Ordinanza ingiunzione nei confronti di Azienda socio sanitaria territoriale Nord di Milano - 27 gennaio 2022 [9746448]

[doc. web n. 9746448]

Ordinanza ingiunzione nei confronti di Azienda socio sanitaria territoriale Nord di Milano - 27 gennaio 2022

Registro dei provvedimenti
n. 34 del 27 gennaio 2022

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

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

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

VISTA la documentazione in atti;

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

RELATORE la prof.ssa Ginevra Cerrina Feroni;

PREMESSO

1. L'attività istruttoria.

È pervenuto al Garante un reclamo in cui un interessato ha rappresentato che nel mese di marzo 2021, accedendo al sito Internet dell'Azienda socio sanitaria territoriale (di seguito ASST) Nord di Milano per prenotare una prestazione sanitaria (tampone per la rilevazione del virus Sars Cov 2), ha constatato che il servizio di prenotazione era effettuato su un protocollo di rete "http" (hypertext transfer protocol) e che, rimuovendo l'estensione "Prenotazione.php" dall'indirizzo del sito Internet della predetta Azienda, era possibile accedere alle informazioni in chiaro relative ad alcuni assistiti dell'ASST che avevano aderito alla campagna vaccinale influenzale 2020/2021 ed in particolare ai seguenti dati: nome, cognome, codice fiscale, recapiti telefonici, luogo di prenotazione e di somministrazione del vaccino antinfluenzale.

A seguito di quanto segnalato, l'Ufficio ha constatato l'assenza nel predetto sito Internet dei file indicati dal reclamante, nonché l'irraggiungibilità delle pagine web indicate dallo stesso (ad eccezione di quella relativa alla prenotazione dei tamponi per la ricerca del SARS-CoV-2) e ha appurato che per il predetto sito è stato utilizzato il protocollo di rete "http" e che sul server che ospita lo stesso veniva utilizzato un software di base non aggiornato con caratteristiche tali da poter compromettere la riservatezza e l'integrità dei dati ivi trattati.

In relazione a quanto rilevato, l'Ufficio ha richiesto informazioni all'ASST nord di Milano (note del 7.4.2021, prot. n. 18256 e del 7.6.2021, prot. n. 30975), la quale ha fornito elementi di riscontro con le note del 23 aprile 2021 (prot. n. 12788), del 22.6.2021 (prot. n.18660), del 28.6.2021 (prot. n. 18977) e dell'8 luglio 2021 (prot. n. 19998) in cui è stato, in particolar modo, rappresentato che:

> "È doveroso per noi sottolineare in primis il contesto (art.32, C.I del GDPR) nel quale è avvenuto il trattamento dei dati da parte della ASST Nord Milano e si è svolto l'evento oggetto di segnalazione, ossia un periodo emergenziale che, da più di un anno a questa parte, sta mettendo a dura prova sia la tenuta del sistema sanitario (ospedaliero e territoriale) nel suo complesso";
>
> "Il sito è stato sviluppato con "phpMyAdmin 2.10.3" ed è stato realizzato in tre giorni lavorativi, per far fonte alle emergenti necessità aziendali in merito alla prenotazione delle sedute di vaccino antinfluenzale, sostituendo una gestione via email troppo onerosa" "successivamente è stata sviluppata anche la sezione relativa alla prenotazione dei Tamponi per la ricerca del Covid-19 in regime di solvenza";
>
> "Sia per i Tamponi che per le vaccinazioni sono stati raccolti nome, cognome, CF e numero di telefono, associati all'orario ed alla sede in cui si sarebbe svolta la prestazione. Tali dati rappresentano il "set" minimo per identificare correttamente una persona e per gestire" ed "eventuali comunicazioni di spostamento dell'appuntamento generate dall'Azienda erogatrice";
>
> "Il Responsabile SIA ha precisato che, proprio essendo ben consci della vetustà dei sistemi operativi adottati — gli unici comunque in grado di rispondere in quel momento alle urgenti esigenze di interesse pubblico connesse alla gestione di gravi minacce per la salute, anche a carattere transfrontaliero - sono stati successivamente pianificati l'installazione ed il test della nuova piattaforma software, basata su "phpMyAdmin 7.3.10";
>
> "I test per la migrazione del software, che hanno portato anche a tutti i necessari aggiornamenti del codice dovuti alla nuova piattaforma di sviluppo, si sono conclusi giovedì 18.3.2021";
>
> "È stato deliberatamente scelto di non migrare il sistema di venerdì, per evitare di lasciare incustodito per tutto un weekend un sistema appena migrato e che avrebbe potuto presentare "difetti di gioventù" (bug non trovati nei cicli di test)";

