Ordinanza ingiunzione nei confronti di Brav s.r.l. - 24 marzo 2022 [9767635]

[doc. web n. 9767635]

Ordinanza ingiunzione nei confronti di Brav s.r.l. - 24 marzo 2022

Registro dei provvedimenti
n. 107 del 24 marzo 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

VISTO il d.lgs. 30 giugno 2003, n. 196, "Codice in materia di protezione dei dati personali", come modificato dal d.lgs. 10 agosto 2018, n. 101, recante disposizioni per l'adeguamento dell'ordinamento nazionale al Regolamento (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 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e in www.gpdp.it, doc. web n. 9107633 (di seguito "Regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni dell'Ufficio 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, in www.gpdp.it, doc. web n. 1098801;

RELATORE il dott. Agostino Ghiglia;

1. Premessa

A seguito di una segnalazione pervenuta nel mese di XX, nonché di notizie stampa, l'Autorità ha appreso che la piattaforma utilizzata dal corpo di Polizia locale del Comune di Genova per la gestione delle contravvenzioni al Codice della Strada, contenente i dati personali dei cittadini destinatari di contravvenzioni, è stata oggetto di un accesso abusivo, da parte di soggetti non autorizzati.
Nel medesimo periodo, inoltre, il citato Comune ha notificato al Garante una violazione di dati personali ai sensi dell'art. 33 del Regolamento, dalla quale emerge che l'accesso abusivo sarebbe stato cagionato "dall'incauto comportamento di alcuni agenti, che violando le disposizioni di servizio, non avrebbero modificato la password di primo accesso e divulgato l'URL di accesso".

2. Attività istruttoria

In relazione al caso è stata avviata un'istruttoria, nel corso della quale è emerso che il Comune di Genova– titolare del trattamento – ha stipulato, in data XX, un contratto per la fornitura delle licenze del software "Scat" con Brav s.r.l. (di seguito, la società), provvedendo a regolare i rapporti con la stessa, ai sensi dell'art. 28 del Regolamento, con provvedimento del Sindaco del XX.

In risposta a una richiesta di informazioni dell'Autorità (nota prot. n. XX del XX) il Comune di Genova, con nota del XX (prot. n. XX), ha fornito elementi istruttori chiarendo, in primo luogo, che l'accesso abusivo al portale ScatWeb deriva dalla divulgazione, da parte del personale interno, delle credenziali di accesso (rimaste invariate rispetto a quelle assegnate per effettuare il primo accesso al portale).

In particolare, il Comune ha rappresentato che "all'epoca dei fatti, le policy relative alle credenziali di accesso erano le seguenti: al primo accesso era consentito all'operatore di Polizia Locale entrare nella piattaforma ScatWeb inserendo, sia come username sia come password, il proprio numero di matricola (di distintivo), composto da quattro cifre. Effettuato il primo accesso l'operatore aveva l'obbligo di modificare la password di accesso con una nuova composta da almeno quattro caratteri, come ribadito nuovamente agli operatori con ultimo ordine di servizio in materia n. XX del XX".

Nel riscontro alla richiesta di informazioni il Comune ha allegato, tra l'altro, una nota del XX, ricevuta dalla società, dalla quale si evince, sul punto, che "con specifico riferimento alle modalità di accesso ai profili utente, l'adozione di credenziali semplificate (prima password uguale alla matricola dell'utente-agente di Polizia Municipale, riservata in ogni caso ai soli agenti con profilo "ACCERTATORE") costituiva una specifica richiesta formulata, nel corso dell'erogazione dei corsi di formazione e di successive conversazioni telefoniche, da parte dei responsabili della formazione della Polizia Locale (quindi, del Titolare stesso) al fine di semplificare la distribuzione delle credenziali stesse verso gli operatori utenti" e che "nel corso dei rapporti intercorsi sino ad oggi, sia stata proprio Brav ad evidenziare ai referenti operativi del Titolare con cui interagiva per la gestione del medesimo portale, l'opportunità di attenersi alle buone prassi vigenti in materia ai fini della impostazione delle password […e ad aver] fornito al Titolare del trattamento specifiche istruzioni per il successivo cambio password che ogni operatore poteva effettuare in autonomia".

È emerso, altresì, che la società "in data XX […] sollecitava, tramite e-mail inviata ai responsabili della Polizia Locale, l'adozione ed attivazione da parte degli stessi di policy più restrittive sull'accesso ai vari profili utente, in particolare facendo espresso riferimento all'opportunità di adottare criteri di generazione delle password più complessi ("8 caratteri di cui 1 numerico, 1 alfanumerico, 1 speciale"), posto che il portale ScatWeb consente tale possibilità al Titolare ed ai suoi operatori, in conformità alle indicazioni dell'AGID", senza ricevere riscontro.

Sul punto, tuttavia, il Comune, con la citata nota del XX, ha rappresentato quanto segue:

- "la società gestrice del sistema ScatWeb avrebbe dovuto imporre un obbligo informatico di cambio password al primo accesso, con le caratteristiche corrispondenti agli obblighi di sicurezza rientranti nelle misure minime di sicurezza di cui all'art. 32 GDPR. La Società BRAV, si era assunta contrattualmente l'onere di porre particolare attenzione nella gestione delle credenziali di accesso basandosi sui principi di accountabilty e della privacy by design. Il mancato rispetto di questo obbligo, costituisce quindi un inadempimento contrattuale" e la società "sostiene di aver ricevuto da parte dei responsabili della formazione della Polizia Locale, sia durante la formazione sia nei successivi contatti telefonici con i medesimi, la richiesta di adottare credenziali semplificate (prima password uguale alla matricola dell'utente-agente, riservata ai soli agenti con profilo "ACCERTATORE") allo scopo di facilitare la distribuzione delle credenziali stesse verso gli operatori utenti";

- "La Brav sostiene inoltre di aver evidenziato al Titolare del trattamento (più precisamente ai referenti operativi della gestione del portale ScatWeb) l'opportunità di attenersi alle buone prassi di cambio password che ogni operatore poteva effettuare in autonomia. A riprova, dichiara di aver inviato, in data XX, un'e-mail ai responsabili della Polizia Locale, attraverso il proprio DPO, nella quale sollecitava l'adozione e l'attivazione di policy più restrittive sull'accesso ai vari profili utente ed evidenziava l'opportunità di adottare criteri di generazione delle password più complessi ("8 caratteri di cui 1 numerico, 1 alfanumerico, 1 speciale") in conformità alle indicazioni dell'AGID. La società dichiara di non aver ricevuto riscontro all'e-mail di cui sopra, nonostante il sollecito del proprio DPO";

- “Secondo le conclusioni di Brav si evince chiaramente che, alla data dell’evento, i referenti operativi della gestione del portale ScatWeb erano perfettamente consapevoli della tipologia e del livello di complessità delle credenziali di accesso utilizzate dai propri operatori-utenti e che il Titolare del trattamento era stato opportunamente avvisato dalla stessa società riguardo all’opportunità di adottare credenziali di accesso più complesse di quelle che lo stesso Titolare aveva in concreto richiesto di implementare (chiaramente in deroga ad ogni indicazione contrattuale). Al contrario, si evidenzia che negli Enti Locali i poteri di gestione dei contratti spettano – in via esclusiva - ai dirigenti, e che pertanto una disposizione contrattuale può subire modifiche solo a fronte della disposizione scritta del Dirigente competente. E’ quindi di tutta evidenza che la richiesta verbale di un soggetto, sia pur appartenente all’organizzazione del Titolare, ma non dotato di poteri di rappresentanza, non è assolutamente idonea a modificare una caratteristica essenziale della prestazione, specialmente nella misura in cui tale richiesta si pone in palese contrasto con i principi cardine dell’accountability e della privacy by design previsti dal Regolamento Europeo”.

In sede di istruttoria è emerso, inoltre, che la piattaforma in esame era disponibile anche su protocollo http.

