Registro dei Provvedimenti

N. 19 del 6 luglio 2021

L'AUTORITÀ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Il COLLEGIO

Nella riunione del 6 luglio 2021, alla quale hanno preso parte l'Avv. Nicola Fabiano, Presidente, il Dott. Umberto Rapetto, Vice Presidente, l'Avv. Patrizia Gigante, Componente e la Dirigente Avv. Maria Sciarrino;

VISTA la segnalazione ricevuta da questa Autorità in data 8 aprile 2021 e sottoscritta congiuntamente dai Signori XXX, XXX e XXX;

VISTA la Legge n. 171/2018, relativa alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, con particolare riguardo agli articoli 4, 5, 35, 58, 59, 72 e 73;

RILEVATO che con la menzionata segnalazione i predetti XXX, XXX e XXX riferivano di aver appreso la notizia della diffusione non autorizzata di dati sensibili afferenti le loro persone, "dati che presumibilmente sarebbero stati illegittimamente estrapolati dai rispettivi profili presenti sui social network ("Facebook")";

RILEVATO, inoltre, che con la predetta segnalazione i citati XXX, XXX e XXX chiedevano l'intervento di questa Autorità "volto a verificare possibili violazioni della legge 171/2018, ovvero la commissione di eventuali altri illeciti a danno delle nostre persone che la stessa riterrà di poter individuare";

RILEVATO che la vicenda della diffusione non autorizzata di dati personali che sarebbero stati illecitamente estratti da account di utenti registrati sulla piattaforma di social network "Facebook" è stata divulgata con ampia diffusione sulla rete Internet;

CONSIDERATO, dunque, che la Legge 171/2018 "*garantisce che il trattamento dei dati personali si svolga nel rispetto dei diritti e delle libertà fondamentali, nonché della dignità dell'interessato, con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali*" e che "*chiunque ha diritto alla protezione dei dati personali che lo riguardano*" (articolo 1, commi 2 e 3);

VISTO il proprio provvedimento numero 4/2021 emesso il 9/04/2021 e notificato alla società "**Facebook Ireland Ltd."** con sede legale in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 Ireland**, e alla società "**Facebook Inc.**" con sede legale in **1 Hacker Way, Menlo Park, CA 94025, United States of America** rispettivamente il 26.04.2021 - ricevuto il 19.05.2021 - e il 26.04.2021 – ricevuto il 14.05.2021 - con il quale, fra l'altro, al punto b) si ingiungeva in via d'urgenza, ai sensi dell'art. 59, comma 2, lettera e), della Legge 171/2018, "*di comunicare con mezzi idonei a tutti gli interessati coinvolti la violazione dei dati entro 10 (dieci) giorni dalla ricezione del presente provvedimento*";

CONSIDERATA l'attività istruttoria effettuata e i chiarimenti pervenuti all'Ufficio di questa Autorità Garante dalla sola società Facebook Ireland Ltd.;

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

CONSIDERATO che la società Facebook Ireland Ltd., precisando di qualificarsi quale titolare del trattamento (mentre la società Facebook Inc. riveste la figura di responsabile del trattamento), assume e riconosce che nel periodo tra gennaio 2018 e settembre 2019 sia stato effettuata la sottrazione di dati personali degli utenti della piattaforma di Facebook mediante una tecnica informatica denominata "*scraping*";

CONSIDERATO che la dichiarazione assertiva di Facebook in ordine alla effettiva riconducibilità alla tecnica dello "*scraping*" non è supportata da alcuna relazione tecnica dettagliata, né dall'esito di rigorose attività investigative interne che riconducano in maniera puntuale ed inequivocabile le dinamiche di esfiltrazione dei dati personali alla citata modalità;

CONSIDERATO che, anche a voler ammettere una modalità paragonabile (certo non per l'entità) allo "*scraping*", la grande mole di dati acquisiti da terzi e il conseguente volume di traffico generato per il trasferimento delle informazioni dai server di Facebook ai computer del presunto "*scraper*" doveva essere immediatamente riconosciuta come pericolosa anomalia e avrebbe dovuto innescare meccanismi di prevenzione e di difesa atti ad evitare il perpetrarsi di qualunque azione potenzialmente lesiva delle riservatezza dei dati personali delle persone che aderiscono al sodalizio virtuale;

CONSIDERATO che nella memoria pervenuta all'Ufficio di questa Autorità il 27/5/2021 a pagina 6 si legge testualmente: "*Facebook Ireland ritiene che lo Scraped Data Set sia stato elaborato tra gennaio 2018 e settembre 2019 ("Periodo Rilevante"), attraverso lo scraping dell'enumerazione dei numeri di telefono utilizzando le funzioni di ricerca dei contatti sulle piattaforme Facebook ("Funzionalità Rilevanti")*", richiamando in nota testualmente "*in particolare, Messenger Contact Importer, Facebook Contact Importer e Facebook Search*";

CONSIDERATO, inoltre, che nella stessa memoria Facebook Ireland Ltd. afferma testualmente: "*... comprendiamo che si intenda riferirsi ai dati degli utenti Facebook oggetto di scraping che sono stati resi disponibili al pubblico in un database non protetto all'inizio di quest'anno, come riportato da alcuni articoli di giornale nell'aprile 2021 (il "Scraped Data Set")*";

CONSIDERATO, quindi, che le società Facebook Inc. e Facebook Ireland Ltd. erano pienamente a conoscenza dei rischi connessi a possibili sottrazioni di dati personali mediante la tecnica dello *scraping*, tanto da descriverla nella memoria e nella documentazione inviata;

CONSIDERATO che Facebook, sul proprio sito web all'indirizzo https://www.facebook.com/help/463983701520800, dichiara che "*I rate limit fissano il numero di volte in cui una persona può interagire con i nostri prodotti in un determinato periodi di tempo*" e "*I limiti di dati impediscono alle persone di ottenere più dati rispetto a quelli di cui hanno bisogno per il normale utilizzo dei nostri prodotti*"), e tuttavia, quanto accaduto nel caso in esame, ha evidenziato la sostanziale inidoneità delle misure di sicurezza asseritamente adottate dal titolare del trattamento;

CONSIDERATO, pertanto, che la stessa Facebook Ireland Ltd. – al di là del periodo di riferimento degli eventi occorsi che ad avviso di questa Autorità, in ragione degli esiti

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

dell'attività istruttoria effettuata, comunque risalgono ai primi mesi del 2021 – ha esplicitamente riconosciuto di aver subito una sottrazione di dati personali da parte di terzi (pur riferendosi ad una asserita e non dimostrata azione con la tecnica dello "*scraping*") e che a tale riconoscimento deve attribuirsi valore confessorio;

CONSIDERATO che, per loro natura, le attività perpetrate con la tecnica dello "*scraping*" e/o con qualsiasi altro sistema atto all'indebita acquisizione massiva di dati e la successiva divulgazione mediante diffusione del dataset di dati personali – come nel caso di specie – sono da considerare illecite;

CONSIDERATO che l'articolo 33 della Legge 171/2018 recita:

> *Art.33 - (Sicurezza del trattamento)*
>
> *1. Tenendo conto 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, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:*
>
> *a) la pseudonimizzazione e la cifratura dei dati personali;*
>
> *b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;*
>
> *c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;*
>
> *d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.*
>
> *2. 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.*
>
> *3. L'adesione a un codice di condotta approvato di cui all'articolo 41 o a un meccanismo di certificazione approvato di cui all'articolo 43 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al comma 1.*
>
> *4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richiedano norme speciali.*

CONSIDERATO, pertanto, che 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;

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

CONSIDERATO che le attività di sottrazione dei dati personali dalla piattaforma Facebook mediante la tecnica dello *scraping* o qualsiasi altra dinamica aggressiva, così come riconosciuto dalla stessa Facebook Ireland Ltd., evidenzia palesemente che detta società, invece, non abbia provveduto, così come previsto dall'art. 33 L. 171/2018, a mettere in atto misure tecniche e organizzative adeguate che fossero idonee quanto meno a ridurre il rischio derivante da attività illecite di sottrazione di dati personali mediante la tecnica dello *scraping* o altra idonea all'indebita acquisizione massiva, né ha fornito prova di aver adottato specifiche misure in tal senso pur avendo pubblicamente fornito specifiche rassicurazioni;

CONSIDERATO che, come descritto nei chiarimenti pervenuti a questa Autorità, entrambe le società Facebook Inc. e Facebook Ireland Ltd. avrebbero dovuto provvedere ad adottare le opportune misure ai sensi del citato articolo 33 L. 171/2018 proprio in quanto già disponevano di piena conoscenza e consapevolezza circa la sussistenza di concreti rischi di attacchi informatici in particolare (ma non solo) mediante la tecnica dello *scraping*;

CONSIDERATO che la Legge 171/2018 definisce la «diffusione» nei termini seguenti "*dare conoscenza dei dati personali a soggetti indeterminati, in qualunque forma, anche mediante la loro messa a disposizione o consultazione*" (art. 2, comma 1, lettera cc);

CONSIDERATO che, ai sensi della Legge 171/2018 "*la diffusione o qualsiasi altra forma di messa a disposizione di dati personali*" costituisce trattamento (articolo 2, comma 1, lettera b);

CONSIDERATO che, ai sensi della Legge 171/2018, devono essere rispettati i principi applicabili al trattamento dei dati personali (art. 4);

CONSIDERATO che, ai sensi della Legge 171/2018, "*il trattamento è lecito solo se e nella misura in cui ricorre almeno una*" delle condizioni indicate all'articolo 5;

CONSIDERATO, pertanto, che la sottrazione dei dati personali di utenti della piattaforma Facebook mediante la tecnica dello "*scraping*" è stata la evidente conseguenza della mancata adozione da parte di Facebook Ireland Ltd. e Facebook Inc. di opportune misure che fossero idonee ad evitare quanto accaduto;

CONSIDERATO che quanto accaduto e – si ribadisce – confermato dalla stessa Facebook Ireland Ltd., comporta la violazione dell'art. 33 della L. 171/2018 con conseguente applicazione della relativa sanzione amministrativa ai sensi dell'art. 72, comma 1, della stessa Legge 171/2018;

CONSIDERATO che le stesse Facebook Ireland Ltd. e Facebook Inc. non hanno comunicato a questa Autorità di essere comunque intervenute successivamente a quanto accaduto con l'adozione di specifiche misure e di ciò questa Autorità dovrà tenerne conto ai fini della valutazione degli elementi indicati all'art. 73, comma 2, con particolare riferimento alla lettera c);

CONSIDERATO che è da revocare il provvedimento numero 4/2021 adottato da questa Autorità Garante, limitatamente al capo b) dello stesso;

CONSIDERATO che per l'applicazione della sanzione, ai sensi dell'art. 73, comma 2, questa Autorità ha valutato i seguenti elementi:

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

Riguardo alla lettera a) "*la natura, la gravità e la durata della violazione tenendo in considerazione la natura, l'oggetto o la finalità del trattamento in questione nonché il numero di interessati lesi dal danno e il livello del danno da essi subito*", questa Autorità ritiene in ragione degli accertamenti eseguiti che, nell'ambito della propria giurisdizione, il numero di interessati coinvolti nella vicenda oggetto del presente provvedimento sia elevato e che quanto accaduto non solo sia estremamente grave, ma in assenza di specifiche informazioni da parte delle società Facebook Inc. e Facebook Ireland Ltd. è plausibile che ancora oggi sussista il rischio che possano essere compiute attività di sottrazione di dati personali con la tecnica dello scraping.

Riguardo alla lettera b) "*il carattere doloso o colposo della violazione*", questa Autorità ritiene che il comportamento delle società Facebook Inc. e Facebook Ireland Ltd. sia da qualificare come colposo, avendo le stesse omesso di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Riguardo alla lettera c) "*le misure adottate dal titolare del trattamento o dal responsabile del trattamento per attenuare il danno subito dagli interessati*", questa Autorità fa riferimento alla documentazione inviata dalla società Facebook Ireland Ltd. dalla quale, tuttavia, non emerge l'adozione di alcuna misura per attenuare il danno subito dagli interessati.

Riguardo alla lettera d) "*il grado di responsabilità del titolare del trattamento o del responsabile del trattamento tenendo conto delle misure tecniche e organizzative da essi messe in atto ai sensi degli articoli 27 e 33*", questa Autorità ritiene che sussista piena responsabilità, ciascuna per il rispettivo ruolo, delle società Facebook Inc. e Facebook Ireland Ltd. in relazione alla mancata adozione di misure tecniche e organizzative quanto meno per mitigare il rischio di attività di sottrazione di dati personali mediante la tecnica dello *scraping*.

Riguardo alla lettera f) "*il grado di cooperazione con l'Autorità Garante per la protezione dei dati personali al fine di porre rimedio alla violazione e attenuarne i possibili effetti negativi*", questa Autorità ha valutato positivamente il comportamento di Facebook Ireland Ltd. nell'invio di memorie e documenti, sebbene vada stigmatizzato il comportamento della società Facebook Inc. che, da quanto emerge dalla memoria presentata da Facebook Ireland Ltd, avrebbe non correttamente risposto *"all'Autorità a titolo di cortesia per confermare la sua posizione"*. Questa Autorità, non solo non ha ricevuto alcuna risposta da Facebook Inc. ma ritiene erroneo ed irrituale affermare di rispondere ad un provvedimento emesso (n. 4/2021) "*a titolo di cortesia*", posto che, ai sensi dell'art. 72, comma 2, lettera d) l'inosservanza di un ordine … dell'Autorità è considerata una violazione oggetto della massima sanzione prevista dalla legge.

Riguardo alla lettera g) "*le categorie di dati personali interessate dalla violazione*", questa Autorità evidenzia che si tratta prevalentemente di dati personali "comuni", con esclusione – all'esito dell'istruttoria – di categorie particolari di dati e di dati personali relativi a condanne penali e reati.

Relativamente alla lettera h) "*la maniera in cui l'Autorità Garante per la protezione dei dati personali ha preso conoscenza della violazione, in particolare se e in che misura il titolare del trattamento o il responsabile del trattamento ha notificato la violazione*", questa Autorità ha preso conoscenza della violazione a seguito di segnalazione da parte di cittadini sammarinesi,

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

benché le società Facebook Inc. e Facebook Ireland Ltd. fossero pienamente a conoscenza di quanto accaduto e delle relative conseguenze e ripercussioni e, pertanto, nulla hanno fatto anche solo per comunicare a questa Autorità gli eventi.

Relativamente alla lettera i) "*qualora siano stati precedentemente disposti provvedimenti di cui all'articolo 59, comma 2, nei confronti del titolare del trattamento o del responsabile del trattamento in questione relativamente allo stesso oggetto, il rispetto di tali provvedimenti*", questa Autorità rileva come fosse stato già emesso il provvedimento n. 4/2021 ma dei due destinatari - e precisamente Facebook Inc. e Facebook Ireland Ltd. – soltanto la società Facebook Ireland lo ha rispettato parzialmente limitandosi a fornire chiarimenti a questa Autorità, non adeguandosi a quanto previsto in via di urgenza mediante notifica ai destinatari ai sensi del punto b) del citato provvedimento. Facebook Inc., invece, non risulta abbia osservato il provvedimento emesso, neppure con l'invio di chiarimenti;

RAVVISATA, pertanto, la necessità, ai sensi dell'art. 59, comma 2, lettera d), della L. 171/2018, di ingiungere alla società "**Facebook Ireland Ltd**." in persona del legale rappresentante pro-tempore con sede legale in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 Ireland**" e alla società "**Facebook Inc.**" in persona del legale rappresentante pro-tempore con sede legale in **1 Hacker Way, Menlo Park, CA 94025, United States of America**, rispettivamente quali titolare del trattamento e responsabile del trattamento, di mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, provvedendo a ridurre al minimo il rischio derivante da attività di sottrazione dei dati personali anche con la tecnica dello "*scraping*".

RAVVISATA, inoltre, la necessità di disporre, ai sensi dell'art. 59, comma 2, lettera i), della L. 171/2018, a carico della società "**Facebook Ireland Ltd.**" in persona del legale rappresentante pro-tempore con sede legale in **4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 Ireland**" e della società "**Facebook Inc.**" in persona del legale rappresentante pro-tempore con sede legale in **1 Hacker Way, Menlo Park, CA 94025, United States of America**, rispettivamente quali titolare del trattamento e responsabile del trattamento, la sanzione prevista dall'art. 72, comma 1, L. 171/2018 per la violazione dell'art. 33 della medesima legge.

RITENUTO che la sanzione per la citata violazione dell'art. 33 della Legge 171/2018, in applicazione degli elementi indicati dall'art. 73, comma 2, e alla luce delle considerazioni svolte per la determinazione della sanzione, è quantificabile in misura congrua nell'importo di EURO 4.000.000 (EUR quattro milioni/00).

Pertanto, tutto ciò premesso e vista la documentazione in atti,

L'AUTORITÀ GARANTE

REVOCA

il proprio provvedimento numero 4/2021 unicamente riguardo al punto b) del dispositivo;

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

INGIUNGE

alla società "**Facebook Ireland Ltd.**" in persona del legale rappresentante pro-tempore, **con sede legale in 4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 – Ireland** e alla società "**Facebook Inc.**" in persona del legale rappresentante pro-tempore, **con sede legale in 1 Hacker Way, Menlo Park, CA 94025, United States of America**, rispettivamente quali titolare del trattamento e responsabile del trattamento, ai sensi dell'art. 59, comma 2, lettera d) della L. 171/2018, di mettere in atto immediatamente e senza indugio misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, provvedendo a ridurre al minimo il rischio derivante da attività di sottrazione dei dati personali, anche con la tecnica dello "*scraping*", e conseguentemente darne riscontro entro sette giorni a questa Autorità.

ORDINA

alla società "**Facebook Ireland Ltd.**" in persona del legale rappresentante pro-tempore, **con sede legale in - 4 Grand Canal – Square - Grand Canal Harbour - Dublin 2 - Ireland**" e alla società "**Facebook Inc.**" in persona del legale rappresentante pro-tempore, **con sede legale in 1 Hacker Way, Menlo Park, CA 94025, United States of America**, rispettivamente quali titolare del trattamento e responsabile del trattamento, ai sensi dell'art. 59, comma 2, lettera i) della L. 171/2018 e alla luce delle motivazioni tutte indicate nella premessa del presente provvedimento, il pagamento – con vincolo solidale tra loro – dell'importo di EURO 4.000.000 (EUR quattro milioni/00) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione;

INGIUNGE

alle predette società di pagare, in solido tra loro, la somma di euro 4.000.000 (quattro milioni), per il titolo di cui sopra, entro 30 (trenta) giorni dalla notificazione del presente provvedimento.

Il pagamento della presente ingiunzione dovrà essere effettuato mediante bonifico bancario:

- **IBAN SM 81 K03225 09800 000010006039**
- **Ecc.ma Camera Repubblica di San Marino**
- **Codice area 225**
- **Causale 592**
- **Indicare nel Bonifico il numero e la data del Provvedimento**

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm

Dell'avvenuto pagamento della sanzione amministrativa dovrà esserne data notizia all'Autorità Garante facendo pervenire l'attestazione del versamento all'Ufficio della medesima Autorità.

DISPONE

l'annotazione del presente provvedimento nel registro interno dell'Autorità e la pubblicazione del presente provvedimento sul sito web del Garante.

Ai sensi dell'art. 69 della Legge 171/2018, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso giurisdizionale ai sensi dell'articolo 70 della stessa Legge 171/2018.

L'opposizione non sospende l'esecuzione del provvedimento.

Si precisa che il mancato riscontro alla richiesta ai sensi dell'art. 59 è punito con la sanzione amministrativa di cui all'art. 72, comma 2 lettera d) della L. 171/2018.

San Marino, 6 luglio 2021

Il Dirigente dell'Ufficio **Il Collegio**

(Avv. Maria Sciarrino)

REPUBBLICA DI SAN MARINO

Scala Bonetti, 2 - 47890 Repubblica San Marino
T +378 (0549) 885476 – segreteria.ufficio@agpdp.sm
www.garanteprivacy.sm