“Alle ore 14.00 di lunedì 22 marzo 2021, la migrazione ha avuto atto e sono stati risolti tutti i problemi evidenziati nella mail del Sig. XX delle ore 01.02 dello stesso giorno. Appare quindi improbabile che lo stesso, dopo le 48 ore successive all'invio della email, abbia potuto accedere ai dati di cui dice di essere entrato in possesso, cosa invece purtroppo possibile fino alle ore 14.00 del 22.3.2021”;

“E' inoltre in fase di scrittura una componente di programma che storicizzi su un sistema non esposto al pubblico le prenotazioni relative ad un tempo passato al fine di minimizzare l'impatto di una nuova eventuale intrusione”;

“Ai sensi dell'art. 34, comma 3, lett. b) del Regolamento (UE) 2016/679, non è richiesta la comunicazione agli interessati (le "1782 righe (non tutte valide) di cittadini della zona di ASST che hanno aderito alla campagna vaccinale influenzale" di cui parla il Sig. XX nella comunicazione al Garante) in quanto il Titolare ha successivamente adottato misure atte a scongiurare il sopraggiungere di un rischio elevato per i diritti e le libertà degli interessati stessi”;

“quando la Vs. Spettabile Autorità in data 7 aprile u.s. ci ha riportato la dichiarazione con la quale il reclamante sosteneva invece di aver avuto accesso ai dati dopo 48 ore (dall'una di notte del 22 marzo), il Responsabile SIA ha giustamente evidenziato che non era possibile che si fosse verificata tale violazione, perché dopo 48 ore quel database non era già più accessibile, in quanto rimosso dal sito unitamente all'avvio del nuovo software (che non conteneva più il database in parola) quindi dalle ore 14.00 del 22 marzo; la stessa Autorità garante, collegandosi da remoto, infatti non ha trovato traccia dei dati in argomento; non essendoci evidenza di una violazione, non c'erano i presupposti per procedere con le notifiche al Garante e agli interessati”;

“Dopo il citato riscontro all'Autorità Garante in data 23 aprile, gli Uffici interessati hanno approfondito due aspetti: - se ci fossero o meno i presupposti per una azione legale nei confronti del segnalante per il reato di cui all'art.615 ter del Codice Penale ("Accesso abusivo a un sistema informatico o telematico protetto da misure di sicurezza"); da considerare anche che il Signor XX ha usato nella XX; - le ragioni per le quali il reclamante poteva aver dichiarato di aver visionato i dati - per fortuna, non particolari"- di circa 1772 persone dopo 48 ore, quando ciò non era oggettivamente possibile”;

“Visto quanto sopra, e a fronte peraltro della richiesta di ulteriori chiarimenti dell'Autorità in data 7 giugno u.s., è stata in effetti svolta una seconda istruttoria sull'accesso ai dati, che ha permesso al Responsabile SIA in data 15 giugno di comunicare che alle ore 3.00 circa del 22 marzo c'era stato un probabile secondo accesso alla banca dati (i dettagli sono presenti nella Relazione citata). Non abbiamo ad oggi però nessuna oggettiva evidenza che a consultare la banca dati alle ore 3.00 circa sia stato effettivamente il reclamante”;

“La notizia della probabile intrusione è stata trattata pertanto come un incidente ex novo, ed è stata effettuata la notifica ex art.33 del Regolamento (UE) 2016/679, entro 72 ore da quando ne ho avuto personalmente conoscenza (ns. prot. n. 18309 del 18.06.2021)”.

Come dichiarato in atti, il 18 giugno 2021 l’ASST, ai sensi dell’art. 33 del Regolamento, ha trasmesso al Garante la notifica di violazione dei dati personali, riguardante l’accesso da parte di un soggetto terzo a dati di oltre 1700 assistiti che hanno aderito alla campagna vaccinale influenzale 2020/2021. La predetta Azienda ha dichiarato che il giorno 16 giugno 2021 è venuta a conoscenza della violazione avvenuta il 22 marzo 2021 “a seguito di ricerche svolte in relazione al procedimento” avviato dallo scrivente Dipartimento (v. nota del 18 giugno 2021, sezione C punti 2 e 3 e relazione del Responsabile dei Sistemi Informativi Aziendali (SIA) del 17/06/2021 allegata alla notifica).

Nella predetta notifica l'ASST ha rappresentato che, prendendo atto della XX, […] nella quale — testualmente, sotto la propria responsabilità - scrive: "ho provveduto a distruggere la copia locale senza mai diffonderla o utilizzarla", ha ritenuto di non dover predisporre alcuna comunicazione nei confronti degli utenti" (v. nota del 18 giugno 2021 sez. G punto 1).

Per quanto attiene alle misure volte a garantire la sicurezza del trattamento in essere al momento della violazione dei dati personali oggetto di notifica, l'ASST ha dichiarato che:

> - "le misure tecniche adottate fino alle ore 14.00 del 22.3.2021, con riferimento all'integrità, sicurezza e riservatezza dei dati, sono state: - Backup due volte al giorno delle prenotazioni registrate, con profondità storica di 15 gg solari e con dati salvati su altro dispositivo non accessibile da rete esterna (dietro firewall) - Accesso fisico protetto al locale server - Utenze amministrative di sistema rilasciate solo a personale tecnico SIA - Presenza di un server di backup "freddo" attivabile in 20 minuti dalla indisponibilità del sistema principale. A tali misure, dalle ore 14.00 del 22.3.2021 è stato aggiunto il Blocco di tutte le pagine non inerenti il servizio e delle backdoor note sulla nuova versione.. È inoltre in fase di scrittura una componente di programma che storicizzi su un sistema non esposto al pubblico le prenotazioni relative ad un tempo passato al fine di minimizzare l'impatto di una nuova eventuale intrusione";
>
> - "L'Azienda, come già dichiarato, non era a conoscenza del fatto che si fosse verificato un accesso "non consentito" al proprio software, svolto con modalità e competenze non "comuni", tali da evidenziare i dati di salute presenti nel software. La consapevolezza della possibile vulnerabilità del sito — tollerata temporaneamente per le ragioni spiegate, vista purtroppo la situazione di emergenza sanitaria in corso - aveva comunque già dato luogo alle necessarie azioni per ripristinarne la sicurezza" (v. nota del 23 aprile 2021).

Per quanto attiene alle misure adottate per prevenire simili violazioni in futuro, l'ASST ha dichiarato che "a partire dal 30/3/2021 è stata attivata una funzione di tracciamento e log, non presente sul sistema precedente, che permette di analizzare lo stato di eventuali tentativi di intromissione e la loro frequenza ed evoluzione […] Dal 21/4/2021 è stato poi introdotto il protocollo https (porta 443) al posto del precedente http (porta 80), al fine di rendere ancora più sicure le transazioni" (cfr. relazione SIA, cit.).

In relazione a quanto emerso dalla documentazione in atti, l'Ufficio, nel disporre la riunione dei procedimenti istruttori avviati a seguito del predetto reclamo e della notifica di violazione effettuata dall'ASST nord di Milano, ha notificato alla stessa, ai sensi dell'art. 166, comma 5, del Codice, l'avvio del procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento, invitando il predetto titolare a produrre al Garante scritti difensivi o documenti ovvero a chiedere di essere sentito dall'Autorità (art. 166, commi 6 e 7, del Codice; nonché art. 18, comma 1, dalla legge n. 689 del 24/11/1981) (nota del 2 novembre 2021, prot. n. 54617).

In tale atto, l'Ufficio, nel prendere atto delle azioni poste in essere dall'ASST per superare le criticità emerse nel corso del procedimento, ha ritenuto che il trattamento di dati personali in questione sia stato effettuato in maniera non conforme ai principi di "integrità e riservatezza" (art. 5, par. 1, lett. f) del Regolamento), omettendo di mettere in atto, fin dalla progettazione del sito/servizio web, misure tecniche e organizzative idonee a garantire un livello di sicurezza adeguato al rischio (artt. 25 e 32 del Regolamento). Nel predetto atto è stato inoltre rappresentato il ritardo della notifica di violazione all'Autorità rispetto a quanto previsto nell'art. 33 del Regolamento.

Con nota del 25 novembre 2021, l'ASST nord di Milano ha fatto pervenire le proprie memorie difensive, in cui sono stati ribaditi il "peculiare "contesto" (…) nel quale è stato posto in essere il sistema di prenotazione oggetto della segnalazione, cioè una situazione di conclamata emergenza

legata alla pandemia", "la dimostrata volontà di applicare misure di sicurezza sempre maggiori, che, come chiarito, erano state progettate a prescindere dalla segnalazione ricevuta" e "il necessario bilanciamento di interessi tra l'urgenza di adottare soluzioni efficienti ed immediate per i cittadini, finalizzate ad assicurare la continuità del servizio di vaccinazione antinfluenzale con tutte le conseguenze sanitarie connesse, e le misure di sicurezza oggettivamente applicabili in quel frangente".

2. Esito dell'attività istruttoria.

Preso atto di quanto rappresentato dall'ASST nord di Milano nella documentazione in atti e nelle memorie difensive, si osserva che:

ai sensi del Regolamento si considerano "dati relativi alla salute" i dati personali attinenti alla salute fisica o mentale di una persona fisica, compresa la prestazione di servizi di assistenza sanitaria, che rivelano informazioni relative al suo stato di salute (art. 4, par. 1, n. 15, del Regolamento). Il considerando n. 35 del Regolamento precisa poi che i dati relativi alla salute "comprendono informazioni sulla persona fisica raccolte nel corso della sua registrazione al fine di ricevere servizi di assistenza sanitaria"; "un numero, un simbolo o un elemento specifico attribuito a una persona fisica per identificarla in modo univoco a fini sanitari";

il Regolamento prevede che i dati personali siano "trattati in maniera da garantire un'adeguata sicurezza (...) compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali («integrità e riservatezza»)" (art. 5, par. 1, lett. f) del Regolamento). Il Regolamento prevede inoltre che il titolare del trattamento, 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 di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, debba mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso, "la cifratura dei dati personali" (art. 32 del Regolamento);

in base al principio di "protezione dei dati fin dalla progettazione", di cui all'art. 25, par. 1, del Regolamento, il titolare del trattamento, tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi aventi probabilità e gravità diverse per i diritti e le libertà delle persone fisiche costituiti dal trattamento, sia al momento di determinare i mezzi del trattamento sia all'atto del trattamento stesso, deve mettere in atto misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati e a integrare nel trattamento le necessarie garanzie al fine di soddisfare i requisiti del Regolamento e tutelare i diritti degli interessati;

il Regolamento stabilisce che "in caso di violazione dei dati personali, il titolare del trattamento notifica la violazione all'autorità di controllo competente a norma dell'articolo 55 senza ingiustificato ritardo e, ove possibile, entro 72 ore dal momento in cui ne è venuto a conoscenza, a meno che sia improbabile che la violazione dei dati personali presenti un rischio per i diritti e le libertà delle persone fisiche. Qualora la notifica all'autorità di controllo non sia effettuata entro 72 ore, è corredata dei motivi del ritardo" (art. 33, par. 1). Al riguardo, le "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" del Gruppo di Lavoro Articolo 29 per la Protezione dei Dati del 3 ottobre 2017, come modificate e adottate in ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018 (di seguito "Linee guida"), stabiliscono che "il titolare del trattamento debba considerarsi "a conoscenza" nel momento in cui è ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla

compromissione dei dati personali. […] Il titolare del trattamento è quindi tenuto a prendere le misure necessarie per assicurarsi di venire "a conoscenza" di eventuali violazioni in maniera tempestiva in modo da poter adottare le misure appropriate" (par. II.A.2). Inoltre, le Linee guida prevedono che "se una persona, un'organizzazione di comunicazione o un'altra fonte informa il titolare del trattamento di una potenziale violazione o se egli stesso rileva un incidente di sicurezza, il titolare del trattamento può effettuare una breve indagine per stabilire se la violazione si sia effettivamente verificata. Durante il periodo di indagine il titolare del trattamento non può essere considerato "a conoscenza. Tuttavia, si prevede che l'indagine iniziale inizi il più presto possibile e stabilisca con ragionevole certezza se si è verificata una violazione; può quindi seguire un'indagine più dettagliata. Dopo che il titolare del trattamento è venuto a conoscenza di una violazione soggetta a notifica, la stessa deve essere notificata senza ingiustificato ritardo e, ove possibile, entro 72 ore. Durante questo periodo il titolare del trattamento dovrebbe valutare il rischio probabile per le persone fisiche al fine di stabilire se è soddisfatto il requisito per la notifica e quali siano le azioni necessarie per far fronte alla violazione" (par. II.A.2);

le disposizioni d'urgenza adottate nel corso degli ultimi mesi prevedono degli interventi emergenziali che implicano il trattamento dei dati e che sono frutto di un delicato bilanciamento tra le esigenze di sanità pubblica e quelle relative alla protezione dei dati personali, in conformità a quanto dettato dal Regolamento per il perseguimento di motivi di interesse pubblico nei settori della sanità pubblica (cfr. art. 9, par. 1, lett. i)). Resta ovviamente fermo che il trattamento dei dati personali connesso alla gestione della predetta emergenza sanitaria deve svolgersi nel rispetto della disciplina vigente in materia di protezione dei dati personali e, in particolare, dei principi applicabili al trattamento, di cui agli artt. 5 e 25, par. 2, del Regolamento, in parte sopra richiamati;

la predetta normativa di urgenza non ha derogato ai principi di riservatezza e integrità dei dati (art. 5, par. 1, lett. f) del Regolamento), di "protezione dei dati fin dalla progettazione) (art. 25 del Regolamento) e alle disposizioni in materia di protezione dei dati personali relative alla sicurezza del trattamento (art. 32 del Regolamento) e alla violazione dei dati personali (art. 33 del Regolamento);

la predetta violazione dei dati personali, come dichiarato in atti dall'ASST nord di Milano, è stata portata a conoscenza della stessa con la richiesta di informazioni dell'Ufficio del Garante del 7 aprile 2021, nel corso dell'attività istruttoria. Ciò stante, si rileva che la stessa Azienda ha provveduto a notificare la violazione solo in data 18 giugno 2021, senza fornire le motivazioni del ritardo. Gli elementi forniti nella predetta richiesta di informazioni erano tali da consentire al titolare di essere "ragionevolmente certo che si è verificato un incidente di sicurezza che ha portato alla compromissione dei dati personali" (cfr. le citate Linee guida, spec. par. II.A.2), tenuto anche conto che nella predetta richiesta sono state espressamente richieste "le valutazioni effettuate in ordine ai rischi per i diritti e le libertà per gli interessati derivanti dall'episodio oggetto di segnalazione, anche al fine di verificare la sussistenza dei presupposti per la notifica della violazione dei dati personali all'Autorità e, se del caso, la comunicazione della stessa agli interessati coinvolti (artt. 33 e 34 del Regolamento)" e, successivamente, le "informazioni di maggiore dettaglio in ordine alle motivazioni in virtù delle quali non è stata effettuata la notifica di violazione di dati personali (art. 33 del Regolamento) e la comunicazione della stessa agli interessati (art. 34)". Il suddetto ritardo nel notificare la violazione di dati personali integra gli estremi di una violazione degli obblighi di cui all'art. 33 del Regolamento;

secondo quanto documentato in atti, i dati personali degli assistiti che hanno aderito alla campagna vaccinale influenzale 2020/2021, conservati sul server che forniva il servizio di "prenotazione "light" per la vaccinazione antinfluenzale", erano indicizzati e liberamente rintracciabili in rete con l'ausilio di comuni motori di ricerca web. Pertanto, chiunque,

effettuando una ricerca con un comune motore di ricerca, avrebbe potuto accedere ai file disponibili alle URL http://2.228.136.235/vacEage/agenda.csv e http://2.228.136.235/vacEage/agenda2020.csv. Ciò è stato determinato dell'assenza di un sistema di autenticazione informatica che avrebbe dovuto limitare l'accesso ai soli soggetti autorizzati, dotati di apposite credenziali di autenticazione. Considerato che il servizio online era esposto ai predetti rischi di attacchi informatici e tenuto conto dell'assenza di un sistema di autenticazione informatica, le misure adottate dall'ASST nord di Milano non risultano conformi alle disposizioni di cui all'art. 5, par. 1, lett. f), e all'art. 32, par. 1, del Regolamento.

allo stato dell'arte, l'utilizzo di tecniche crittografiche è una delle misure comunemente adottate per proteggere, in particolar modo, i dati personali degli utenti di un servizio online durante la loro trasmissione su rete Internet. Dall'accertamento compiuto sulla base degli elementi acquisiti e dei fatti emersi a seguito dell'attività istruttoria, risulta che l'accesso al servizio web di prenotazione dei tamponi per la ricerca del SARS-CoV-2 è avvenuto in modo non sicuro, mediante il protocollo di rete "http" (hypertext transfer protocol). Tale protocollo, infatti, non garantisce la riservatezza e l'integrità dei dati scambiati tra il browser dell'utente e il server che ospita il sito web dell'Azienda, e non consente agli utenti di verificare l'autenticità del sito visualizzato. Tenuto conto della natura, dell'oggetto e della finalità del trattamento, nonché dei rischi che insistono sui dati e della possibile "clonazione" del sito web in questione per l'acquisizione dei dati trasmessi per fini illeciti, la soluzione adottata dall'ASST nord di Milano non può essere considerata una misura tecnica idonea a garantire un livello di sicurezza adeguato ai rischi presentati dal trattamento, che prevede la trasmissione di dati, anche relativi alla salute, su una rete pubblica di comunicazioni. Il mancato utilizzo di tecniche crittografiche per il trasporto dei dati configura, quindi, una violazione dell'art. 5, par. 1, lett. f), e dell'art. 32 del Regolamento, che peraltro, al par. 1, lett. a), individua espressamente la cifratura dei dati come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio (sul punto, cfr. anche il considerando n. 83 del Regolamento nella parte in cui prevede che "il titolare del trattamento […] dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura"). L'ASST nord di Milano, infatti, avrebbe dovuto mettere in atto, fin dalla progettazione del proprio sito/servizio web, misure tecniche e organizzative adeguate, volte ad attuare in modo efficace i principi di protezione dei dati, tra cui il principio di "integrità e riservatezza", provvedendo ad adottare un protocollo di rete sicuro, quale il predetto protocollo "https" (hypertext transfer protocol over secure socket layer), nell'ambito del sito/servizio web oggetto del reclamo.

3. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare nel corso dell'istruttoria e considerato 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" gli elementi forniti dal titolare del trattamento nelle memorie difensive non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del Regolamento del Garante n. 1/2019.

Per tali ragioni, si rileva l'illiceità del trattamento di dati personali effettuato dall'ASST nord di Milano, nei termini di cui in motivazione, in violazione degli artt. 5, par.1, lett. f), 25, 32 e 33 del Regolamento.
In tale quadro, fermo restando che il reclamante ha dichiarato di aver distrutto copia della documentazione a cui ha acceduto, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, atteso che l'ASST ha scelto per i servizi sopra descritti una nuova piattaforma software, ha introdotto la funzione di tracciamento, nonché ha adottato un protocollo di comunicazione sicura

("https"), non ricorrono i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, del Regolamento.

4. 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).

La violazione degli artt. 5, par.1, lett. f), 25, 32 e 33 del Regolamento, causata dalla condotta posta in essere dall'ASST nord di Milano, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4 e 5, del Regolamento.

Si consideri che 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).

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenuto conto dei principi di effettività, proporzionalità e dissuasività, indicati nell'art. 83, par. 1, del Regolamento, alla luce degli elementi previsti all'art. 85, par. 2, del Regolamento in relazione ai quali si osserva che:

- l'Autorità ha preso conoscenza dell'evento a seguito di un reclamo; sui medesimi fatti il titolare ha successivamente presentato una notifica di violazione dei dati personali (art. 83, par. 2, lett. h), del Regolamento);

- il trattamento effettuato dall'ASST riguarda categorie particolari di dati quali quelli idonei a rilevare informazioni sulla salute di un numero significativo di interessati (oltre 1700) (art. 83, par. 2, lett. a) e g), del Regolamento);

- l'ASST ha dimostrato un elevato grado di cooperazione adoperandosi al fine di introdurre, anche nella concomitanza del contesto emergenziale- misure idonee a superare i rilievi manifestati dall'Ufficio con l'atto di avvio del procedimento sanzionatorio (art. 83, par. 2, lett. c), d) e f), del Regolamento);

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria prevista dall'art. 83, par. 5, lett. a), del Regolamento, nella misura di 20.000 (ventimila) per la violazione artt. 5, par.1, lett. f), 25, 32 e 33 del Regolamento o, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Si ritiene, altresì, che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e dall'art. 16 del Regolamento del Garante n. 1/2019, anche in considerazione della tipologia di dati personali oggetto di illecito trattamento.

Si rileva, infine, che ricorrono 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.

TUTTO CIÒ PREMESSO IL GARANTE

dichiara l'illiceità del trattamento di dati personali effettuato dalla Azienda socio sanitaria territoriale Nord di Milano per la violazione degli artt. 5, par.1, lett. f), 25, 32 e 33 del Regolamento nei termini di cui in motivazione.

ORDINA

ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento, nonché dell'art. 166 del Codice, all'Azienda socio sanitaria territoriale Nord di Milano, codice fiscale 09320420962, in persona del legale rappresentante pro-tempore, di pagare la somma di euro 20.000 (ventimila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento; si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata.

INGIUNGE

alla predetta Azienda, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 20.000 (ventimila) secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice, la pubblicazione per intero del presente provvedimento sul sito web del Garante e 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, 27 gennaio 2022

IL PRESIDENTE
Stanzione

IL RELATORE
Cerrina Feroni

IL SEGRETARIO GENERALE
Mattei