Sul punto, secondo quanto asserito dal Comune di Genova nella nota del XX citata, la società avrebbe dichiarato “di avere effettivamente adottato tale protocollo ma lasciando disponibile ed utilizzabile il protocollo non sicuro “http”, di fatto utilizzato dall’utenza che certamente non poteva avere nel suo complesso le necessarie cognizioni tecniche per prediligere il protocollo sicuro. Solo successivamente alla segnalazione via e-mail da parte delle strutture tecniche del Titolare del trattamento, segnalazione avvenuta il giorno XX, la società Brav si è adoperata per effettuare automaticamente il cosiddetto “Redirect” da protocollo “http” ad “https” per tutte le connessioni in ingresso, rendendo di fatto impossibile utilizzare il protocollo non sicuro”.

In merito, con la nota del XX, la società ha dichiarato che “il protocollo https è sempre stato attivo con regolare certificato valido e quindi perfettamente funzionante e BRAV ha fornito al Titolare apposita indicazione per accedere alla piattaforma attraverso tale protocollo” e che “ad oggi, la scrivente società [.. ha] già adottato tutti gli adeguamenti tecnici volti a correggere le criticità da voi accertate e rilevate […] e, in particolare: - la modifica dell’url di accesso al portale ScatWeb; - il reset di tutte le password di accesso; - l’impostazione dell’obbligo di cambio password al primo accesso con password di complessità elevata. - reindirizzamento automatico delle chiamate http su protocollo https”.

In una successiva risposta a una richiesta di informazioni dell’Autorità (prot. n. XX del XX), il Comune di Genova ha fornito ulteriori elementi istruttori (nota del XX), allegando una nota del XX di codesta società, dalla quale si evince che «con riferimento al tema della mancata trasmissione dei “log di sistema” si premette che Brav mantiene attivo un presidio di tracciatura dei “log di sistema” in relazione a tutti i sistemi in cui svolge le proprie attività, incluso il sistema ScatWeb, riconoscendo in tale presidio una forma elevata di sicurezza cibernetica. Si trasmette in allegato file contenete i “log di sistema” registrati dal server. Tuttavia, con specifico riferimento alla tracciatura degli indirizzi IP degli accessi al sistema ScatWeb, che vengono registrati dal webserver (“log di IIS”), qualche settimana prima del verificarsi dell’episodio di data breach, la scrivente Brav ha ricevuto dei messaggi di allerta dal proprio sistema di monitoraggio dei server […] , che evidenziavano il superamento di specifiche soglie critiche con conseguente rischio di saturazione del disco principale. Conseguentemente, l’intervento tecnico ha richiesto l’interruzione temporanea e cautelativa di ogni fonte di ulteriore scrittura del disco principale, ivi inclusa la tracciatura dei “log di IIS”, al fine di evitare la saturazione del disco e conseguenti gravi danni, e ciò sino al completamento dell’intervento di espansione del disco. Avuta conferma dal tecnico incaricato del completamento dell’intervento sopra menzionato, il sistema di tracciatura dei “log di IIS” è stato riattivato a decorrere dalla data del XX. In ragione di quanto sopra, risulta confermato che: - a causa dell’intervento tecnico sopra descritto, non risulta disponibile a Brav un report di tracciatura degli indirizzi IP per il periodo richiesto intercorrente dal XX al XX».

Pertanto, con nota del XX (prot. n. XX), l’Ufficio, sulla base degli elementi acquisiti, ha notificato alla società, 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 la società a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentita dall’Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24/11/1981).

Con la nota sopra menzionata, l'Ufficio ha rilevato, in primo luogo, che alcuni soggetti non autorizzati hanno avuto la possibilità di prendere visione di dati personali di alcuni interessati accedendo alla piattaforma utilizzata dalla Polizia Locale del Comune di Genova per la gestione delle contravvenzioni. Inoltre, è emerso che il servizio in questione era disponibile anche su protocollo http, ossia tramite un protocollo di rete che non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato. Risulta altresì accertato che, a causa di un intervento tecnico volto a evitare la saturazione del disco, la società non disponeva dei log del server, contenenti, fra l'altro, gli indirizzi IP degli accessi al sistema ScatWeb, del periodo in cui è avvenuta la violazione dei dati personali in esame (XX - XX), in violazione degli artt. 5, par. 1 lett. f) e 32 del Regolamento.

