Provvedimento dell'8 febbraio 2024 [9991020]

VEDI ANCHE Newsletter del 7 marzo 2024

[doc. web n. 9991020]

Provvedimento dell'8 febbraio 2024

Registro dei provvedimenti
n. 65 dell'8 febbbraio 2024

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, l'avv. Guido Scorza e il dott. Agostino Ghiglia, componenti, e il dott. Claudio Filippi, vice 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 violazione di dati personali notificata all'Autorità il 22 ottobre 2018, ai sensi dell'art. 33 del Regolamento, da UniCredit S.p.a. relativa ad un attacco informatico al sistema di on-line banking per il canale web mobile;

ESAMINATA la documentazione in atti;

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

RELATORE il dott. Agostino Ghiglia;

PREMESSO

1. La violazione di dati personali e l'attività istruttoria.

1.1. L'istruttoria nei confronti di UniCredit S.p.a.

In data 22 ottobre 2018, UniCredit S.p.a. (di seguito "UniCredit" o "la Banca") ha notificato al Garante, ai sensi dell'art. 33 del Regolamento, la violazione di dati personali verificatasi a seguito di un attacco informatico al sistema di on-line banking per il canale web mobile (di seguito "Portale di mobile banking") che ha determinato l'acquisizione illecita di alcuni dati personali di clienti (in particolare, nome, cognome, codice fiscale e codice identificativo interno della banca, con esclusione dei dati bancari degli stessi).

In particolare la Banca ha rappresentato che i primi tentativi di accesso indebito sono stati

effettuati nel periodo compreso tra l'11 e il 20 ottobre 2018 e che l'attacco informatico si è realizzato massivamente il 21 ottobre 2018, data in cui la Banca, avendo rilevato un gran numero di tentativi di login verso il sito di mobile banking, ha immediatamente provveduto alla notifica di cui dell'art. 33 del Regolamento, specificando che:

> "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 (solo nome, cognome, codice fiscale e codice identificativo della banca) 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".

Con successiva nota del 16 novembre 2018, la Banca, in riscontro a una richiesta di informazioni formulata dall'Ufficio in data 9 novembre 2018, ha altresì precisato che:

> "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 nome e cognome, codice fiscale e NDG, che è un codice identificativo interno, assegnato a ciascun cliente al momento in cui viene inserito nei […] sistemi informatici [di UniCredit S.p.a.]. 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, che sarà disponibile in produzione a decorrere dal 23 novembre prossimo e che con successivi rilasci coprirà l'intera clientela della banca";
>
> nel caso de quo la Banca, "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" ed "ha, invece, avvisato quei clienti ai quali era stato necessario bloccare la password perché individuata dagli attaccanti, e che ammontavano a 6.859".

Alla luce di un complessivo esame delle circostanze rappresentate dalla Banca, l'Autorità ha ritenuto che la violazione dei dati personali in argomento, diversamente dalla valutazione effettuata dalla Banca, fosse suscettibile di presentare un rischio elevato per i diritti e le libertà delle persone fisiche (condizione per cui è richiesta la comunicazione agli interessati) e, pertanto, con provvedimento n. 499 del 13 dicembre 2018 (doc. web n. 9076378) ha ingiunto a UniCredit, ai sensi dell'art. 58, par. 2, lett. e), del Regolamento, di comunicare la violazione dei dati personali a

tutti gli interessati che non fossero già stati destinatari della comunicazione medesima, invitandola a fornire un riscontro adeguatamente motivato in merito alle iniziative a tal fine assunte nonché in ordine alle misure adottate per attenuare gli effetti negativi della violazione dei dati personali nei confronti degli interessati.

Con nota del 25 gennaio 2019, la Banca, nel descrivere le modalità e le tempistiche con le quali ha provveduto a dare attuazione alle prescrizioni impartite con il citato provvedimento n. 499, ha precisato di avere predisposto comunicazioni differenziate per i clienti e per gli ex-clienti (di cui ha allegato copia) il cui contenuto è risultato conforme a quanto previsto dall'art. 34, par. 2, del Regolamento.

Con la medesima nota, UniCredit ha altresì comunicato che, a seguito delle ulteriori analisi effettuate al fine di individuare gli interessati a cui inviare la comunicazione dell'avvenuta violazione, è emerso che il numero dei soggetti coinvolti era superiore a quello inizialmente individuato (per un numero complessivo di 777.765 clienti ed ex-clienti); la Banca ha anche precisato di avere introdotto un meccanismo di enforcement delle password in uso agli utenti, dapprima diretto ai clienti coinvolti nella violazione dei dati personali e progressivamente esteso all'intera clientela entro il mese di marzo 2019.

All'esito di successivi approfondimenti (cfr. richiesta di informazioni del 1° febbraio e 12 aprile 2019), la Banca ha fornito ulteriori elementi di precisazione (cfr. note del 26 febbraio e 3 maggio 2019) in base ai quali, anche alla luce della documentazione acquisita agli atti, è risultato che:

a) al momento della violazione dei dati personali, per quanto attiene alla sicurezza del trattamento nell'ambito del Portale di mobile banking, le misure tecniche e organizzative di cui all'art. 32 del Regolamento consistevano in:

1. "login protetto da username e password consegnati separatamente al cliente in filiale;

2. blocco dell'account dopo l'inserimento di tre password errate;

3. blocco di credenziali individuate in data leak online da parte dei […] servizi di intelligence/antifrode;

4. possibilità per il cliente di aderire ad un servizio via sms (SMS premium) di notifica di attività quali gli accessi online, le variazioni di Pin e di dati personali effettuati da Banca via internet;

5. protezione delle transazioni e delle attività sensibili (es. modifica dati personali) attraverso la richiesta di un ulteriore One Time Password (OTP);

6. analisi comportamentale e monitoraggio delle transazioni per individuare frodi a scapito dei clienti;

7. esecuzione di VA/PT periodici […] sull'infrastruttura e l'applicazione di internet/banking;

8. web application firewall (WAF) a protezione di eventuali attacchi web (es. sql injection)" (cfr. nota del 26 febbraio 2019, pp.1-2);

b) nel periodo compreso "tra il 1° ottobre 2018 ed il 22 ottobre 2018 era in corso un Penetration Test sul sistema Mobile Site (sito e APP per dispositivi Mobili)" la cui esecuzione era stata affidata alla società NTT Data Italia S.P.A. (di seguito "NTT Data") sulla base di un agreement stipulato il 5 giugno 2017 con UniCredit Business Integrated Solutions S.c.p.a.

(ora UniCredit Services S.c.p.a., di seguito “UBIS”) avente ad oggetto la fornitura di servizi di “Banking Application Penetration Test & Vulnerability Assessment”. Nell’ambito di tale agreement NTT Data era stata designata da UniCredit quale responsabile del trattamento – ai sensi dell’allora vigente art. 29 del Codice – ricevendo dalla stessa precise istruzioni cui attenersi, tra le quali:

- il divieto espresso di affidare a terze parti l’esecuzione, parziale o totale, delle attività di vulnerability assessment e penetration testing (cfr. par. 14 dell’agreement);
- laddove, per l’esecuzione di determinate attività, risulti necessario il ricorso a una terza parte, l’obbligo di informarne il titolare perché lo stesso provveda, dopo averne valutato l’esperienza, le capacità e l’affidabilità, alla sua designazione quale responsabile del trattamento;
- l’obbligo, in caso di rilevamento di vulnerabilità con gravità di livello critical o high, di informare immediatamente il titolare al fine di consentire alla stessa una rapida rimozione di tali vulnerabilità (cfr. Annex 3 dell’agreement);

c) NTT Data, nell’esecuzione delle attività di cui sopra, ha ritenuto di doversi avvalere della collaborazione di un altro soggetto, Truel IT S.r.l. (di seguito “Truel IT”), che, con atto di nomina del 17 settembre 2018, è stata designata quale sub-responsabile del trattamento, in assenza tuttavia di preventiva autorizzazione scritta da parte di UniCredit;

d) in data 19 ottobre 2018 NTT Data è venuta a conoscenza di due vulnerabilità con gravità di livello high (“User Data disclosure” e “Lack of Reverse Bruteforce Protection”) per il tramite di Truel IT – che gli ha trasmesso la bozza di report contenente gli esiti delle attività di Vulnerability Assessment e Penetration Testing – ed ha informato UniCredit solo in data 22 ottobre 2018.

1.2. L’istruttoria nei confronti di NTT Data Italia S.p.a..

Con nota del 15 maggio 2019, l’Autorità ha formulato una richiesta di informazioni nei confronti di NTT Data che, con comunicazioni del 24 e 27 maggio 2019, ha precisato che “le attività di Penetration Test e di Vulnerability Assessment sono state condotte dal 1 al 26 ottobre 2018 secondo la seguente tempistica:

- l’esecuzione dei test […] è stata effettuata dall’1 al 12 ottobre 2018;
- l’analisi degli esiti, la rimozione dei falsi positivi, la valutazione e classificazione delle vulnerabilità, la redazione del report tecnico ed invio del medesimo report in bozza al cliente dal 13 al 22 ottobre 2018;
- ulteriori affinamenti al documento tecnico circa le vulnerabilità rilevate dal 22 al 26 ottobre 2018, con invio del report definitivo al cliente in data 26 ottobre 2018”.

NTT Data ha fornito, altresì, copia dei report tecnici contenenti gli esiti delle citate attività di vulnerability assessment e penetration testing (sia nella versione bozza che in quella definitiva) nei quali sono illustrate dieci vulnerabilità rilevate da Truel IT, comprese due vulnerabilità con gravità di livello elevato (high):

- la prima vulnerabilità, di tipo “User Data Disclosure”, consentiva di enumerare tutte le User ID valide (composte da 8 cifre decimali) per l’accesso al Portale di mobile banking e di acquisire alcuni dati personali (quali il nome, il cognome e il codice fiscale) associati a tali User ID anche senza conoscere il relativo PIN (composto da 8 cifre decimali);

la seconda vulnerabilità, di tipo “Lack of Reverse Bruteforce Protection”, consentiva di effettuare un numero illimitato di tentativi di autenticazione al Portale di mobile banking con User ID sempre diverse, senza essere bloccato; in tale scenario, un attaccante poteva tentare di individuare coppie di User ID / PIN valide, provando ad esempio PIN particolarmente “deboli” come “00000000” o “12345678”.

NTT Data ha inoltre dichiarato di essere “venuta a conoscenza della vulnerabilità “User Data disclosure” in data 19 ottobre 2018 con l’invio della bozza di report da parte di Truel IT S.r.l.” che, dal canto suo, aveva identificato le due vulnerabilità anzi descritte rispettivamente il 10 ottobre 2018 (la prima) e il giorno immediatamente successivo (la seconda); nella medesima nota NTT Data ha altresì evidenziato come “tipicamente le potenziali vulnerabilità di un sistema sono rilevate nel corso delle attività di Penetration Test” e che “tale rilevazione, tuttavia, richiede, ai fini di una valutazione del rischio della stessa e, quindi, di una tempestiva comunicazione al cliente, l’esecuzione di una ulteriore attività di analisi (eliminazione di falsi positivi) e classificazione (high, medium and low) e remediation suggerite”.

Per questa ragione la stessa ha effettuato, “come da prassi, una propria analisi dei dati ricevuti ed una valutazione ulteriore delle classificazioni di tutte le 10 vulnerabilità rilevate” e, solo a conclusione, ha provveduto a darne comunicazione a UniCredit “in data 22 ottobre 2018 ore 10:00 CEST”.

Da ultimo, NTT Data ha precisato che “la rilevazione […] delle vulnerabilità in parola non poteva determinare e non ha determinato la conoscenza/rilevazione da parte di NTT DATA Italia medesima anche della violazione dei dati personali”.

2. L’avvio del procedimento per l’adozione dei provvedimenti correttivi e sanzionatori e le deduzioni di UniCredit S.p.a.

All’esito degli approfondimenti istruttori sopra descritti, caratterizzati da una elevata complessità dei profili di natura tecnologica (cfr. relazione tecnica del 10 dicembre 2019), l’Ufficio ha evidenziato le criticità riscontrate, in ordine all’adempimento, da parte del titolare e del responsabile del trattamento, degli obblighi in materia di protezione dei dati personali.

In particolare, dall’analisi della documentazione acquisita agli atti e delle dichiarazioni rese dal titolare del trattamento (di cui lo stesso 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”) è stato accertato che le misure tecniche e organizzative di cui all’art. 32 del Regolamento adottate da UniCredit nell’ambito del Portale di mobile banking (v. par. 1.1) presentavano le seguenti criticità:

il portale di mobile banking, a causa di una c.d. “condizione applicativa”, rendeva disponibili all’interno del codice HTML restituito, anche in caso di tentativi di autenticazione non riusciti, alcuni dati personali (nome, cognome, codice fiscale, NDG) di clienti ed ex-clienti di UniCredit che, pertanto, erano suscettibili di essere liberamente consultati e acquisiti da chiunque;

non era stato previsto, nell’ambito della procedura di autenticazione informatica degli utenti del predetto portale, alcun meccanismo in grado di contrastare efficacemente attacchi di tipo brute force condotti mediante l’utilizzo dei c.d. bot (programmi informatici che accedono ai siti web attraverso lo stesso canale utilizzato dagli utenti umani simulandone l’operatività).

Tenuto conto di quanto sopra, l’Ufficio, con nota del 5 febbraio 2020, ha notificato a UniCredit S.p.a., titolare del trattamento, l’avvio del procedimento per l’adozione dei provvedimenti di cui agli artt. 58, par. 2, e 83 del Regolamento, in conformità a quanto previsto dall’art. 166, comma 5, del

Codice, in relazione alla presunta violazione del principio di integrità e riservatezza e degli obblighi di sicurezza del trattamento di cui agli artt. 5, par. 1, lett. f), e 32, parr. 1 e 2, del Regolamento.

Con la medesima nota, UniCredit è stata invitata a produrre 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, legge n. 689 del 24 novembre 1981).

In data 5 marzo 2020, la Banca ha fatto pervenire un'articolata memoria difensiva (corredata di allegati), che qui integralmente si richiama, con la quale, nel formulare richiesta di audizione, ha chiesto all'Autorità di valutare "come alla luce delle condotte […] prima e immediatamente dopo il data breach, […] un'eventuale sanzione appar[irebbe] del tutto ingiustificata", tanto più che non "è stata fornita alcuna prova di danni eventualmente subiti dagli Interessati i cui dati personali sono stati oggetto della violazione".

In particolare, la Banca ha evidenziato che:

a) "in data 21 ottobre 2018 i sistemi di controllo interno di UniCredit hanno rilevato un attacco informatico perpetrato da soggetti terzi non identificati (gli "Hacker") […] che ha determinato la possibilità di visualizzare, in relazione ad alcuni utenti, alcuni dati […] senza che ci sia stata alcuna evidenza dell'effettiva visualizzazione, né tanto meno della raccolta, estrazione o copia degli stessi da parte degli hacker"; […] "a seguito dell'attacco la Società ha prontamente provveduto ad adottare le misure in grado di bloccare la violazione dei dati personali e il giorno successivo ha inviato apposita notifica del data breach al Garante, fornendo dettagli sull'accaduto e informando il Garante di essere in procinto di comunicare la violazione dei dati personali agli Interessati il cui account era stato bloccato"; il successivo 16 novembre 2018, la Banca ha fornito ulteriori dettagli circa la violazione occorsa nonché in ordine alle misure adottate al fine di mitigare il rischio per gli Interessati;

b) "UniCredit rappresenta uno tra i maggiori gruppi bancari operanti a livello europeo. […] Alla luce della posizione di rilevanza ricoperta e nell'ottica di una gestione societaria responsabile, la tutela e la sicurezza dei dati dei propri clienti sono per UniCredit una assoluta priorità […] come provato dalla circostanza che nell'ambito del recente piano industriale Transform 2019 il gruppo ha investito 2,3 miliardi di euro per migliorare ulteriormente e rendere sempre più sicuri i propri sistemi informatici […]. Tuttavia l'esposizione a rischi del sistema finanziario è tale che anche le misure di sicurezza più avanzate non valgono ad escludere ogni e qualsiasi ipotesi di attacco informatico sempre e comunque. In particolare, come ampiamente rappresentato dalle più autorevoli fonti in materia di sicurezza cibernetica, nel 2018 si è registrato un incremento notevole in termini di evoluzione delle minacce "cyber" e dei relativi impatti sia dal punto di vista quantitativo che qualitativo […]. Le statistiche mostrano inoltre come il 2018 sia stato l'anno in cui si è registrata una sensibile evoluzione legata agli attacchi di tipo APT (Advanced Persistent Threat). Tali attacchi, mirati a soggetti specifici, diventano sempre più evoluti e sofisticati e utilizzano in maniera estensiva tecniche massive che portano inevitabilmente a manifestare le debolezze di sistema. Quindi, anche i sistemi di sicurezza più avanzati, nonostante siano costantemente aggiornati, non sono immuni dal rischio di essere oggetto di attacchi perché la sofisticatezza e l'evoluzione repentina delle modalità in cui gli stessi sono eseguiti rende di fatto impossibile l'adozione di misure che siano in grado di proteggere da ogni possibile tipologia di cyber attacco. Ciò è assolutamente rilevante nel caso di specie: il verificarsi di un data breach non prova di per sé la violazione tout court del principio di integrità e riservatezza ex art. 5, par. 1 lett. f) del Regolamento, né la mancata adozione delle misure di sicurezza adeguate al rischio ai sensi dell'art. 32 del Regolamento. Come rilevato da autorevole dottrina infatti, la garanzia di adeguata sicurezza può essere interpretata non soltanto come una misura preventiva rispetto ad eventuali eventi dannosi, ma anche come intervento ex post per sanare le anomalie riscontrate. Nel seguito si dimostrerà infatti che le misure adottate da UniCredit all'epoca in cui si è verificato il data breach, insieme con quelle adottate prontamente a seguito del suo verificarsi, fossero adeguate al

livello di rischio e allo stato dell'arte al momento del data breach e quindi conformi con quanto previsto dalla normativa in materia di protezione dei dati personali. Al contrario, non è possibile contestare rispetto ad eventi accaduti nel 2018, la mancanza di misure di sicurezza che sarebbero adeguate nel 2020 perché nel settore della sicurezza informatica due anni di differenza rappresentano un cambiamento enorme degli standard applicabili";

c) quanto alle "criticità" rilevate dal Garante, è stato ulteriormente precisato (anche tramite allegazioni documentali) che "al tempo dell'attacco, UniCredit adottava le seguenti misure di sicurezza:

> blocco automatico dell'account utente dopo l'inserimento di quattro password errate;
>
> adozione di log-in protetto tramite credenziali di accesso consegnate separatamente agli utenti in filiale;
>
> blocco delle credenziali compromesse individuate in data leak online da parte dei servizi di intelligence/antifrode;
>
> disponibilità di un servizio di notifica via SMS di attività quali gli accessi online al proprio account, le variazioni del PIN e dei dati personali effettuate dalla banca o via Internet;
>
> protezione delle transazioni e delle attività sensibili quali modifiche dei dati personali tramite doppio meccanismo di autenticazione (One Time Password);
>
> adozione di tool di monitoraggio per individuare tentativi di frodi a scapito dei clienti;
>
> esecuzione di vulnerability assessment e penetration test ("VA-PT") periodici, con cadenza almeno annuale, sugli asset individuati come critici, ivi incluse l'infrastruttura e le applicazioni di internet banking tramite terze parti certificate leader di mercato, a rotazione in modo da garantire la massima efficacia e imparzialità dei test e seguendo una metodologia per lo svolgimento dei test di valutazione della sicurezza degli asset informatici […] che richiedeva il rispetto di determinati standard internazionali nella loro esecuzione, quali lo standard OWASP, riconosciuto come stato dell'arte di settore dal Laboratorio Nazionale di Cybersecurity, e l'effettuazione di scan dell'infrastruttura IT e di ulteriori tecniche di test in caso di VA-PT basati su potenziali vulnerabilità individuate, quali ad esempio password cracking e social engineering;
>
> esecuzione di vulnerability assessment periodici attraverso tool di scansione automatica sugli asset esposti su Internet, Extranet e Intranet, ed elaborazione dei relativi report;
>
> svolgimento di test di vulnerabilità sui sistemi di pagamento attraverso red team ad hoc;
>
> implementazione di web application firewall a protezione di eventuali attacchi web, quali ad esempio iniezioni di codice SQL.

In aggiunta a quanto sopra […] i sistemi di fraud prevention e fraud detection adottati al tempo dei fatti, erano statisticamente tra i più performanti ed efficaci del mercato, con una percentuale di frodi sventate pari al 98,6% (rispetto al 96,5% del mercato) come acclarato dal CERT Finanziario Italiano […]. Oltretutto ogni vulnerabilità informatica identificata veniva gestita in conformità con una procedura (Security Vulnerability Management […]) che prevedeva l'osservanza di processi certificati ai sensi dello standard internazionale ISAE 3402 e l'utilizzo del sistema di controllo dei rischi di cui allo standard internazionale ISO 27001. Inoltre, nell'ottobre 2017, UniCredit aveva già introdotto un sistema di raccolta e gestione delle vulnerabilità individuate, analogo a quello utilizzato dalle funzioni di audit, con un costante presidio del rischio svolto dalle diverse funzioni aziendali preposte. Inoltre, nel 2018 con l'inizio della piena applicabilità del Regolamento,

UniCredit ha ulteriormente rafforzato le proprie procedure introducendo un obbligo di segnalazione immediata in caso di vulnerabilità High e Critical individuate, con una gestione delle evidenze in ambito di security incident per cui, nei casi più gravi, al fine di salvaguardare i dati e le infrastrutture, era prevista la chiusura preventiva del sistema coinvolto fino alla risoluzione della problematica individuata. Quindi il sistema di misure di sicurezza già adottato da UniCredit al tempo del data breach consisteva in una serie di misure preventive volte ad evitare le violazioni e in una serie di controlli volti ad identificare eventuali vulnerabilità dei sistemi informatici aziendali che, a giudizio della banca, rappresenta l'unico approccio in grado di ridurre effettivamente il rischio di attacchi informatici".

La Banca ha anche rappresentato che l'adeguatezza delle misure preventive rispetto allo stato dell'arte al momento del verificarsi della violazione dei dati personali è stata "confermata dal report tecnico sulle misure di sicurezza […] prodotto dalla società Reply S.r.l, azienda leader nel settore della consulenza in materia di sicurezza informatica […]" secondo la quale le stesse misure erano "sostanzialmente in linea con quanto comunemente praticato da altri istituti di credito per la protezione delle funzionalità di login. Il report evidenzia infatti che soluzioni quali la two factor authentication o il CAPTCHA su funzionalità di login non erano al momento della violazione adottate dalla maggior parte degli istituti di credito Italiani a protezione delle procedure di login. La two factor authentication è diventata una modalità di autenticazione standardizzata e riconosciuta solamente a partire dal 14 settembre 2019 a seguito dell'entrata in vigore della Direttiva europea sui Servizi di Pagamento (PSD2), ma – in previsione dell'obbligo normativo – UniCredit vi stava già lavorando dal luglio 2017, con effettivo rollout avvenuto tra marzo e maggio 2019 e quindi ben 4 mesi prima dell'entrata in vigore dell'obbligo di legge. Rispetto al CAPTCHA, lo stesso non avrebbe comunque permesso di limitare del tutto il rischio dell'attacco in quanto, come dimostrato dai ricercatori della Columbia University, persino tali sistemi possono essere aggirati";

d) la Banca ha quindi evidenziato come "lo svolgimento di controlli volti a identificare eventuali vulnerabilità è l'unica soluzione che consente di minimizzare il rischio di attacchi informatici tenendo conto che non esistono software senza bachi. I bachi applicativi fanno parte del ciclo di vita naturale dello sviluppo informatico e la loro insorgenza è proporzionata al livello di complessità di struttura dell'applicativo. Infatti il processo di collaudo degli applicativi per l'individuazione dei bachi è una attività dinamica che si protrae nel tempo ed è legata all'evoluzione del software, in relazione al quale potrebbero insorgere dei bachi anche a causa dell'utilizzo da parte degli utenti". Ne deriva che "La presenza di un baco applicativo nel Portale non integra di per sé una violazione del principio di integrità e riservatezza e non dimostra l'assenza, né tantomeno la prova dell'inadeguatezza delle misure di sicurezza adottate da UniCredit perché la presenza di bachi è una caratteristica intrinseca di qualsiasi software e l'unico modo per identificarli e correggerli è di svolgere dei test come quelli eseguiti da UniCredit. A riprova della consapevolezza circa l'importanza dei controlli, UniCredit ha investito in attività di vulnerability assessment e penetration test oltre 2 milioni di euro nel triennio 2017- 2019, con l'effettuazione di oltre 500 penetration test e 1000 vulnerability assessment, mentre per il 2020 è in piano un investimento di oltre 3,8 milioni di euro. La correttezza di questo approccio è confermata dal fatto che la condizione applicativa da cui è nato il data breach è stata individuata durante i controlli avvenuti nel 2018, ma il motivo per cui il data breach non è stata bloccato è dovuto alla ritardata notificata della condizione applicativa a UniCredit da parte di NTT DATA Italia S.p.A. che ha svolto i test". In particolare, "NTT Data – pur avendo ricevuto incarico da parte di UniCredit durante il mese di settembre 2018 di eseguire un penetration test ed un vulnerability assessment sul Portale – e pur essendo vincolata ad informare immediatamente UniCredit in caso di rilevamento di vulnerabilità con gravità di livello critical o high, ha agito in violazione dei propri obblighi, come espressamente disciplinati nel contratto di servizi già prodotto al Garante […], omettendo di trasmettere immediatamente la notizia circa la rilevazione della condizione applicativa, nonostante NTT Data avesse già classificato tale vulnerabilità come high in data 16 ottobre 2018 […] e quindi ben 5 giorni prima del verificarsi dell'attacco. In 5 giorni, UniCredit

avrebbe avuto tutto il tempo di adottare le misure urgenti correttive volte ad evitare la violazione dei dati personali". Quindi, "[…] UniCredit ha adottato le misure preventive e i controlli che erano in linea con lo stato dell'arte al momento del data breach, ma è stata vittima della condotta negligente di NTT Data per la quale non può essere considerata responsabile";

e) per quanto concerne la condizione applicativa del Portale (cfr. par. 2, punto 1), la stessa, "a differenza di quanto sostenuto dal Garante, non rendeva i dati "suscettibili di essere liberamente consultati e acquisiti da chiunque". Il baco infatti non era visibile a chiunque provasse ad autenticarsi sul Portale ed è stato individuato solo a seguito di una fase preliminare in cui gli Hacker hanno messo a punto la tecnica d'attacco attraverso ripetuti complessi tentativi di accesso. La modalità di attacco adottata dagli Hacker si connotava di un elevato grado di sofisticatezza […] in quanto:

> i tentativi di accesso sono stati condotti utilizzando appositi software volti a prevenire l'intercettazione della provenienza delle comunicazioni attraverso l'inibizione dell'analisi del traffico in entrata. Tali software permettono infatti di instradare le comunicazioni (i.e. i tentativi di accesso al Portale) by-passando il normale transito da client a server e dirottando la connessione su un circuito virtuale di router crittografati a strati (c.d. onion router). L'uso di tale tecnica permette il traffico anonimo in uscita e la realizzazione di servizi anonimi, oltretutto la crittografia garantisce la c.d. perfect forward secrecy, ossia la totale riservatezza delle comunicazioni anche in caso di compromissione delle stesse;
>
> la quantità di tentativi di accesso posti in essere a partire dal 16 ottobre 2018 è stata appositamente calibrata per non oltrepassare le ordinarie soglie di traffico ed evitare di essere intercettata dai sistemi di controllo di UniCredit. Gli attaccanti infatti effettuavano solo tentativi di accesso diretti al "form" di login della pagina, evitando di effettuare il download degli oggetti che di norma costituiscono la pagina web (es. immagine css ecc.) riducendo di molto il traffico complessivo veicolato dalle connessioni malevole;
>
> soltanto dopo aver individuato il baco del Portale attraverso una strategia di bug hunting, gli Hacker hanno lanciato un attacco massivo, utilizzando specifici software in grado di consentire l'adozione del metodo reverse brute force per effettuare tentativi di accesso di cui però solo una minima percentuale (i.e. meno del 16%) ha permesso la potenziale esposizione di dati dei clienti;
>
> gli Hacker hanno inoltre inserito appositi caratteri sbagliati nelle richieste di accesso inoltrate per evitare di essere intercettati dal tool di monitoraggio applicativo, che ha in ogni caso portato alla rilevazione degli accessi;
>
> le tempistiche scelte denotano una particolare intenzione malevola e confermano l'abitualità di tali comportamenti da parte degli Hacker; l'attacco massivo è stato infatti condotto durante un giorno festivo (domenica 21 ottobre 2018) peraltro a cominciare dalle ore dalle 06:15 del mattino. Pertanto, la portata dell'attacco, le tempistiche scelte, i software utilizzati e le tecniche adottate denotano chiaramente che gli Hacker erano a disposizione di ingenti risorse computazionali oltre ad essere dotati di un livello molto avanzato di competenze informatiche specialistiche. Tali condizioni non sono affatto comuni e appare quindi evidente che […] il baco non permetteva un accesso libero ed indiscriminato ai dati dei clienti di UniCredit, bensì tale azione non poteva prescindere dalla disponibilità di competenze e risorse complesse e avanzate. Questa conclusione è confermata dal report di Reply secondo cui "la problematica di sicurezza rientra in una casistica di vulnerabilità difficilmente individuabili da strumenti automatici, e che vengono tipicamente individuate tramite analisi manuali condotte da personale specializzato nell'analisi di sicurezza delle applicazioni web";

f) in ordine all'ulteriore criticità rilevata dall'Autorità (cfr. par. 2, punto 2), la Banca ha evidenziato

che, “già prima del data breach, aveva adottato un sistema di prevenzione da attacchi di tipo brute force nell’ambito della procedura di autenticazione informatica degli utenti del Portale, i.e. relativamente al processo di inserimento della password per effettuare l’autenticazione. Il sistema garantiva infatti una efficace protezione da attacchi condotti da c.d. bot automatici in quanto, dopo quattro tentativi di accesso errati, l’utenza veniva bloccata e l’attacco impedito. Pertanto – a differenza di quanto ritenuto dal Garante – le misure adottate da UniCredit consentivano di proteggere i sistemi informatici aziendali da attacchi di brute force. La tipologia di attacco condotta contro il Portale non è qualificabile come brute force, che come sopra dimostrato, riferendosi all’autenticazione, era adeguatamente protetto, ma più precisamente come “reverse brute force” in quanto gli Hacker non hanno cercato di individuare la password degli utenti provando il maggior numero di combinazioni possibili, ma hanno tuttalpiù cercato di enumerare gli username di autenticazione degli utenti utilizzando una password fissa banale (12*****89). In tale contesto, l’adozione di ulteriori sistemi di contrasto utili a limitare impedire l’accesso, o tentativi di accesso, provenienti dal medesimo indirizzo IP non sarebbero risultati né efficaci né praticabili considerando in particolare le caratteristiche ed abitudini peculiari della clientela di UniCredit. Vi è infatti un elevato numero di clienti che utilizzano i sistemi di Internet-Mobile banking quotidianamente rispetto ai quali è rilevabile l’utilizzo di medesimi indirizzi IP per l’accesso, anche a causa dell’utilizzo diffuso dei c.d. carrier grade nat (CGN) per via della nota saturazione degli indirizzi IPv4. Ciò è confermato dal report di Reply secondo cui “questa tecnica è stata progressivamente abbandonata a causa del sempre maggiore utilizzo di NAT da parte degli operatori mobili e fissi (es., CGN – Carrier Grade NAT): questo strumento rischierebbe quindi di inibire l'accesso al sistema a molti utenti legittimi provenienti dallo stesso IP pubblico utilizzato da un attaccante”.

Inoltre, “come sopra indicato, le altre possibili soluzioni quali la two factors authentication e il CAPTCHA non erano adottate dalla maggior parte degli istituti di credito al momento del data breach. In ogni caso, UniCredit si era dotata di un sistema di protezione anti DDOS (Denial Of Services) che si attivava in caso di attacchi provenienti da multipli indirizzi IP (cd. Botnet o reti di bot). Tuttavia, la sofisticazione delle modalità di sfruttamento del baco del Portale da parte degli Hacker permetteva di ridurre il traffico totale veicolato mantenendolo, di fatto, sotto la soglia di mitigazione della soluzione tecnologica utilizzata, denominata Akamai Prolexic, inibendone la capacità di rilevare un volume di traffico e caratteristiche di attacco tali da attivare la mitigazione. Ciò a ulteriore conferma che qualora l’attacco fosse stato perpetrato da Hacker con un livello di sofisticazione meno avanzato, lo stesso sarebbe stato identificato e bloccato dai sistemi di sicurezza di UniCredit […]; ciò che in ogni caso va sottolineato è che “le misure di sicurezza e di mitigazione dei rischi adottate da UniCredit si sono dimostrate efficaci in quanto a seguito dell’immediata risposta tecnologica della Società […] gli Hacker non sono riusciti a continuare l’attacco né ad accedere agli account degli Interessati e men che meno ad eseguire transazioni. L’attacco ha consentito meramente la possibilità di visualizzare un numero limitato di dati personali, non contenenti dati bancari, non appartenenti a categorie particolari ex art. 9 o dati di cui all’art. 10 del Regolamento, e non c’è alcuna prova che i Dati siano stati in alcun modo raccolti, copiati o archiviati dagli Hacker […]; […] questo dimostra che – grazie alle misure adottate da UniCredit – l’attacco non ha portato ad alcuna sottrazione di dati personali”.

In sintesi, secondo Unicredit, le contestazioni mosse dall’Autorità non avrebbero potuto ritenersi fondate, in quanto “UniCredit aveva adottato le misure di sicurezza adeguate ed in linea con gli standard di mercato al fine di contrastare in maniera efficace attacchi di tipo brute force nell’ambito della procedura di autenticazione informatica degli utenti del Portale. Queste misure hanno comportato che, anche con riferimento ad un attacco di reverse brute force, l’incidenza dello stesso fosse limitata al massimo, tenendo conto che in ogni caso qualora NTT Data avesse tempestivamente notificato la condizione applicativa, l’attacco sarebbe stato evitato del tutto”;

g) sia nell’immediatezza dell’attacco e anche nei giorni successivi, UniCredit ha rappresentato di

aver messo in atto misure di sicurezza e “misure aggiuntive ampiamente idonee a ulteriormente mitigare il rischio per la protezione dei dati personali causato dal data breach”, tra cui in particolare:

> “mettere a disposizione di tutti i clienti un vademecum per la gestione sicura delle credenziali di accesso e inoltrare delle raccomandazioni alla rete di responsabili delle filiali per incentivare la diffusione delle indicazioni contenute nel vademecum;
>
> implementare un blocco quantitativo delle connessioni oltre soglia critica e un CAPTCHA, quale ulteriore misura temporanea in vista della prossima implementazione della two factors authentication;
>
> adottare un meccanismo per forzare l’utilizzo di password complesse in fase di sign-in su tutta la rete clienti;
>
> comunicare, a seguito della richiesta del Garante, a tutti gli Interessati la violazione dei dati personali, includendo adeguate indicazioni di sicurezza per la gestione delle credenziali, anche su altri siti”.

Nel corso dell’audizione, tenutasi il 29 settembre 2020, UniCredit S.p.a., nel richiamarsi a quanto già argomentato nelle memorie difensive, ha chiesto l’archiviazione del procedimento sanzionatorio ribadendo che:

> a) “le misure di sicurezza adottate dalla banca all'epoca in cui si è verificato l'attacco informatico - che possono essere individuate in misure di prevenzione e misure di controllo - erano in linea con gli standard di mercato dell'epoca” e, differentemente da quanto ritenuto dal Garante, “erano in grado di contrastare un eventuale attacco di brute force”;
>
> b) “l'analisi condotta a seguito dell'attacco ha evidenziato come il rischio di utilizzo illecito dei dati oggetto di violazione fosse solo potenziale, considerato che non è stata accertata la memorizzazione dei dati […] né sono stati rilevati accessi non autorizzati ai conti correnti dei clienti coinvolti. Tra l'altro, […] i dati personali oggetto di violazione hanno riguardato nome e cognome, codice fiscale e codice NDG, che di per sé non consentono di effettuare login ai sistemi di online banking né altre tipologie di operazioni”;
>
> c) “i sistemi di monitoraggio di UniCredit hanno rilevato tempestivamente l'attacco informatico […] e malgrado il ritardo di NTT Data che, in violazione dei propri obblighi contrattuali, non ha dato immediata comunicazione della vulnerabilità non appena venutane a conoscenza, il che ha poi consentito l'attacco. Tale ritardo è dovuto ad un riconosciuto errore da parte di NTT Data di qualificazione della gravità della vulnerabilità e di comunicazione della stessa una volta qualificata correttamente, così come dichiarato dalla stessa NTT Data […]. NTT Data aveva infatti individuato la vulnerabilità ben 5 giorni prima dell'attacco ma l'ha notificata ad UniCredit solo dopo l'incidente ed a seguito di espressa richiesta della Banca. Qualora la vulnerabilità fosse stata notificata tempestivamente, UniCredit avrebbe avuto tempo di eliminarla e l'incidente non sarebbe avvenuto. Vulnerability assessment eseguiti tramite primari fornitori quali NTT Data rientrano tra le misure di sicurezza adeguate adottate da UniCredit perché non esiste alcun software privo di bug. Il fatto che i Vulnerability assessment eseguiti tramite NTT Data abbiano rilevato la vulnerabilità e che il contratto con il fornitore prevedesse la notifica immediata della stessa confermano ulteriormente l'adeguatezza delle misure di sicurezza adottate da UniCredit”;
>
> d) “rispetto alla violazione di dati personali in esame, allo stato non sono pervenuti reclami e/o azioni risarcitorie da parte degli interessati coinvolti”.

3. Le disposizioni rilevanti in relazione al caso di specie.

L’art. 5, par. 1, lett. f), del Regolamento stabilisce, tra i princìpi generali che sovrintendono il trattamento dei dati personali, che i dati personali devono essere “trattati in maniera da garantire un’adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali (“integrità e riservatezza”).

L’art. 32 del Regolamento (“Sicurezza del trattamento”) dispone altresì, al par. 1, che “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, 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 […]”; il successivo par. 2 stabilisce inoltre 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”.

4. Le valutazioni dell’Autorità e l’esito dell’istruttoria.

All’esito dell’esame della documentazione prodotta e delle dichiarazioni rese dal titolare del trattamento nel corso del procedimento, 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, questa Autorità formula le seguenti considerazioni conclusive.

In particolare, con riferimento alle misure tecniche e organizzative di cui all’art. 32, par. 1, del Regolamento adottate da UniCredit nell’ambito del Portale di mobile banking (v. par. 1.1, lett. a)) e alle contestazioni mosse sul punto dall'Autorità (cfr. par. 2, punti 1 e 2), nel prendere atto di quanto ampiamente illustrato dall’Istituto di credito nella memoria difensiva e nel corso dell’audizione, questa Autorità rileva che:

a) rispetto alla “c.d. condizione applicativa che rendeva disponibili all’interno della risposta HTTP (HyperText Transfer Protocol), anche in caso di tentativi di autenticazione non riusciti, alcuni dati personali (nome, cognome, codice fiscale, NDG) di clienti ed exclienti di UniCredit che pertanto erano suscettibili di essere liberamente consultati e acquisiti da chiunque” (cfr. par. 2, punto 1), risulta evidente come consentire l’accesso ad alcuni dati personali di clienti ed ex-clienti, anche senza il superamento di una procedura di autenticazione informatica, non sia conforme alla disciplina in materia di protezione dei dati personali.

La mancata adozione, da parte di UniCredit, di misure tecniche in grado di limitare l’accesso ai dati personali al solo personale autorizzato o allo stesso interessato, ha determinato la possibilità che i dati personali fossero liberamente accessibili da parte di chiunque. Infatti, tali dati erano resi disponibili all’interno della risposta HTTP (HyperText Transfer Protocol) fornita dai sistemi informatici della Banca al browser di chiunque tentasse, anche senza riuscirvi, di superare la procedura di autenticazione informatica che all’epoca era presente nel Portale di mobile banking.

Fermo restando che con il termine “chiunque”, si intende indicare un qualunque soggetto anche diverso dal personale autorizzato e dall’interessato, questa Autorità ritiene che le considerazioni svolte da UniCredit in merito alle asserite elevate capacità tecniche necessarie per sfruttare la vulnerabilità presente nel Portale di mobile banking, più che comprovare l’adeguatezza delle misure tecniche adottate dall’istituto, dimostrino una sottovalutazione dei rischi connessi alla fornitura di servizi di online banking. Infatti, il settore finanziario rappresenta, da sempre, un obiettivo primario per i criminali informatici, come indicato anche in un documento denominato “Sicurezza cibernetica: il contributo della Banca d'Italia e dell'Ivass”, pubblicato ad agosto 2018, predisposto dal Gruppo di coordinamento sulla sicurezza cibernetica (GCSC) della Banca d’Italia

e dell'IVASS, che evidenzia come "già nel 2014 un attacco coordinato contro numerose banche statunitensi condusse, tra l'altro, al furto dei dati personali di 80 milioni di clienti di JP Morgan Chase. Negli anni successivi si sono moltiplicati episodi simili; quasi nessuna delle grandi istituzioni finanziarie private è rimasta immune e sono state colpite anche alcune banche centrali. Gli attacchi al sistema finanziario sono talvolta condotti con metodi molto semplici, come il furto di credenziali di accesso ai conti mediante il phishing, o il denial of service, che, sovraccaricando i server con milioni di richieste simultanee di dati, rende inutilizzabili i servizi bancari erogati via rete. Altre volte le intrusioni sono condotte con metodi complessi e portano alla sottrazione di fondi o di dati su larga scala. La difesa del sistema finanziario è assai complessa: il settore è altamente digitalizzato, è interconnesso a livello globale mediante un piccolo numero di infrastrutture che possono presentare vulnerabilità, è attaccabile attraverso possibili comportamenti imprudenti di centinaia di milioni di utenti di servizi finanziari online";

b) quanto al secondo profilo oggetto di contestazione, ovvero la mancata adozione, nell'ambito della procedura di autenticazione informatica degli utenti del Portale di mobile banking, di alcun meccanismo in grado di contrastare efficacemente attacchi di tipo brute force condotti mediante l'utilizzo dei c.d. bot (programmi informatici che accedono ai siti web attraverso lo stesso canale utilizzato dagli utenti umani simulandone l'operatività) (cfr. par. 2, punto 2), l'Autorità rileva che il sistema di autenticazione informatica all'epoca adottato da UniCredit – che prevedeva l'utilizzo di credenziali di autenticazione costituite solamente da un User ID e da un PIN, entrambi composti da 8 cifre decimali – si prestava a essere oggetto di attacchi di tipo brute force, ossia attacchi informatici che hanno l'obiettivo di individuare credenziali di autenticazione informatica valide per l'accesso a un determinato sistema o servizio online. Ciò, anche in considerazione del fatto che, al momento della violazione, UniCredit non aveva adottato alcuna misura tecnica che impedisse agli utenti di utilizzare PIN semplici, quali, ad esempio, quelli composti da ripetizioni o sequenze di numeri oppure coincidenti con la data di nascita o con lo User ID.

Al riguardo, occorre evidenziare che esistono diversi attacchi informatici di tipo brute force, quali, ad esempio, gli attacchi brute force semplici (volti a individuare la password o il PIN utilizzato da uno specifico utente, verificando tutte le possibili combinazioni di lettere e numeri), gli attacchi a dizionario (volti a individuare la password o il PIN utilizzata da uno specifico utente, verificando le possibili combinazioni presenti in dizionari composto da password o PIN più comuni o da password o PIN compromessi nell'ambito di altri attacchi informatici), gli attacchi credential stuffing (volti a verificare la validità di credenziali di autenticazione acquisite nell'ambito di altri attacchi informatici), gli attacchi reverse brute force (volti a individuare gli utenti che utilizzano una specifica password o PIN, spesso molto comune o semplice) o anche una loro combinazione. Nel caso in esame, un'adeguata valutazione dei rischi presentati dai trattamenti effettuati nell'ambito del Portale di mobile banking avrebbe consentito a UniCredit di analizzare correttamente le caratteristiche del sistema di autenticazione informatica, di individuare le debolezze suscettibili di compromettere la sicurezza del trattamento e, conseguentemente, di adottare misure per gestire e mitigare i rischi connessi a tali debolezze, incluse quelle di difesa proattiva da attacchi informatici di reverse brute force.

5. Conclusioni: dichiarazione di illiceità del trattamento. Provvedimenti correttivi ex art. 58, par. 2, del Regolamento.

Per i suesposti motivi l'Autorità ritiene che le dichiarazioni rese dal titolare del trattamento nelle memorie difensive - della cui veridicità si può essere chiamati a rispondere ai sensi del citato art. 168 del Codice - seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentirne l'archiviazione, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del regolamento del Garante n. 1/2019, concernente le procedure interne all'Autorità aventi rilevanza esterna.

In particolare, le criticità anzi rappresentate hanno evidenziato che le violazioni di dati personali

occorse - a latere delle considerazioni in ordine ai profili di responsabilità di NTT Data, responsabile del trattamento, che sono oggetto di un distinto e separato provvedimento di questa Autorità – si sono verificate in quanto UniCredit S.p.a., titolare del trattamento cui è attribuita la "responsabilità generale" dei trattamenti di dati personali direttamente posti in essere o che altri abbiano effettuato per suo conto - ha omesso di verificare, in relazione alla natura, al contesto, alle finalità e ai rischi dei trattamenti realizzati nell'ambito del Portale di home banking, l'effettiva conformità degli stessi ai principi di integrità e riservatezza 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 e 2, del Regolamento.

Purtuttavia, tenuto di quanto dichiarato dalla Banca nel corso del procedimento, in ordine all'avvenuta messa in atto, nell'immediatezza della violazione, di misure di sicurezza e "misure aggiuntive ampiamente idonee a ulteriormente mitigare il rischio per la protezione dei dati personali causato dal data breach" (cfr. par. 1.1, lett. g)) nonché del fatto che, a seguito dell'evento, non sono pervenuti reclami ai sensi dell'art. 77 del Regolamento da soggetti interessati dalla violazione, questa Autorità, nell'esercizio dei poteri correttivi attribuiti dall'art. 58, par. 2, del Regolamento, ritiene di non dover ingiungere misure correttive ai sensi dell'art. 58, par. 2, lett. d), e dispone una sanzione amministrativa pecuniaria ai sensi dell'art. 83 del Regolamento, commisurata alle circostanze del caso concreto (art. 58, par. 2, lett. i)).

6. Ordinanza ingiunzione.

La violazione delle disposizioni sopra richiamate comporta l'applicazione della sanzione amministrativa prevista dall'art. 83, parr. 4, lett. a), e 5, lett. a), del Regolamento.

In merito, si rileva che la violazione dell'art. 32 del Regolamento, in quanto riferita alla mancata adozione di misure di sicurezza attuative di un principio ricompreso nella disposizione, di portata generale, di cui all'art. 5 del Regolamento e inerente l'"integrità e riservatezza" dei dati oggetto di trattamento (art. 5, par. 1, lett. f), del Regolamento) sarà complessivamente valutata nell'ambito della violazione della predetta disposizione normativa con conseguenziale applicazione della sola sanzione prevista all'art. 83, par. 5, lett. a), del Regolamento.

Tale disposizione, nel fissare il massimo edittale nella somma di 20 milioni di euro ovvero, per le imprese, nel 4% del fatturato mondiale annuo dell'esercizio precedente ove superiore, specifica le modalità di quantificazione della predetta sanzione, che deve "in ogni caso [essere] effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), individuando, a tal fine, una serie di elementi, elencati all'art. 83, par. 2, del Regolamento, da valutare all'atto di quantificarne il relativo importo; in adempimento di tale previsione, nel caso di specie, assumono rilevanza le circostanze sotto riportate:

a) con riferimento alla natura, alla gravità e alla durata della violazione (art. 83, par. 2, lett. a), del Regolamento) è stata presa in considerazione l'avvenuta perdita di confidenzialità verificatasi a causa di una violazione dei dati personali determinata dall'inosservanza di princìpi di portata generale relativi alle misure di sicurezza (artt. 5, par. 1, lett. f), e 32 del Regolamento), nonché la circostanza che la violazione ha interessato un numero estremamente rilevante di interessati;

b) con riferimento al carattere doloso o colposo delle violazioni e al grado di responsabilità del titolare (art. 83, par. 2, lett. b) e d), del Regolamento), è stato preso in considerazione il comportamento del titolare del trattamento che non si è conformato alla disciplina in materia di protezione dei dati personali relativamente ai principi generali in materia di misure di sicurezza del trattamento;

c) con riferimento all'adozione, da parte del titolare, di misure atte a mitigare il danno subito

dagli interessati (art. 83, par. 2, lett. c), del Regolamento), sono state considerate positivamente le diverse iniziative di informazione e supporto poste in essere nei confronti della clientela interessata dalla violazione dei dati personali sin dal giorno del rilevamento dell'incidente, anche in ottemperanza al provvedimento dell'Autorità n. 499 del 13 dicembre 2018; altrettanto positivamente devono essere valutate le implementazioni alle misure di sicurezza adottate nell'immediatezza dell'evento (cfr. punto 1.1, lett. g));

d) l'esistenza di precedenti provvedimenti dell'Autorità nei confronti del titolare adottati anche a seguito di un'altra violazione dei dati personali (art. 83, par. 2, lett. e), del Regolamento);

e) la fattiva collaborazione con l'Autorità, anche in ordine alla ricostruzione degli eventi e ai rapporti con il responsabile del trattamento (art. 83, par. 2, lett. f), del Regolamento);

f) con riferimento alle categorie di dati personali interessate dalla violazione (art. 83, par. 2, lett. g), del Regolamento), è stato considerato che sono stati oggetto di violazione dati comuni degli interessati, con esclusione di dati bancari.

In considerazione dei richiamati principi di effettività, proporzionalità e dissuasività (art. 83, par. 1, del Regolamento) ai quali l'Autorità deve attenersi nella determinazione dell'ammontare della sanzione, sono state prese in considerazione le condizioni economiche del contravventore, determinate in base ai ricavi conseguiti riferiti al bilancio d'esercizio per l'anno 2022.

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro di euro 2.800.000 (duemilioniottocentomila) per la violazione degli artt. 5, par. 1, lett. f), e 32, par. 1 e 2, del Regolamento.

In tale quadro, anche in considerazione della tipologia di violazione accertata, che ha riguardato i principi di protezione dei dati personali, si ritiene che, ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del regolamento del Garante n. 1/2019, si debba procedere alla pubblicazione del presente provvedimento sul sito internet del Garante.

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, ai sensi degli artt. 57, par. 1, lett. f), e 83 del Regolamento, l'illiceità del trattamento effettuato, nei termini di cui in motivazione, per la violazione degli artt. 5, par. 1, lett. f), e 32, par. 1 e 2, del Regolamento.

ORDINA

a UniCredit S.p.a., con sede legale in legale in Milano, Piazza Gae Aulenti, 3, C.F./P.I. 00348170101, ai sensi dell'art. 58, par. 2, lett. i), del Regolamento, di pagare la somma di euro 2.800.000 (duemilioniottocentomila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

alla medesima UniCredit S.p.a. di pagare la somma di euro 2.800.000 (duemilioniottocentomila) secondo le modalità indicate in allegato, entro 30 giorni dalla notifica del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge n. 689/1981.

Si rappresenta che ai sensi dell'art. 166, comma 8, del Codice, resta salva la facoltà per il trasgressore di definire la controversia mediante il pagamento – sempre secondo le modalità indicate in allegato – di un importo pari alla metà della sanzione irrogata entro il termine di cui all'art. 10, comma 3, del d.lgs. n. 150 del 1° settembre 2011 previsto per la proposizione del ricorso come sotto indicato.

DISPONE

ai sensi dell'art. 166, comma 7, del Codice e dell'art. 16, comma 1, del Regolamento del Garante n. 1/2019, la pubblicazione del presente provvedimento sul sito web del Garante e ritiene che ricorrano i presupposti di cui all'art. 17 del regolamento n. 1/2019.

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 è possibile proporre ricorso dinanzi 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, 8 febbraio 2024

IL PRESIDENTE
Stanzione

IL RELATORE
Ghiglia

IL VICE SEGRETARIO GENERALE
Filippi