Ordinanza ingiunzione nei confronti di Società Med Store Saronno s.r.l. - 2 dicembre 2021 [9734934]

[doc. web n. 9734934]

Ordinanza ingiunzione nei confronti di Società Med Store Saronno s.r.l. - 2 dicembre 2021

Registro dei provvedimenti
n. 423 del 2 dicembre 2021

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

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

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

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

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

VISTA la documentazione in atti;

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

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. La violazione dei dati personali.

Con nota del XX la Casa di cura Fondazione Gaetano e Piera Borghi s.r.l. (di seguito "Casa di cura") ha notificato al Garante, ai sensi dell'art. 33 del Regolamento, una violazione dei dati personali in relazione a un attacco informatico riconducibile al gruppo hacker LulzSec_ITA, che ha

comportato la pubblicazione, sul profilo Twitter del medesimo gruppo, di immagini radiologiche riconducibili alla Casa di cura, dichiarando di essere venuta a conoscenza del descritto episodio in data XX, a seguito di comunicazione da parte della polizia postale.

In particolare, la Casa di cura ha rappresentato che "un soggetto qualificatosi come hacker e denominato LulzSecITA, ha pubblicato sul proprio account di Twitter il seguente messaggio: «Tanti soldi spesi nella sanità, e poi nostri dati privati e sensibili, sono protetti da password di default. Che schifo». Da controlli immediatamente richiesti al Responsabile del Trattamento dei dati — Amministratore di Sistema Società Med Store Saranno S.r.l., tale nominato con atto del XX (…), è emerso che dalla schermata che avrebbe dovuto consentire ai soli medici facenti capo alla Fondazione l'accesso da remoto ad esami diagnostici, misura questa introdotta in data XX nel quadro delle misura anti assembramento per fronteggiare il Covid, era possibile accedere ai dati mediante password di default e non dedicate, in tal modo rendendo l'accesso ai dati non impossibile. In particolare, dai citati controlli sui file di log eseguiti dal citato responsabile, è emerso che sono state visionate dall'hacker un solo fotogramma di indagine radiologica di un interessato (l'indagine completa è composta da una pluralità di immagini) e la radiografia di altro interessato, senza poter vedere in entrambi i casi alcun referto, poiché non accessibile dal web. In ogni caso la pubblicazione su Twitter è avvenuta oscurando il cognome e ogni altro dato utile all'identificazione. Il citato responsabile ha ammesso l'accaduto, assumendosi la responsabilità dello stesso e precisando di aver subito rimosso le cause. (…). Il legale della Fondazione provvederà alle necessarie iniziative nei confronti del Responsabile del trattamento".

2. L'attività istruttoria.

A seguito della citata notifica, l'Ufficio ha chiesto alla Casa di cura di fornire alcuni elementi utili alla valutazione dei profili in materia di protezione dei dati personali (nota del XX, prot. n. XX).

La Casa di cura ha fornito riscontro, anche sulla base dei chiarimenti forniti dal responsabile del trattamento, dichiarando che "questo gruppo [gli hacker, n.d.a.] è riuscito ad entrare nell'IP pubblico […] nello specifico non è stata usata per la configurazione la porta standard "80" ma la una porta NON STANDARD "88", solo arrivando a questo punto ha trovato l'accesso "admin" "admin" […] Il radiologo ha sempre usato questa password per gli accessi". Per quanto attiene, poi, alle misure adottate per porre rimedio alla violazione dei dati personali e per attenuarne i possibili effetti negativi nei confronti degli interessati, la Casa di cura ha rappresentato che "il Responsabile del Trattamento conferma nelle sue comunicazioni di avere provveduto alla sostituzione delle password di accesso immediatamente dopo aver ricevuto la segnalazione" e che "l'adozione del protocollo sicuro HTTPS è stata commissionata e sarà implementata nei tempi tecnici a ciò strettamente necessari" (v. nota del XX punti c), d) e h)).

In relazione alla comunicazione ricevuta, l'Ufficio, con atto del XX, prot. n. XX, ha avviato, ai sensi dell'art. 166, comma 5, del Codice, con riferimento alle specifiche situazioni di illiceità in esso richiamate, un procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2 del Regolamento, nei confronti della Società Med Store Saronno S.r.l, (di seguito "Società"), invitandola 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, l. n. 689 del 24 novembre 1981).

In particolare l'Ufficio, nel predetto atto, ha preliminarmente rappresentato che:

- le informazioni oggetto della violazione costituiscono dati personali relativi alla salute, che meritano una maggiore protezione dal momento che il contesto del loro trattamento potrebbe creare rischi significativi per i diritti e le libertà fondamentali (Cons. n. 51);

- la disciplina in materia di protezione dei dati personali stabilisce che i medesimi dati devono

essere “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);

- in materia di sicurezza dei dati personali, il titolare del trattamento e il responsabile del trattamento devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, “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” (…). “Nel valutare l’adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall’accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati” (art. 32 del Regolamento);

- dall’esame della documentazione in atti, sono emersi alcuni profili di criticità relativi agli obblighi in materia di sicurezza del trattamento, con particolare riferimento all’utilizzo di protocolli di rete non sicuri e alla mancata definizione di password policy;

• in relazione al primo profilo, al momento della violazione, l’installazione volta a consentire al radiologo di visionare le immagini da refertare, effettuata da remoto il XX, consentiva l’accesso al software MED Dream -visualizzatore DICOM ideato per diagnosi, visualizzazione, archiviazione e trasmissione di immagini medicali fruibile mediante browser web e una password di accesso- su protocollo http (hypertext transfer protocol), un protocollo di rete che non garantisce l’integrità e la riservatezza dei dati scambiati tra il browser dell’utente e il server che ospita il servizio/sito web e non consente agli utenti di verificare l’autenticità del server a cui si collegano;

• quanto al secondo profilo, al momento della violazione, l’accesso al software MED Dream da parte del radiologo era effettuato con un’utenza di tipo amministrativo (admin) e password non robusta (admin).

Nel predetto atto, era stato, quindi, evidenziato che il mancato utilizzo di strumenti di crittografia per la trasmissione dei dati e l’accesso al software MED Dream in assenza di controlli sulla qualità delle password utilizzate-per utenze tecniche e per utenze in uso a soggetti autorizzati-, di misure per la modifica obbligatoria delle stesse al primo utilizzo o, comunque, periodicamente, nonché di meccanismi di blocco automatico delle utenze in caso di ripetuti tentativi di accesso non andati a buon fine, non risultavano conformi alle disposizioni di cui all’art. 5, par. 1, lett. f) e all’art. 32 del Regolamento, tenuto conto della natura dei dati in questione (anche relativi alla salute) e degli elevati rischi derivanti dalla loro possibile acquisizione da parte di terzi.

Ciò premesso, sulla base degli elementi in atti, con la predetta nota del XX, l’Ufficio ha reputato che, al momento in cui si è verificata la violazione dei dati personali, la Società Med Store Saronno S.r.l., in qualità di responsabile del trattamento, avesse effettuato un trattamento in violazione degli obblighi in materia di sicurezza del trattamento di cui all’art. 32 del Regolamento e dei principi di base di cui all’art 5 del medesimo Regolamento.

Con nota del XX, la Società Med Store Saronno s.r.l. ha fatto pervenire le proprie memorie difensive, nelle quali, in particolare, è stato rappresentato che:

a) “La Med Store Saronno S.r.l. è una società che ha quale oggetto sociale il commercio all'ingrosso ed al dettaglio di macchine ed attrezzature per ufficio, sistemi informatici e periferiche, produzione, sviluppo e commercializzazione di programmi applicativi di carattere

commerciale, didattico, creativo e consulenza ed assistenza software e hardware";

b) "la Med Store è distributrice in esclusiva per il territorio italiano del software MedDream DICOM Viewer realizzato per la diagnosi, visualizzazione, archiviazione e trasmissione di immagini medicali. Come visualizzatore di immagini diagnostiche, MedDream è costituito da un componente Viewer, che gira in un browser e non richiede alcuna installazione sul dispositivo client, e da un application server MedDream, che gestisce la comunicazione con i sistemi ospedalieri (HIS/RIS/PACS e qualsiasi altro EMR) e prepara le immagini per lo streaming sul visualizzatore DICOM di MedDream. MedDream utilizza un'interfaccia di integrazione flessibile e aperta per la connessione ai sistemi HIS e/o EMR basata principalmente sulle chiamate URL, consentendo così di integrarla in qualsiasi applicazione medica";

c) "la Società Med Store Saronno S.r.l., in relazione alla fornitura alla Casa di Cura Fondazione Gaetano e Piera Borghi S.r.l. del software sopra identificato, è stata dalla stessa nominata Responsabile del Trattamento con atto del XX";

d) "in data XX, la Fondazione richiedeva alla Med Store l'installazione del programma MedDream per fare fronte all'esigenze derivanti dall'emergenza pandemica COVID-19 le quali avevano fatto sorgere la necessità di permettere a tecnici radiologi di poter visionare le immagini DICOM da remoto. Al momento dell'installazione l'accesso al software era garantito da un userid e da una password di sistema da associare – nel periodo di training che di solito viene svolto in loco ma che non è stato possibile svolgere causa COVID - al nominativo del soggetto a cui è garantito l'accesso e ad una password alfanumerica da quest'ultimo prescelta";

e) "in merito alla natura del software è, tuttavia, necessario effettuare una preliminare precisazione: MedDream (…) è solo un visualizzatore di immagini radiologiche. Tramite la visualizzazione delle stesse non è possibile accedere a nessun dato sensibile del paziente che ne rilevi lo stato di salute. Oltre a ciò, nessun dato personale, oltre al nominativo, al sesso e alla data di nascita è ricavabile dall'accesso al predetto software. Il software MedDream, inoltre, non consente il salvataggio dei dati in locale, in quanto al logout tutti i dati vengono cancellati";

f) "con una telefonata del XX, la Polizia Postale informava la Med Store (in quanto esclusivista del programma Med Dream ed essendo tale dato l'unico direttamente ricavabile dal tweet in oggetto) della pubblicazione sul profilo Twitter @LuIzSec_ITA di un tweet contenente alcune sparute immagini di diagnostica strumentale commentata come segue "Tanti soldi spesi nella sanità, e poi i nostri dati privati e sensibili, sono protetti da password di default. Che schifo" con un tweet successivo di precisazione in cui si specificava ciò "Ragazzi ma nessuno ha detto che il tweet precedente parlasse del San Raffaele. Si parla di Sanità in generale, quello è sempre un ospedale, ma non il San Raffaele";

g) "tale account Twitter, sospeso nel XX dalla piattaforma ma riaperto ora sotto diverso nickname @LulzSecurityITA, è riconducibile alla "divisione" italiana del collettivo di hacker Lulz, tristemente noto a livello mondiale per le sue attività di hackeraggio e divulgazione/compromissione di dati personali e che si è contraddistinto, in epoca COVID, per numerosi attacchi a strutture sanitarie italiane a fini puramente emulativi";

h) "nelle singole immagini diagnostiche pubblicate su Twitter veniva oscurato, da parte del predetto gruppo hacker, ogni riferimento idoneo a ricondurre le predette immagini a persona identificata e/o identificabile anche in via indirettamente. Veniva, infatti, occultato sia il nominativo che la data di nascita del paziente nonché ogni elemento relativo alla struttura ove tale diagnostica era stata eseguita";

i) “immediatamente, la Med Store si attivava al fine di supportare il lavoro della Polizia postale onde identificare la provenienza della predetta immagine; compito, questo, non agevole, avendo a disposizione esclusivamente un codice paziente. Identificata la provenienza delle immagini e provveduto immediatamente a sostituire la password violata, la Med Store comunicava tempestivamente alla Polizia Postale i dati di provenienza delle immagini. Ne seguiva l’informativa della medesima alla Fondazione e la conseguente notifica effettuata dalla Fondazione titolare del trattamento ai sensi dell’art. 33 del Regolamento”;

j) “a seguito di ciò, la Med Store con propria mail del XX (…) informava la Fondazione che, in data 25 maggio alle ore 11.50, erano stati effettuati accessi molto veloci in cui erano state visualizzate le singole immagini poi postate nel tweet. La Med Store informava, altresì, la Fondazione che: nel giorno precedente e successivo all’indebito accesso non era stata effettuato alcun ulteriore accesso da soggetti non autorizzati; l’oggetto dell’accesso era riferito soltanto ad alcune singole e non significative immagini, essendo precluso ogni accesso allo studio clinico; si era già provveduto alla sostituzione delle password violate”;

k) “la Med Store si faceva subito parte proattiva nell’individuare meccanismi correttivi tesi a meglio integrare la rete aziendale col predetto software, proponendo alla Fondazione di dotarsi di protezione in HTTPS (certificato SSL) adempimento, questo, che è stato tempestivamente posto in essere dalla Fondazione stessa”;

l) “la scrivente Med Store ritiene non possa ravvisarsi in capo al responsabile del trattamento alcuna violazione degli obblighi in materia di sicurezza del trattamento di cui all’art. 32 del Regolamento e dei principi di base di cui all’art 5 del medesimo Regolamento” in quanto “per quanto attiene l’utilizzo di protocolli di rete non sicuri, si significa che l’accesso ai dati è stato frutto di una intenzionale ed esperta azione di hackeraggio che ha coinvolto diversi soggetti espletanti l’attività sanitaria e no. L’ingresso nell’IP pubblico della Fondazione (…) è avvenuto tramite configurazione della porta non standard “88”. Trattasi, come noto, di un ben identificato attacco hacker da parte di un gruppo dedito a tali attività da tempo e più volte oggetto di provvedimenti dell’autorità giudiziaria. Peraltro, la Med Store – fornitrice del software e Responsabile per il trattamento dei dati personali ad esso correlati – non è responsabile della gestione della rete aziendale della Fondazione e dei suoi protocolli di sicurezza. Nonostante quanto sopra, nell’immediatezza dell’avvenuto e al fine di ottimizzare i sistemi di sicurezza della rete, la MED Store ha suggerito alla Fondazione di attivare la protezione in HTTPS (certificato SSL), associando l’indirizzo IP pubblico della Fondazione ad un dominio web e conseguentemente acquisendo un certificato SSL per il dominio stesso. Oltre a ciò, è stata rappresentata la possibilità di interfacciamento attraverso LDAP al sistema di generazione delle password, utilizzando le policy già in vigore da parte della Fondazione. Entrambi tali adempimenti sono stati posti successivamente in essere dalla Fondazione”; “nessuna responsabilità da parte di Med Store è configurabile, pertanto, sotto tale profilo”; “in merito alla mancata definizione di password policy (…), il software Med Store risulta essere già aderente al dettato normativo in merito ai controlli sulla qualità delle password utilizzate, alle misure per la modifica obbligatorie delle stesse, nonché ai meccanismi di blocco automatico delle utenze”;

m) “ciò che è avvenuto è imputabile esclusivamente alla mancata assegnazione specifica di userid e password al momento dell’installazione del software medesimo in quanto, (…) per ragioni evidenti di forza maggiore; la predetta installazione è avvenuta in modalità remota senza avere la possibilità – per ragioni non imputabili a Med Store – di effettuare la formazione on site dei soggetti preposti all’utilizzo anche al fine di verificare le corrette modalità di accesso al programma”;

n) “l’accesso all’IP pubblico della Fondazione non è avvenuto dalla porta standard 80 ma da

una porta NON STANDARD “88” (il che denota la particolare perizia dell’autore dell’hackeraggio). Solo grazie a ciò, i soggetti autori hanno potuto accedere al programma tramite la password originariamente inserita e non ancora assegnata”;

o) “dall’installazione del programma presso la Fondazione (in modalità remota) all’attacco hacker erano decorsi soli 60 gg in periodo di totale Lockdown in cui era precluso ogni ingresso alla struttura da parte di personale non indispensabile sotto il profilo sanitario”;

p) “si ribadisce che il software MED Dream è esclusivamente un software di visualizzazione di diagnostica per immagini”;

q) “nessun dato personale o sensibile è contenuto nell’immagine medesima, nessuno studio o referto clinico, nessuna informazione atta a ricondurre tale immagine ad un determinato paziente né tantomeno alla struttura dove è stata effettuata l’indagine diagnostica. Ne consegue che nessun danno materiale o immateriale, nemmeno potenziale, si è verificato in relazione all’accesso abusivo di che trattasi da parte del gruppo hacker LulzITA”;

r) con particolare riferimento agli elementi per le valutazioni di cui all’art. 83, par. 2 del Regolamento:

in relazione alla lett. a) “l’azione (perpetrata dal gruppo hacker) ha avuto durata pressoché istantanea. Non vi è stato nessun accesso al software né precedentemente né successivamente all’ingresso abusivo del XX. A seguito dell’informativa della Polizia Postale si è, altresì, proceduto immediatamente alla modifica delle credenziali di accesso. Come già rappresentato dalla Fondazione e documentalmente comprovato dai file di log ad essa trasmessi dalla scrivente e da quest’ultima prodotti all’Autorità, gli ingressi hanno consentito la visualizzazione esclusivamente di singole e sparute immagini diagnostiche (in alcun modo significative) senza che sia stato accessibile alcun dato sensibile”; “nella pubblicazione sul profilo Twitter dell’autore dell’attività di hackeraggio, il gruppo hacker ha oscurato qualsiasi riferimento a persone o alla struttura stessa della Fondazione”; “l’installazione del software è avvenuta necessariamente da “remoto” in quanto ogni attività on site era preclusa dalla normativa COVID all’epoca in vigore. A ciò si aggiunga il brevissimo lasso di tempo intercorso tra l’installazione del programma e l’attività di hackeraggio in questione”;

in relazione alla lett. b) “escluso per ovvie ragioni alcun elemento di dolo, si ritiene che nel caso di specie non vi possa essere responsabilità del Responsabile del Trattamento dei dati personali nemmeno sotto il profilo della colpa lieve”;

in relazione alla lett. c) “non ci è stato alcun danno per gli interessati. Sotto il profilo dei terzi, in quanto non è stato divulgato alcun dato personale o sensibile. Sul punto si ricorda, peraltro, che la identificazione dell’immagine postata su twitter e la sua riconducibilità ad un paziente della Fondazione è stata oltremodo complessa anche per la Scrivente fornitrice del software. Nessun danno è derivato alla Fondazione in quanto l’accesso non ha comportato nessuna perdita, manomissione o distruzione di dati né alcun danno reputazionale a carico della stessa”;

in relazione alla lett. d) “le misure tecniche e organizzative poste in essere appaiono adeguate alla luce dello stato dell'arte, 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. Tali misure, ovviamente e sotto il profilo della formazione on site, vanno valutate all’epoca dell’accadimento dei fatti e del regime di lockdown allora vigente”;

in relazione alla lett. f) “non appare in dubbio il massimo grado di cooperazione posto in essere dalla scrivente nei confronti del Responsabile del Trattamento dei dati personali nel segnalare la violazione e nell’assisterla (…) in relazione a tutti i chiarimenti richiesti dall’Autorità”;

in relazione alla lett. g) “l’asserita violazione non concerne dati “particolari” (di cui all’art. 9 del Regolamento) ovvero “relativi a condanne penali e reati” (di cui all’art. 10 del Regolamento). Trattasi (…) di singole e sparute immagini di diagnostica, non riconducibili alla persona oggetto dell’analisi né alla struttura in cui è stata effettuata nonché assolutamente inidonee a derivarne qualsivoglia informazione in merito allo stato di salute”;

in relazione alla lett. h) “l’Autorità è venuta a conoscenza della violazione per effetto della tempestiva notifica effettuata dal Titolare ai sensi dell’art. 33 del Regolamento”;

in relazione alla lett. i) “allo stato non ci sono provvedimenti correttivi adottati dal Garante a cui, se del caso, la scrivente si conformerà tempestivamente. Per quanto riguarda il pregresso si ricorda che, rilevato l’accesso abusivo, Med Store si è subito attivata nella sostituzione delle password e nella verifica (negativa) di eventuali ulteriori tentativi di accesso. Inoltre, pur non essendo di competenza specifica della scrivente, è stata consigliata alla Fondazione l’adozione del protocollo HTTPS con le caratteristiche sopra descritte”;

in relazione alla lett. k), si fa riferimento “all’emergenza pandemica e al regime di lockdown in corso all’epoca dello svolgimento dei fatti”.

Pertanto, “poiché il Responsabile del trattamento risponde per il danno causato dal trattamento (danno non verificato), solo se non ha adempiuto gli obblighi del Regolamento specificatamente diretti ai responsabili del trattamento o ha agito in modo difforme o contrario rispetto alle legittime istruzioni del titolare del trattamento”, la Med Store ha chiesto la conclusione del procedimento, tramite archiviazione senza disporre alcuna sanzione a suo carico.

3. Esito dell’attività istruttoria.

Preliminarmente, si osserva che il titolare può affidare un trattamento “a responsabili del trattamento che presentino garanzie sufficienti per mettere in atto di misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i principi del Regolamento”, anche per la sicurezza del trattamento, tenuto conto degli specifici rischi derivanti dallo stesso (artt. 28, par. 1, 24 e 32 del Regolamento; cfr. anche Cons. n. 81). In questo caso “i trattamenti da parte di un responsabile sono disciplinati da un contratto o da altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, che vincoli il responsabile al titolare e che stipuli la materia disciplinata e la durata del trattamento, la natura e la finalità del trattamento, il tipo di dati personali e le categorie di interessati, gli obblighi e i diritti del titolare” (art. 28, par. 3 del Regolamento).

Inoltre, sebbene sul titolare del trattamento, che determina le finalità e le modalità del trattamento dei dati, ricada una “responsabilità generale” per i trattamenti posti in essere (v. art. 5, par. 2, c.d. “accountability”, e 24 del Regolamento), anche quando questi siano effettuati da altri soggetti “per suo conto” (Cons. n. 81, artt. 4, punto 8), e 28 del Regolamento), il Regolamento ha disciplinato gli obblighi e le altre forme di cooperazione a cui è tenuto il responsabile del trattamento e l’ambito delle relative responsabilità (v. artt. 30, 32, 33, par. 2, 82 e 83 del Regolamento).

L’art. 32 del Regolamento stabilisce, infatti, che, non solo il titolare, ma anche il responsabile del trattamento, nell’ambito delle proprie competenze e dei compiti delegati dal titolare, “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" metta in atto "misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio" e che "nel valutare l'adeguato livello di sicurezza si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati".

Dall'esame dell'Atto di nomina del XX, risulta che "l'incarico viene assegnato per il seguente scopo: fornitura del software gestionale; assistenza in loco e in teleassistenza; aggiornamento dei software. L'incarico avrà competenza ai dati presenti sui seguenti sistemi: Sw applicativo Workstation per la visualizzazione delle immagini DICOM; server: per archiviazione e visualizzazione delle immagini WEB in HTLM 5".

Ciò premesso, si rileva che, nel corso dell'istruttoria è emerso che l'installazione che consentiva al medico radiologo di visionare le immagini da refertare, permetteva l'accesso al citato software MED Dream -visualizzatore DICOM pensato per diagnosi, visualizzazione, archiviazione e trasmissione di immagini medicali fruibile mediante browser web - mediante protocollo http (hypertext transfer protocol), ossia un protocollo di rete che non garantisce l'integrità e la riservatezza dei dati scambiati tra il browser dell'utente e il server che ospita il servizio/sito web e non consente agli utenti di verificare l'autenticità del server a cui si collegano.

Al riguardo, tenuto conto della natura dei dati oggetto di accesso e degli elevati rischi derivanti dalla loro possibile acquisizione da parte di terzi, si ritiene che la modalità di accesso al software MED Dream, utilizzando il protocollo http, non possa essere considerata una misura idonea a garantire un adeguato livello di sicurezza (art. 32, par. 1, lett. a) del Regolamento, che individua espressamente la cifratura come una delle possibili misure di sicurezza idonee a garantire un livello di sicurezza adeguato al rischio; v. anche Cons. n. 83 del Regolamento nella parte in cui prevede che "il titolare o il responsabile del trattamento dovrebbe valutare i rischi inerenti al trattamento e attuare misure per limitare tali rischi, quali la cifratura").

Al riguardo, non può inoltre essere ritenuto rilevante quanto dichiarato dalla Società in ordine all'utilizzo di una porta c.d. "non standard" (88) per la configurazione del protocollo http e, in relazione a questo punto, e al fatto che la Società, che si limiterebbe a fornire il software, sarebbe responsabile per il trattamento dei dati personali a esso correlati e non anche responsabile della gestione della rete aziendale della Casa di cura e dei suoi protocolli di sicurezza. Ciò, in quanto, allo stato dell'arte, l'utilizzo di una porta non standard 88 (in luogo di quella standard 80) non costituisce una misura idonea a ridurre in modo significativo i rischi di intrusioni informatiche, considerata la facilità con cui è possibile effettuare una scansione, anche mediante strumenti liberamente disponibili online, di un server o un host connesso alla rete Internet al fine di stabilire quali porte su cui è in ascolto (port scan) e identificare i servizi in esecuzione per sfruttarne le eventuali vulnerabilità.

La Società, in quanto responsabile del trattamento, avrebbe dovuto, in ogni caso, effettuare la configurazione per l'accesso al citato software MED Dream mediante protocollo HTTPS o, in ogni caso, adeguare, nel breve periodo e non a seguito della violazione, l'installazione effettuata da remoto il XX, per consentire al radiologo di visionare le immagini da refertare, nella fase crescente dell'emergenza pandemica da COVID-19.

Nel corso dell'istruttoria è emerso altresì che, al momento della violazione, l'accesso al software MED Dream da parte del radiologo era effettuato con un'utenza di tipo amministrativo (admin) e password non robusta (admin).

Sul punto, in relazione all'asserita impossibilità, dichiarata dalla Società, di assegnare specificatamente userid e password al momento dell'installazione del software medesimo in

quanto, "(…) per ragioni evidenti di forza maggiore, la predetta installazione è avvenuta in modalità remota senza avere la possibilità – per ragioni non imputabili a Med Store – di effettuare la formazione on site dei soggetti preposti all'utilizzo anche al fine di verificare le corrette modalità di accesso al programma", non risulta dimostrato che la predetta assegnazione potesse avvenire solo al momento della formazione dei soggetti autorizzati. L'esigenza di evitare l'accesso in sede dei professionisti e la necessità di fornire loro, nei tempi più rapidi possibili, gli strumenti per poter accedere da remoto alla diagnostica per immagini non giustificano l'utilizzo, da parte di un soggetto autorizzato, di un'utenza tecnica con privilegi amministrativi. La creazione e l'assegnazione di utenze nominali ai soggetti autorizzati al trattamento sono infatti operazioni che ben avrebbero potuto essere effettuate da remoto (e non necessariamente nell'ambito di un'attività di formazione dei soggetti da effettuarsi in presenza), anche nel contesto emergenziale, in un lasso di tempo ragionevole (considerato che sono trascorsi 60 giorni tra l'installazione del software e l'attacco hacker). Infatti, dopo essere venuta a conoscenza della violazione dei dati personali, la Società ha provveduto a sostituire le credenziali di autenticazione in uso al medico radiologo.

Inoltre, si rileva che, se un'utenza tecnica con privilegi amministrativi, come quella in questione, viene assegnata e utilizzata da un soggetto autorizzato in luogo di un'utenza nominale, potrebbe verificarsi un'incongruenza tra i profili di autorizzazione attribuiti e le effettive esigenze di operatività, rendendo possibile a tale soggetto di effettuare talune operazioni di trattamento in assenza di una specifica intenzione e istruzione da parte del titolare o del responsabile del trattamento.

Pertanto, anche in tal caso, si ritiene che le predette modalità di accesso al citato software, considerata l'assenza di misure per la modifica obbligatoria delle stesse al primo utilizzo o, comunque, periodicamente, nonché di meccanismi di blocco automatico delle utenze (in caso di ripetuti tentativi di accesso non andati a buon fine), non risultano adeguate sotto il profilo della sicurezza, in quanto, non conformi, all'art. 32, par. 1, lett. b) del Regolamento, che stabilisce che il titolare e il responsabile del trattamento debbano mettere in atto misure per "assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento".

4. Conclusioni

Il Regolamento ha disciplinato gli obblighi e le specifiche responsabilità non solo del titolare, ma anche del responsabile del trattamento, anche con riguardo alla sicurezza del trattamento (v. artt. 32 e 83, par. 4, del Regolamento).

Dall'istruttoria effettuata, emerge che le misure tecniche e organizzative previste e messe in atto dalla Società Med Store Saronno s.r.l., responsabile per il trattamento della Casa di cura, per la gestione dell'accesso al citato software MED Dream, con particolare riferimento all'utilizzo di protocolli di rete non sicuri (http) e alla mancata definizione di password policy, non sono idonee a garantire un livello di sicurezza adeguato ai rischi dello specifico trattamento. Ciò ha contribuito, peraltro, a creare le premesse per il verificarsi della violazione dei dati personali, oggetto di notifica, con la conseguente illecita acquisizione, da parte di terzi, di dati personali, anche relativi alla salute, degli interessati.

Pertanto, 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"), all'esito dell'esame della documentazione acquisita nonché delle dichiarazioni rese all'Autorità nel corso del procedimento, e alla luce delle valutazioni sopra richiamate, gli elementi forniti dal responsabile del trattamento nelle memorie difensive seppure meritevoli di considerazione e

indicative della piena collaborazione del responsabile del trattamento al fine di attenuare i rischi del trattamento - 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 dalla Società Med Store Saronno s.r.l., in qualità di responsabile del trattamento, per la violazione dei principi di base di cui all'art 5, par. 1, lett. f) del Regolamento e degli obblighi in materia di sicurezza del trattamento di cui all'art. 32, par. 1 del medesimo Regolamento.

In tale quadro, considerando, in ogni caso, che la condotta ha esaurito i suoi effetti, non ricorrono i presupposti per l'adozione delle misure correttive di cui all'art. 58, par. 2, del Regolamento.

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

La violazione degli artt. 5 e 32 del Regolamento, determinata dal trattamento di dati personali, oggetto del presente provvedimento, effettuato dalla Società, è soggetta all'applicazione della sanzione amministrativa pecuniaria ai sensi dell'art. 83, par. 4, lett. a) e par. 5, lett. a) del Regolamento.
Si consideri che il Garante, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del Regolamento del Garante n. 1/2019).

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. 83, par. 2, del Regolamento in relazione ai quali si osserva che:

dalle risultanze degli atti, l'episodio risulta essere stato isolato e determinato da un comportamento doloso da parte di un soggetto terzo rilevato anche dalla polizia postale (art. 83, par. 2, lett. a) e b) del Regolamento);

la violazione ha riguardato dati sulla salute ma non ha interessato referti, in quanto si è trattato di un solo fotogramma di indagine radiologica di un interessato e di una radiografia relativa ad altro interessato; inoltre la pubblicazione su Twitter da parte degli hacker è avvenuta oscurando il cognome e ogni altro dato utile all'identificazione (art. 83, par. 2, lett. a) e g) del Regolamento);

la Società è intervenuta prontamente per attenuare gli effetti della violazione occorsa nonché per prevenire il ripetersi di eventi analoghi, proponendo alla Casa di cura di attivare la protezione in HTTPS (certificato SSL) e sostituendo le password utilizzate (art. 83, par. 2, lett. c) del Regolamento);

l'Autorità ha preso conoscenza dell'evento a seguito della notifica di violazione dei dati personali effettuata, senza ingiustificato ritardo, dal titolare del trattamento (art. 83, par. 2, lett. f) del Regolamento);

non sono pervenuti reclami o segnalazioni al Garante sull'accaduto, non risultano precedenti

violazioni pertinenti commesse dal titolare del trattamento né sono stati precedentemente disposti provvedimenti di cui all'art. 58 del Regolamento (art. 83, par. 2, lett. i) del Regolamento);

la necessità di implementare un sistema di accesso da remoto alla diagnostica per immagini è nata nel contesto emergenziale da pandemia da Covid-19, al fine di consentire lo svolgimento di consulti medici e clinici tra l'equipe curante ed il professionista in grado di interpretare correttamente tali immagini, evitando l'accesso in sede (art. 83, par. 2, lett. k) 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. 4, lett. a) e par. 5, lett. a) del Regolamento, nella misura di euro 7.000,00 (settemila) per la violazione degli artt. 5 e 32 del medesimo Regolamento 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 art. 16 del Regolamento del Garante n. 1/2019.

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

rilevata la violazione degli artt. 5 e 32 del Regolamento, dichiara l'illiceità del trattamento di dati personali effettuato dalla Società Med Store Saronno s.r.l. nei termini di cui in motivazione;

ORDINA

alla Società Med Store Saronno s.r.l., con sede legale in via Garibaldi 43 angolo via Caduti della Liberazione, 21047 Saronno (VA) - P.IVA/C.F 03000070122, in persona del legale rappresentante pro-tempore, ai sensi degli artt. 58, par. 2, lett. i) e 83 del Regolamento, nonché dell'art. 166 del Codice, di pagare la somma di euro 7.000,00 (settemila) a titolo di sanzione amministrativa pecuniaria per la violazione di cui al 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 Società, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 7.000,00 (settemila), 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

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

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

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, 2 dicembre 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL SEGRETARIO GENERALE
Mattei