Con nota del XX, la società ha presentato le memorie difensive, dichiarando di essersi "immediatamente impegnata per il miglioramento dei servizi offerti adottando le seguenti misure: - Brav ha adottato procedure rigorose per il controllo dei propri sistemi; in particolare ha nominato due amministratori di sistema che con cadenza settimanale verificano il buon funzionamento dei sistemi e ne riferiscono in un report di "controlli periodici" - A XX Brav ha trasferito tutti i servizi nel Private Cloud di ARUBA (cloud qualificato AGID) e da allora ogni 6 mesi viene svolto un Vulnerability assessment dell'intera infrastruttura. - Nel mese di XX Brav ha conseguito la certificazione ISO27001, incluse le linee guida ISO/lEC 27017, ISO/IEC 27018".

Con la successiva nota del 1XX la società ha altresì dichiarato "le mancanze che sono state attribuite alla nostra azienda relative a - logs di IIS disattivati - protocollo HTTP attivo derivano da un errore umano e non rientrano assolutamente nella prassi. Normalmente infatti - i logs di IIS sono attivi - si applica il redirect automatico di qualunque chiamata HTTP in HTTPS. Lo dimostra il fatto che le contromisure sono state applicate in tempi rapidissimi, in quanto attive abitualmente. Per evitare futuri errori di questa natura, si è intrapreso fin da subito un processo di miglioramento interno che ha portato la nostra azienda a conseguire la certificazione ISO 27001 con l'ulteriore utilizzo delle line guida XX e XX in data XX, inoltre è stata ottenuta la qualificazione AgID ed ora i servizi di BRAV sono disponibili sull'omonimo marketplace. Con la suddetta certificazione BRAV ha adottato procedure come: - Sorveglianza settimanale dello stato dei sistemi e istituzione di apposita documentazione - Istituzione di un security TEAM (Admin di sistema e D.P.O.)".

Da ultimo, per completezza, giova rappresentare che, in risposta ad una ulteriore richiesta di informazioni dell'Autorità (prot. XX del XX) con la nota del XX (prot. XX) il Comune di Genova ha rappresentato:

> "I dipendenti della Direzione Corpo di Polizia Locale trattano i dati personali nel rispetto delle misure di sicurezza previste e delle istruzioni impartite dal Comandante. La Direzione ha formalizzato con la Circolare interna […] le modalità di trattamento dei dati personali per gli "incaricati del trattamento";
>
> "per il corretto utilizzo dell'applicativo di gestione del sistema sanzionatorio (Scat) la Direzione ha provveduto, prima della sua messa in esercizio, a formare il personale attraverso appositi corsi in presenza, fornendo elementi tecnici sull'utilizzo del programma e sensibilizzando il personale sul corretto trattamento dei dati personali raccolti";
>
> "nel Piano di formazione del Comune di Genova, triennio 2021–2023, […] è previsto un Programma di formazione continua in materia di protezione dei dati personali a carattere trasversale per tutti i dipendenti, per esempio, su temi quali le misure di sicurezza ICT, i principi del GDPR, la protezione dei dati personali nel contesto pubblico, etc. unitamente ad altri aspetti rilevanti, come ad es. la transizione digitale";
>
> "l'Ente sta proseguendo nella revisione delle procedure interne in materia di protezione dei dati personali, attraverso un approccio più sostanziale e meno formale rispetto agli adempimenti del Codice privacy. A tale riguardo l'Ente si è dotato di un Regolamento in materia di protezione dei dati personali e privacy, […] allo scopo di rendere la struttura organizzativa più aderente ai principi del Regolamento (UE) 2016/679 operando, tra gli altri, una qualificazione del ruolo dei dirigenti che effettuano il trattamento in relazione alle banche dati degli ambiti di competenza, in un'ottica di forte legame tra gestione delle risorse umane e finanziarie e gestione del dato personale";
>
> "a dimostrazione dell'attenzione dell'Ente verso la tutela dei dati personali è da considerare che già nel XX, e quindi anteriormente al data breach, il titolare del trattamento con nota della Direzione del Personale […] aveva reso obbligatoria la corretta gestione delle password, sensibilizzando sul fatto un

loro utilizzo inappropriato "aumenta il rischio di accessi non autorizzati, che possono innescare problemi o minacce alla sicurezza del trattamento dei dati dell'Ente";

"contravvenendo a un preciso ordine di servizio n. […] in occasione del data breach, sono state disattese tutte le misure di sicurezza imposte dall'Ente";

"con riguardo alle misure tecniche interne assunte, anche al fine di sensibilizzare il personale sul rispetto della normativa in materia di protezione dei dati personali ed evitare il ripetersi di violazioni analoghe in futuro, si rappresenta che al momento della conoscenza della criticità in data XX, il Reparto Contravvenzioni ha prontamente provveduto a contattare la società BRAV affinché, nella sua qualità di gestore del sistema Scat, bloccasse tutti gli accessi ove non era mai avvenuto il cambio password, nonché a verificare successivamente le criticità. Dalla data del XX [… la società] ha aumentato il livello di sicurezza della password, imponendo al primo accesso l'obbligo informatico di cambio password con una chiave di accesso di complessità elevata rispetto alla precedente (numero di matricola), di conseguenza, se non viene sostituita la password non viene consentito l'accesso, inoltre, la password deve essere obbligatoriamente cambiata ogni tre mesi e ha le seguenti caratteristiche: estensione compresa tra 8 e 12 caratteri, almeno una maiuscola, almeno una minuscola, almeno un numero, almeno un carattere speciale non alfanumerico. Con l'imposizione della modifica della password dopo il primo acceso e con la formazione continua sono osservabili comportamenti orientati verso una maggiore prudenza sulle attività di trattamento, in ragione anche di un aumentato senso di consapevolezza sui rischi che comporta il trattamento dei dati personali";

"l'Ente è in procinto di assumere nuove linee guida sul corretto utilizzo degli strumenti informatici in dotazione ai dipendenti (es. pc portatili, tablet, cellulari, smart phone)";

"l'Ente si è, inoltre, attivato per un più intenso controllo sull'operato del fornitore. In particolare, è stato preteso lo svolgimento semestrale di un vulnerability assessment dell'intera infrastruttura, che è stato eseguito durante il mese di XX […]. E' stato eseguito inoltre un penetration test sul server che ospita la procedura".

3. Esito dell'attività istruttoria

In base alla disciplina in materia di protezione dei dati personali i soggetti pubblici possono trattare i dati solo se necessario "per adempiere un obbligo legale al quale è soggetto il titolare del trattamento" 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). In tale quadro, la gestione delle violazioni amministrative e delle violazioni al Codice della Strada rientra tra le attività istituzionali affidate agli enti locali.

Come emerso nel corso dell'istruttoria, il trattamento dei dati in esame è svolto dalla società per conto del Comune di Genova. Ai sensi dell'art. 28 del Regolamento, infatti, il titolare può affidare un trattamento anche a terzi soggetti che presentino garanzie sufficienti sulla messa in atto di misure tecniche e organizzative idonee a garantire che il trattamento sia conforme alla disciplina in materia di protezione dei dati personali ("responsabili del trattamento").

Pur in presenza di una condizione di liceità, ad ogni modo, il trattamento dei dati personali deve avvenire nel rispetto dei principi in materia di protezione dei dati, fra i quali quello di "integrità e riservatezza" in base al quale i dati devono essere "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali" (art. 5, par. 1, lett. e f) del Regolamento).

L'art. 32 del Regolamento pone in capo sia al titolare che al responsabile -tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio- l'adozione di misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso "una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento".

Come già precedentemente chiarito dal Garante, taluni obblighi sono posti direttamente anche a carico dello stesso responsabile il quale, in base anche alle competenze tecniche specifiche, deve collaborare, anche manifestando un'autonomia propositiva, nell'adozione di misure adeguate e nella verifica sistematica dell'efficacia delle stesse, soprattutto nel caso in cui fornisca servizi a una pluralità di titolari del trattamento che coinvolgono un numero elevato di interessati, come nel caso in esame (cfr. provvedimenti n. 48 dell'11 febbraio 2021, doc. web n. 9562831 e n. 293 del 22 luglio 2021, doc. web. n. 9698597).

La società, proprio in ragione della sua esperienza nel settore, era tenuta a verificare costantemente l'efficacia delle misure poste a presidio della piattaforma fornita alla Polizia Locale del Comune di Genova per la gestione delle contravvenzioni, così come chiaramente anche disciplinato nel provvedimento sindacale di nomina, quale responsabile del trattamento, del XX.

Risulta invece accertato che alcuni soggetti non autorizzati hanno avuto la possibilità di accedere alla citata piattaforma. Pur essendo, in sintesi, emerso che tale accesso è avvenuto a causa di una fuoriuscita di informazioni riservate (credenziali) da parte di personale interno del corpo di polizia locale del Comune di Genova, la società avrebbe comunque dovuto adottare misure tecniche e organizzative volte ad assicurare che le password dei soggetti autorizzati rispettassero criteri di qualità e fossero obbligatoriamente modificate al primo utilizzo.

Inoltre, è emerso che il servizio in questione era disponibile anche su protocollo http, ossia tramite un protocollo di rete che non garantisce una comunicazione sicura sia in termini di riservatezza e integrità dei dati scambiati che di autenticità del sito web visualizzato. Risulta altresì accertato che, a causa di un errore umano, la società non disponeva dei log del server contenenti fra l'altro gli indirizzi IP degli accessi al sistema ScatWeb, del periodo in cui è avvenuta la violazione dei dati personali in esame (XX - XX).

Pertanto, risulta accertata la mancata adozione, da parte della società, di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, in violazione degli artt. 5 par. 1 lett. f), e 32 del Regolamento.

Per completezza si rappresenta che, in base agli elementi raccolti, non si ravvisano i presupposti per adottare un provvedimento prescrittivo o inibitorio del Collegio nei confronti del Comune di Genova (v. art. 11 del Regolamento n. 1/2019 del 4 aprile 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).

Ciò in quanto si è tenuto conto che nell'atto di nomina a responsabile del trattamento ai sensi dell'art. 28 del Regolamento, il Comune di Genova ha esplicitamente previsto, tra l'altro, l'obbligo, per la società, in ragione della sua esperienza tecnica nel settore, di mettere in atto misure tecniche e organizzative adeguate a garantire un livello di sicurezza adeguato al rischio inclusa una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche ed organizzative al fine di garantire la sicurezza del trattamento.

Si è preso atto, infine, che il Comune di Genova si è attivato, oltre che per ripristinare le misure di sicurezza adeguate ai rischi presentati dal trattamento, anche per garantire una sensibilizzazione del personale interno con linee guida, circolari interne, e una formazione permanente in materia di protezione dei dati personali.

4. Conclusioni

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

Dalle verifiche compiute sulla base degli elementi acquisiti, anche attraverso la documentazione inviata, nonché dalle successive valutazioni, è stata accertata la non conformità dei trattamenti svolti dalla società per conto e nell'interesse del Comune di Genova aventi a oggetto la fornitura del portale utilizzato dal corpo di Polizia locale per la gestione delle contravvenzioni.

La violazione dei dati personali, oggetto dell'istruttoria, è avvenuta nella piena vigenza delle disposizioni del Regolamento e del Codice, come modificato dal d.lg.n.101/2018, e dunque, al fine della determinazione del quadro normativo applicabile sotto il profilo temporale (art. 1, comma 2, della l. 24 novembre 1981, n. 689), queste costituiscono le disposizioni vigenti al momento della predetta violazione.

Si confermano pertanto le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato dalla società in quanto esso è avvenuto in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza permanente e adeguato al rischio presentato dal trattamento, in violazione degli artt. 5 par. 1 lett. f), e 32 del Regolamento.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa ai sensi degli artt. 58, par. 2, lett. i), e 83, parr. 4 e 5, del Regolamento medesimo, come richiamato anche dall'art. 166, comma 2, del Codice.

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).

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

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie la violazione delle disposizioni citate è soggetta all'applicazione della 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 dei dati personali raccolti attraverso il portale utilizzato dal corpo di Polizia locale del Comune di Genova per la gestione delle contravvenzioni, a partire verosimilmente dal mese di XX (periodo in cui è iniziata la collaborazione con il Comune di Genova), e fino al XX, è avvenuto in assenza di misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento.

Tale violazione è stata portata a conoscenza dall'Autorità mediante una segnalazione e dalla notifica della violazione dei dati personali ai sensi dell'art. 33 del Regolamento.

Di contro è stato considerato che non risultano pervenuti altri reclami o segnalazioni che possano indurre a pensare che la predetta violazione possa aver coinvolto un numero rilevante di interessati. Da quanto emerso, infatti dall'istruttoria (nota del Comune di Genova del XX), "in merito al data breach in questione si può desumere che siano stati effettuati accessi solo a scopo dimostrativo da parte dello stesso giornalista, senza la volontà né la necessità di acquisire i dati inseriti nel sistema. Infatti, l'accesso effettuato il giorno XX con la matricola […] richiamata nell'articolo e dunque presumibilmente utilizzata dal giornalista), parrebbe aver consultato solamente i dati del veicolo […] di proprietà dello stesso giornalista […] Si può affermare con ragionevole sicurezza che non siano avvenuti altri accessi da parte dei lettori dell'articolo, in quanto nel giorno di pubblicazione dello stesso (XX) i profili erano già stati disabilitati in data XX per motivi precauzionali (come indicato nella lettera h della presente nota) a seguito della segnalazione sopra richiamata".

Si è tenuto conto, altresì, che la società si è attivata immediatamente per porre rimedio alla violazione e attenuarne i possibili effetti negativi, collaborando con il titolare del trattamento.

Si evidenzia, in ogni caso, il comportamento non doloso della violazione.

Non risultano, infine, precedenti violazioni del Regolamento commesse dalla società.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di dover determinare ai sensi dell'art. 83, par. 2 e 3, del Regolamento l'ammontare della sanzione pecuniaria, prevista dall'art. 83, par. 5, lett. a) del Regolamento, nella misura di euro 10.000 (diecimila) per la violazione degli artt. 5, par. 1, lett. f) e 32 del Regolamento quale sanzione amministrativa pecuniaria ritenuta effettiva, proporzionata e dissuasiva sensi dell'art. 83, par. 1, del medesimo Regolamento.

Tenuto conto della mancata adozione di misure tecniche di sicurezza adeguate, si ritiene che debba applicarsi la sanzione accessoria della pubblicazione sul sito web del Garante del presente provvedimento, prevista dall'art. 166, comma 7 del Codice e art. 16 del Regolamento del Garante n. 1/2019.

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

TUTTO CIÒ PREMESSO IL GARANTE

dichiara illecita la condotta tenuta da Brav s.r.l., per la violazione degli artt. 5, par. 1, lett. f) e 32 del Regolamento, nei termini di cui in motivazione,

ORDINA

a Brav s.r.l., in persona del legale rappresentante pro-tempore, con sede legale in Vignola (MO), Via del Portello n. 4/B, 41058, - C.F. 02818030369 - di pagare la somma di euro 10.000 (diecimila) a titolo di sanzione amministrativa pecuniaria per le violazioni di cui in motivazione; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

a Brav s.r.l., di pagare la somma di euro 10.000 (diecimila), 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;

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. 1/2019;

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

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

Roma, 24 marzo 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei