GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

Provvedimento su data breach - 13 dicembre 2018 [9076378]

[doc. web n. 9076378]

Provvedimento su data breach - 13 dicembre 2018

Registro dei provvedimenti
n. 499 del 13 dicembre 2018

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016 (di seguito "Regolamento");

VISTO il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al regolamento (UE) 2016/679 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. 10 agosto 2018, n. 101, di seguito "Codice");

VISTA la notifica di violazione dei dati personali, ai sensi dell'art. 33 del Regolamento, trasmessa il 22 ottobre 2018 da UniCredit S.p.a., con la quale la stessa ha rappresentato all'Autorità che:

> i "sistemi di controllo interno hanno rilevato, in data 21 corr., dei tentativi, provenienti dall'esterno, di forzare il sistema di on-line banking [OMISSIS] per accedere ai rapporti dei clienti";
>
> "l'attacco è stato attuato attraverso l'utilizzo massivo di codici sequenziali per individuare quali di essi corrispondessero a REB code effettivamente esistenti (codice identificativo personale per l'accesso al sistema di on-line banking)";
>
> la violazione ha interessato "731.519 REB code, dei quali […] 6.859 sono quelli bloccati dalla banca perché era stata individuata la password";
>
> "alcuni dati personali di clienti [OMISSIS] erano visibili nel codice di risposta all'interrogazione, mentre non risulta che ci sia stato accesso a dati bancari dei clienti né che siano state effettuate operazioni";

VISTA la nota del 16 novembre 2018 con la quale UniCredit S.p.a. ha fornito un riscontro alla richiesta di informazioni formulata dall'Autorità in data 9 novembre 2018, precisando che:

> "in data 21 ottobre 2018 alle ore 16:17, a fronte delle prime analisi delle evidenze emerse dai […] tool di monitoraggio applicativo, sono stati intercettati un gran numero di tentativi di login verso il sito internet [OMISSIS];
>
> "le verifiche condotte hanno evidenziato una fase preliminare, volta verosimilmente a mettere a punto la tecnica di attacco, e condotta attraverso alcuni tentativi di accesso, a partire dal giorno 11 ottobre";
>
> "l'attacco, proveniente da rete anonimizzata (TOR), avente lo scopo di mascherare il reale indirizzo IP dell'attaccante, aveva l'obiettivo di enumerare una serie di clienti utilizzando una password fissa";
>
> "una condizione applicativa ha consentito la restituzione di informazioni anche in caso di autenticazione fallita, e quindi quando il REB Code inserito corrispondeva ad un cliente, indipendentemente dal fatto che la password fosse quella

corretta, venivano restituiti [OMISSIS]. Per i 6.859 clienti, che avevano una password “debole” utilizzata dagli attaccanti ([…]), è stata individuata anche la password”;

“l’immediata risposta tecnologica, avvenuta a seguito dell’identificazione che ha dato luogo all’incidente di sicurezza, è consistita nel bloccare le singole connessioni provenienti da rete anonimizzata (TOR) ed aventi le caratteristiche proprie dell’attacco informatico”; oltre a ciò, è stato “implementato un blocco quantitativo delle connessioni che oltrepassino una soglia critica per intervallo temporale definito ed un meccanismo informatico (captcha) finalizzato all’identificazione umana dell’utente che esegue la richiesta di Login, con lo scopo di bloccare connessioni automatiche o script informatici”;

“è in corso di implementazione un meccanismo per forzare l’utilizzo di password complesse da parte degli utenti, [OMISSIS];

PRESO ATTO che, nella citata nota del 16 novembre 2018, UniCredit S.p.a. ha altresì rappresentato che, “non ravvisando il “rischio elevato” di cui all’art. 34 del Regolamento ed in considerazione del numero elevato di interessati, ha pubblicato un comunicato sul proprio sito web” e che “ha, invece, avvisato quei clienti ai quali era stato necessario bloccare la password perché individuata dagli attaccanti, e che ammontavano a 6.859”;

CONSIDERATO che il predetto comunicato pubblico, rilasciato da UniCredit S.p.a. in data 22 ottobre 2018, laddove afferma che “per motivi di sicurezza le credenziali di circa 10.000 clienti sono state bloccate” e che “UniCredit si sta occupando di contattare i clienti interessati per procedere con il reset della password”, lascia intendere che la violazione dei dati personali ha riguardato solamente tali clienti;

RILEVATO che la violazione si è verificata in conseguenza di un attacco informatico al citato sito web [OMISSIS] che, ancorché prontamente arginato, ha permesso che fosse acquisita, da parte di soggetti terzi ignoti, una grande quantità di dati personali, anche a causa di una non meglio specificata “condizione applicativa” riscontrata nel medesimo sito web;

RILEVATO che UniCredit S.p.a., a fronte di una violazione che ha coinvolto complessivamente 731.519 interessati, ha provveduto a informare direttamente soltanto i 6.859 interessati per i quali era stata “individuata anche la password“ (rectius “PIN”), al dichiarato fine di “ridurre al più breve tempo possibile il periodo di durata del blocco della password” tempestivamente disposto per contenere gli effetti della violazione;

CONSIDERATO, tuttavia, che l’acquisizione dei citati dati personali [OMISSIS] è da ritenere già di per sé fonte di potenziale grave pregiudizio per gli interessati, in considerazione dell’abitudine diffusa tra gli utenti dei servizi online di utilizzare password o PIN facilmente memorizzabili e, dunque, della concreta possibilità che diversi interessati, ancorché UniCredit S.p.a. fornisca ai propri clienti “indicazioni utili su come creare e aggiornare il PIN” [OMISSIS], non abbiano tenuto conto di tali consigli [OMISSIS];

CONSIDERATO, inoltre, che [OMISSIS] costituiscono dati direttamente e univocamente identificativi che, alla luce delle tecnologie disponibili, possono essere utilizzati come chiavi di ricerca per individuare in rete l´interessato e conseguentemente accedere anche ad altre informazioni allo stesso riferibili (quali, a esempio, un recapito telefonico o un indirizzo di posta elettronica); tali informazioni potrebbero essere utilizzate per rivolgere agli interessati comunicazioni telefoniche o messaggi di phishing a scopo fraudolento, grazie alla conoscenza dei dati personali da parte dei soggetti terzi che hanno condotto l’attacco informatico;

VISTO l’art. 34, par. 1, del Regolamento che stabilisce che “quando la violazione dei dati personali è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, il titolare del trattamento comunica la violazione all'interessato senza ingiustificato ritardo”, fatti salvi i casi in cui tale comunicazione non è richiesta in quanto risulta essere soddisfatta una delle condizioni previste al par. 3 del medesimo articolo;

VISTI i considerando nn. 75 e 76 del Regolamento che suggeriscono che, di norma, nella valutazione dei rischi si dovrebbero prendere in considerazione tanto la probabilità quanto la gravità dei rischi per i diritti e le libertà degli interessati e che tali rischi dovrebbe essere determinati in base a una valutazione oggettiva;

VISTE 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, che hanno, fra l’altro, individuato i fattori da considerare nella valutazione del rischio – presentato da una violazione dei dati personali – per i diritti e le libertà delle persone fisiche: tipo di

violazione; natura, carattere sensibile e volume dei dati personali; facilità di identificazione delle persone fisiche; gravità delle conseguenze per le persone fisiche; caratteristiche particolari dell'interessato; caratteristiche particolari del titolare del trattamento dei dati; numero di persone fisiche interessate; altri aspetti generali;

RILEVATO l'elevato numero di persone fisiche a cui si riferiscono i dati personali oggetto di violazione, caratterizzati peraltro da particolare qualità ed esattezza in quanto acquisiti a seguito di identificazione certa del cliente secondo le procedure tipiche del settore bancario;

RILEVATA la facilità con cui è possibile identificare specifiche persone fisiche direttamente dai dati personali oggetto di violazione, senza che sia necessaria alcuna speciale ricerca per scoprire l'identità degli interessati;

RILEVATO che la violazione dei dati personali si è verificata nell'ambito di un attacco informatico di ampia portata, preceduto peraltro da "una fase preliminare, volta verosimilmente a mettere a punto la tecnica di attacco", finalizzato a individuare credenziali di autenticazione valide e, con molta probabilità, a utilizzare le stesse per successive attività illecite;

RILEVATO il particolare contesto (attività bancaria) nel quale il titolare del trattamento, tra i maggiori gruppi bancari operanti a livello europeo, effettua il trattamento di dati personali;

RILEVATE la gravità e la permanenza delle possibili conseguenze per le persone fisiche che potrebbero derivare dalla violazione, la quale può provocare il furto o l'usurpazione di identità, la perdita di controllo da parte degli interessati sui dati personali che li riguardano, anche idonei a rivelare la loro situazione economica, nonché l'utilizzo dei dati personali degli interessati a scopo di phishing;

CONSIDERATO che, alla luce di un complessivo esame delle circostanze portate all'attenzione dell'Autorità e delle considerazioni svolte, la violazione dei dati personali in argomento, diversamente dalla valutazione effettuata dal titolare del trattamento, è suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche, condizione per cui è richiesta la comunicazione agli interessati;

RITENUTO che, allo stato, non risulta essere soddisfatta nessuna delle condizioni di cui all'art. 34, par. 3, del Regolamento;

CONSIDERATA l'urgenza di comunicare la violazione dei dati personali agli interessati, fornendo loro indicazioni specifiche sulle misure che gli stessi possono adottare per proteggersi da eventuali conseguenze negative della violazione;

RAVVISATA, pertanto, la necessità di esercitare il potere dell'Autorità di ingiungere, ai sensi dell'art. 58, par. 2, lett. e), del Regolamento, al titolare del trattamento di comunicare agli interessati la violazione dei dati personali;

RITENUTO necessario disporre che la predetta comunicazione sia effettuata senza ritardo e comunque entro trenta giorni dalla data di ricezione del presente provvedimento, riservandosi ogni altra determinazione all'esito della definizione dell'istruttoria avviata sul caso;

TENUTO CONTO che, ai sensi dell'art. 83, par. 6, del Regolamento, "l'inosservanza di un ordine da parte dell'autorità di controllo di cui all'articolo 58, paragrafo 2, è soggetta a sanzioni amministrative pecuniarie fino a 20 000 000 EUR, o per le imprese, fino al 4 % del fatturato mondiale totale annuo dell'esercizio precedente, se superiore";

RITENUTO, altresì, ai sensi dell'art. 58, par. 1, lett. a), del Regolamento e art. 157 del Codice, di ingiungere a UniCredit S.p.a. di fornire all'Autorità, entro i successivi sette giorni, un riscontro adeguatamente documentato in merito alle iniziative intraprese al fine di comunicare la violazione agli interessati, nonché alle eventuali ulteriori misure adottate per attenuare i possibili effetti negativi della violazione nei confronti degli interessati;

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 del 28 giugno 2000;

RELATORE la dott.ssa Augusta Iannini;

TUTTO CIÒ PREMESSO, IL GARANTE

1) ai sensi dell'art. 58, par. 2, lett. e), del Regolamento, ingiunge a UniCredit S.p.a. di comunicare, senza ritardo e comunque entro trenta giorni dalla data di ricezione del presente provvedimento, la violazione dei dati personali a tutti gli interessati che non siano già stati destinatari della comunicazione di avvenuta violazione, fornendo almeno le informazioni di cui all'art. 34, par. 2, del Regolamento;

2) ai sensi degli artt. 58, par. 1, lett. a), del Regolamento e 157 del Codice, ingiunge altresì a UniCredit S.p.a. di fornire all'Autorità, entro i successivi sette giorni, un riscontro adeguatamente documentato in merito alle iniziative intraprese al fine di dare attuazione a quanto disposto al punto 1) nonché alle eventuali ulteriori misure adottate per attenuare i possibili effetti negativi della violazione nei confronti degli interessati. Si ricorda che il mancato riscontro alla presente richiesta è punito con la sanzione amministrativa ai sensi del combinato disposto di cui agli artt. 83, par. 5, lett. e), del Regolamento e 166 del Codice.

Ai sensi dell'art. 78 del Regolamento, nonché degli artt. 152 del Codice e 10 del d.lgs. 1° settembre 2011, n. 150, avverso il presente provvedimento può essere proposta opposizione all'autorità giudiziaria ordinaria, con ricorso depositato al tribunale ordinario del luogo ove ha la residenza il titolare del trattamento dei dati, entro il termine di trenta giorni dalla data di comunicazione del provvedimento stesso, ovvero di sessanta giorni se il ricorrente risiede all'estero.

Roma, 13 dicembre 2018

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia