dall'azienda, ma che è risultato comunque non inferiore ad un anno e due mesi (visto che l'email più risalente prodotta in giudizio è datata 12.4.2017), ed il successivo accesso effettuato dalla società per verificare, attraverso l'effettuazione a posteriori di una indagine interna volta a verificare possibili "acquisizioni fraudolente, utilizzazione indebita o rivelazione di segreti", ha permesso al datore di lavoro di trattare dati personali del dipendente in violazione di quanto prescritto dalla disciplina di settore in materia di controlli a distanza (art. 4, l. 20.5.1970, n. 300).

Ciò ha inoltre consentito alla società di conoscere informazioni relative alla vita privata del lavoratore non rilevanti ai fini della valutazione dell'attitudine professionale dello stesso, considerato che almeno in una delle email raccolte e depositate in giudizio sono presenti documenti riferiti al reclamante non attinenti all'attività lavorativa (v. email n. 16 allegata al riscontro della società del 6.6.2019; v. altresì ricorso ex art. 700 c.p.c. al Tribunale di Venezia, sez. Tribunale delle imprese, depositato da Gaypa s.r.l. il 23.7.2018, n. 15, dove si riferisce che "l'ex lavoratore inviava a sé stesso documenti personali (polizza auto, bollo auto, dati relativi ad utenze gas/luce, etc.)").

Tale trattamento configura pertanto la violazione degli artt. 113 e 114 del Codice (che richiamano gli artt. 4 e 8 della l. 20.5.1970, n. 300 e l'art. 10 del d.lgs.10.9.2003, n. 276, quali condizioni di liceità del trattamento). Tale disciplina lavoristica costituisce 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" richiamate dall'art. 88 del Regolamento.

2.4.1. È emerso, infine, che la società ha adottato un nuovo regolamento aziendale, con decorrenza dal 1° settembre 2018 (v. precedente punto 1.2., lett. m), relativo, tra l'altro, all'uso della posta elettronica aziendale (v. punto 5.7). All'interno di tale regolamento è previsto che: (a) in caso di cessazione del rapporto di lavoro "la documentazione presente nel profilo del singolo utente […] verrà considerata presuntivamente dell'azienda, quale corrispondenza e documentazione lavorativa e non personale"; (b) la casella di posta "viene disattivata al momento della conclusione del rapporto di lavoro […]. Gaypa srl si riserva, tuttavia, di valutare a proprio esclusivo ed insindacabile giudizio la necessità di mantenere attiva in ricezione la casella per un congruo periodo di tempo al fine di garantire la funzionalità aziendale"; (c) "poiché la casella di posta assegnata costituisce strumento di lavoro […] i messaggi ivi contenuti, avendo presuntivamente natura di corrispondenza commerciale, verranno conservati nei server aziendali

per 3 anni"; (d) "sarà comunque consentito al superiore gerarchico dell'utente o, comunque, sentito l'utente, a persona individuata dall'azienda, accedere alla casella di posta elettronica dell'utente per ogni ipotesi in cui si renda necessario".

2.4.1.1. Con riferimento ai trattamenti effettuati sull'account di posta elettronica dopo la cessazione del rapporto di lavoro, la prevista "presunzione" di appartenenza all'azienda di tutta la corrispondenza presente nell'account di posta aziendale, di tipo individualizzato, così come la prevista possibilità di mantenere attiva per un periodo non precisato la predetta casella in ipotesi non definite bensì individuate (anche di volta in volta) all'esito di un giudizio, definito "insindacabile", volto a garantire la "funzionalità aziendale", non sono conformi ai principi di minimizzazione dei dati (art. 5, par. 1, lett. c) del Regolamento) e di limitazione della conservazione (art. 5, par. 1, lett. e) del Regolamento). Ciò anche tenuto conto del fatto che è comunque previsto l'invio di "mail ai mittenti con indicazione della diversa casella di posta elettronica aziendale cui trasmettere i messaggi", misura già idonea a garantire la continuità dei rapporti con l'azienda da parte dei soggetti interessati.

Risulta parimenti in contrasto con i richiamati principi di minimizzazione dei dati (art. 5, par. 1, lett. c) del Regolamento) e di limitazione della conservazione (art. 5, par. 1, lett. e) del Regolamento) la prospettata sistematica conservazione sul server aziendale per un esteso periodo di tempo, pari a tre anni, di tutte le email inviate e ricevute dagli account aziendali (v. provv. 1.2.2018, n. 53, doc. web n. 8159221, spec. punto 3.2.). Così come la prevista possibilità per il superiore gerarchico o qualunque altro dipendente (benché "sentito" l'interessato) di accedere alla casella di posta in relazione ad una indefinita pluralità di scopi.

Inoltre, la possibilità per la società di accedere sia ai dati esterni che al contenuto delle caselle email in costanza del rapporto di lavoro, comporta un trattamento di dati personali illecito in violazione dell'art. 4, l. 20.5.1970, n. 300, richiamato dall'art. 114 del Codice come condizione di liceità del trattamento (esercitando un controllo sull'attività del lavoratore), nonché la possibilità di accedere ad informazioni relative all'interessato non rilevanti, in violazione dell'art. 8, l. 20.5.1970, n. 300 e dell'art. 10 del d.lgs.10.9.2003, n. 276, richiamati dall'art. 113 del Codice come condizione di liceità del trattamento (contenenti il divieto di effettuare indagini o comunque trattare dati che non siano strettamente attinenti alla valutazione dell'attitudine professionale del dipendente). Tale disciplina lavoristica costituisce 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 (e, come misura appropriata e specifica ai sensi del par. 2 del medesimo art. 88, non consente controlli massivi, prolungati e indiscriminati dell'attività del dipendente).

Ciò configura pertanto la violazione del principio di liceità del trattamento (art. 5, par. 1, lett. a) del Regolamento in relazione agli artt. 113 e 114 del Codice) e dell'art. 88 del Regolamento quanto alla disciplina applicabile in materia.

2.4.2. Successivamente alla notifica delle presunte violazioni ai sensi dell'art. 166, comma 5, la società ha adottato un nuovo regolamento aziendale (v. precedente punto 1.5., lett. a.). La nuova sezione relativa all'uso della posta elettronica (punto 5.7), in vigore dal 1° maggio 2020, prevede che "tutti i messaggi in entrata e in uscita in transito sull'account [sono] automaticamente oggetto di salvataggio sul server aziendale. La conservazione di tali dati è limitata [a] dodici […] mesi", premesso che "la casella di posta elettronica assegnata all'utente è uno strumento di lavoro". Se, di regola, l'accesso alla casella è riservato al dipendente assegnatario dell'account, l'amministratore di sistema può "avere accesso agli account previo reset della password prescelta dall'utente assegnatario". E' inoltre precisato che "in via del tutto eccezionale, l'accesso al contenuto dell'account di posta è consentito al titolare del trattamento [per il tramite dell'amministratore di sistema]: nel caso in cui la casella di posta elettronica sia stata utilizzata dal dipendente per la commissione di reati o illeciti di qualsiasi natura"; nonché "nel caso in cui vi sia il fondato sospetto che il dipendente abbia utilizzato la casella di posta elettronica per far fuoriuscire dalla rete aziendale informazioni aziendali, esperienze tecnico-industriali e commerciali, documentazione riservata di qualsiasi genere, sia di proprietà dell'Azienda che di clienti o fornitori dell'Azienda, al fine di acquisirli, utilizzarli o rivelarli a terzi".

Il regolamento prevede altresì che in caso di recesso la casella di posta sarà disattivata entro tre giorni dall'ultimo giorno di lavoro, con contestuale impostazione di un servizio di autoreplay con indicazione di un diverso account aziendale. Inoltre "il contenuto della casella di posta elettronica disattivata verrà mantenuto sul server dell'Azienda per i sei mesi successivi" durante i quali la società potrà accedere al contenuto dell'account in tre casi (contestazione da parte di clienti, fornitori, pubbliche amministrazioni; nel caso in cui la casella "sia stata utilizzata dal dipendente al quale era concessa in uso per la commissione di reati o di illeciti di qualsiasi natura" nonché "nel caso in cui vi sia il fondato sospetto che il dipendente abbia utilizzato la casella di posta elettronica per far fuoriuscire dalla rete aziendale informazioni aziendali, esperienze tecnico-industriali e commerciali, documentazione riservata di qualsiasi genere, sia di proprietà dell'Azienda che di clienti o fornitori dell'Azienda, al fine di acquisirli, utilizzarli o rivelarli a terzi").

2.4.2.1. Anche con riferimento a quanto stabilito dalla società con il nuovo regolamento aziendale la sistematica conservazione per 12 mesi di tutte le email presenti sull'account, in costanza del rapporto di lavoro, in vista di futuri possibili contenziosi che potrebbero interessare la società non è conforme ai principi di minimizzazione dei dati (art. 5, par. 1, lett. c) del Regolamento) e di limitazione della conservazione (art. 5, par. 1, lett. e) del Regolamento). Medesima valutazione riguarda la prospettata conservazione per sei mesi del contenuto della casella affidata all'ex dipendente (che pertanto si aggiungerebbero ai 12 mesi previsti durante il rapporto di lavoro) in relazione ad ipotetiche ipotesi di illeciti (o sospetto di commissione di illeciti) compiuti dal lavoratore. Peraltro si osserva che anche in relazione al prospettato accesso al contenuto dell'account da parte dell'amministratore di sistema, il regolamento non individua alcuna specifica finalità, relativa alla necessità di garantire il corretto funzionamento del servizio di posta, che legittimi l'accesso.

Il Garante ha ribadito che il trattamento di dati personali effettuato per finalità di tutela dei propri diritti in giudizio deve riferirsi a contenziosi in atto o a situazioni precontenziose, non ad astratte e indeterminate ipotesi di possibile difesa o tutela dei diritti, posto che tale estensiva interpretazione avanzata dalla società risulterebbe elusiva delle disposizioni sui criteri di legittimazione del trattamento (v. artt. 6, par. 1, lett. b), c) e f) e 9, par. 2, lett. b) del Regolamento; v., da ultimo, provv. 1° febbraio 2018, n. 53, doc. web n. 8159221).

In relazione alla rappresentata finalità di far fronte ad eventuali contestazioni da parte di clienti, fornitori, pubbliche amministrazioni, si osserva altresì che il Garante ha già ritenuto che la legittima necessità di assicurare la conservazione di documentazione necessaria per l´ordinario svolgimento e la continuità dell´attività aziendale, anche in relazione ai rapporti intrattenuti con soggetti privati e pubblici, nonché in base a specifiche disposizioni dell´ordinamento, è assicurata, in primo luogo, dalla predisposizione di sistemi di gestione documentale con i quali attraverso l´adozione di appropriate misure organizzative e tecnologiche individuare i documenti che nel corso dello svolgimento dell´attività lavorativa devono essere via via archiviati con modalità idonee a garantire le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità prescritte dalla disciplina di settore applicabile. I sistemi di posta elettronica, per loro stessa natura, non consentono di assicurare tali caratteristiche (v. provv. 1° febbraio 2018, n. 53, doc. web n. 8159221).

Inoltre, come già ritenuto con riguardo alla precedente versione del regolamento aziendale, il prospettato accesso sia ai dati esterni che al contenuto della casella email costituisce un trattamento di dati personali illecito in quanto in violazione dell'art. 4, l. 20.5.1970, n. 300, richiamato dall'art. 114 del Codice come condizione di liceità del trattamento (esercitando un controllo sull'attività del lavoratore), nonché in violazione dell'art. 8, l. 20.5.1970, n. 300 e dell'art. 10 del d.lgs.10.9.2003, n. 276, richiamati dall'art. 113 del Codice come condizione di liceità del trattamento (contenenti il divieto di effettuare indagini o comunque trattare dati che non siano strettamente attinenti alla valutazione dell'attitudine professionale del dipendente). Come già esposto in precedenza la citata disciplina lavoristica, costituisce una delle norme del diritto nazionale richiamate dall'art. 88 del Regolamento (e, come misura appropriata e specifica ai sensi del par. 2 del medesimo art. 88, non consente controlli massivi, prolungati e indiscriminati dell'attività del dipendente).
Per i suesposti motivi il trattamento dei dati relativi agli account di posta elettronica aziendali effettuato a partire dal 1° maggio 2020, configura la violazione del principio di liceità del trattamento (art. 5, par. 1, lett. a) del Regolamento in relazione agli artt. 113 e 114 del Codice) e dell'art. 88 del Regolamento quanto alla disciplina applicabile in materia.

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

Per i suesposti motivi, il trattamento dei dati personali riferiti al reclamante effettuato dalla società attraverso la conservazione e l'accesso al contenuto dell'account individualizzato di posta elettronica, nonché i trattamenti relativi alla gestione della posta elettronica dei dipendenti effettuati in base ai regolamenti aziendali adottati, rispettivamente, il 1° settembre 2018 e il 1° maggio 2020, risulta illecito, nei termini su esposti, in relazione agli artt. 5, par. 1, lett. a), c) e e), 12, 13 e 88 del Regolamento e agli artt. 113 e 114 del Codice.

Pertanto, 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 dall'account di posta elettronica aziendale riferito al reclamante, fatta salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, per il tempo necessario a tale scopo, tenuto conto 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";

- si dispone il divieto del trattamento dei dati relativi agli account aziendali dei dipendenti conservati sul server aziendale in base a quanto previsto nei regolamenti aziendali del 1° settembre 2018 e 1° maggio 2020, tenuto conto che ai sensi dell'art. 2-decies del Codice "i dati personali trattati in violazione della disciplina rilevante in materia di trattamento dei dati personali non possono essere utilizzati, salvo quanto previsto dall'art. 160-bis";

- si ingiunge alla società di conformare al Regolamento i propri trattamenti con riferimento a quanto previsto nel regolamento aziendale del 1° maggio 2020 relativamente alla gestione della posta elettronica aziendale;

- si dispone, in aggiunta alla misura correttiva, una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i) Regolamento).

4. Ordinanza ingiunzione.

Ai sensi dell'art. 58, par. 2, lett. i) del Regolamento e dell'art. 166, commi 3 e 7 del Codice, il Garante dispone l'applicazione della sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, lett. a) del Regolamento, mediante adozione di un'ordinanza ingiunzione (art. 18, l. 24.11.1981, n. 689), in relazione ai trattamenti dei dati personali del reclamante e dei dipendenti effettuati dalla società attraverso la memorizzazione sul server aziendale e l'accesso al contenuto degli account di posta elettronica aziendale, di cui è risultata accertata l'illiceità, nei termini su esposti, in relazione agli artt. 5, par. 1, lett. a), c) e e), 12, 13 e 88 del Regolamento e agli artt. 113 e 114 del Codice, all'esito del procedimento di cui all'art. 166, comma 5 svolto in contraddittorio con il titolare del trattamento (v. precedente punto 1.5).

Ritenuto di dover applicare il paragrafo 3 dell'art. 83 del Regolamento laddove 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", considerato che le accertate violazioni dell'art. 5 del Regolamento sono da considerarsi più gravi, in quanto relative alla inosservanza di una pluralità di principi di carattere generale applicabili al trattamento di dati personali, l'importo totale della sanzione è calcolato in modo da non superare il massimo edittale previsto per la predetta violazione. Conseguentemente si applica la sanzione prevista dall'art. 83, par. 5, lett. a), del Regolamento, che fissa il massimo edittale nella somma di 20 milioni di euro ovvero, per le imprese, nel 4% del fatturato mondiale annuo dell'esercizio precedente ove superiore.

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; le violazioni hanno anche riguardato le condizioni di liceità del trattamento (disposizioni più specifiche riguardo ai trattamenti nell'ambito dei rapporti di lavoro) e le disposizioni sull'informativa;

b) con riferimento al carattere doloso o colposo della violazione e al grado di responsabilità del titolare è stata presa in considerazione la negligente 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 complessivamente e attivamente cooperato con l'Autorità nel corso del procedimento;

f) l'assenza di precedenti specifici (relativi alla stessa tipologia di trattamento) 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 2018. Da ultimo si tiene conto della comminatoria edittale disposta, nel regime previgente, per gli illeciti amministrativi corrispondenti e dell'entità delle sanzioni irrogate in casi analoghi.

Alla luce degli elementi sopra indicati e delle valutazioni effettuate, si ritiene, nel caso di specie, di applicare nei confronti di Gaypa s.r.l. la sanzione amministrativa del pagamento di una somma pari ad euro 20.000,00 (ventimila).

In tale quadro si ritiene, altresì, in considerazione della tipologia delle violazioni accertate che hanno riguardato le condizioni di liceità del trattamento e l'obbligo di fornire un'idonea informativa all'interessato, 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 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante.

Si ricorda che, ai sensi dell'articolo 170 del Codice, chiunque, essendovi tenuto, non osserva il presente provvedimento di divieto è punito con la reclusione da tre mesi a due anni; in ogni caso può essere applicata in sede amministrativa la sanzione di cui all'art. 83, par. 5, lett. e) del Regolamento.

TUTTO CIÒ PREMESSO, IL GARANTE

rileva l'illiceità del trattamento effettuato da Gaypa s.r.l. in persona del legale rappresentante pro tempore, con sede legale in Quinto Vicentino, Via Monte Grappa 33, C.F. 00285560249, ai sensi degli artt. 57, par. 1, lett. f) e 83 del Regolamento, nonché dell'art. 166 del Codice, per la violazione degli artt. 5, par. 1, lett. a), c) e e), 12, 13 e 88 del Regolamento nonché degli artt. 113 e 114 del Codice;

IMPONE

ai sensi dell'art. 58, par. 2, lett. f) del Regolamento a Gaypa s.r.l. il divieto dell'ulteriore trattamento dei dati estratti dall'account di posta elettronica aziendale riferito al reclamante, fatta salva la loro conservazione per esclusiva finalità di tutela dei diritti in sede giudiziaria, per il tempo necessario a tale scopo nei limiti di cui all'art. 160-bis del Codice;

IMPONE

ai sensi dell'art. 58, par. 2, lett. f) del Regolamento a Gaypa s.r.l. il divieto dell'ulteriore trattamento dei dati relativi agli account aziendali dei dipendenti conservati sul server aziendale in base a quanto previsto nei regolamenti aziendali del 1° settembre 2018 e 1° maggio 2020;

INGIUNGE

ai sensi dell'art. 58, par. 2, lett. d) Regolamento a Gaypa s.r.l. di conformare al Regolamento i propri trattamenti con riferimento a quanto previsto nel regolamento aziendale del 1° maggio 2020 relativamente alla gestione della posta elettronica aziendale, entro 60 giorni dal ricevimento del presente provvedimento;

ORDINA

ai sensi dell'art. 58, par. 2, lett. i) del Regolamento a Gaypa s.r.l. di pagare la somma di euro 20.000,00 (ventimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

altresì alla medesima Società di pagare la somma di euro 20.000,00 (ventimila), 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, el Regolamento del Garante n. 1/20129, e ritiene che ricorrano i presupposti di cui all'art. 17 del Regolamento n. 1/2019.

Richiede a Gaypa s.r.l. 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, 29 ottobre 2020

IL PRESIDENTE
Stanzione

IL RELATORE
Scorza

IL VICE SEGRETARIO GENERALE
Filippi