Provvedimento dell'8 febbraio 2024 [9991064]

VEDI ANCHE Newsletter del 7 marzo 2024

[doc. web n. 9991064]

Provvedimento dell'8 febbraio 2024

Registro dei provvedimenti
n. 66 dell'8 febbraio 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;

VISTO che nel corso dell'istruttoria nei confronti di UniCredit S.p.a. sono emersi profili di responsabilità a carico di NTT Data Italia S.p.a., responsabile del trattamento dei dati personali;

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 dall'Istituto, 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 altresì 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:

> "login protetto da username e password consegnati separatamente al cliente in filiale;
>
> blocco dell'account dopo l'inserimento di tre password errate;
>
> blocco di credenziali individuate in data leak online da parte dei […] servizi di intelligence/antifrode;
>
> 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;
>
> protezione delle transazioni e delle attività sensibili (es. modifica dati personali) attraverso la richiesta di un ulteriore One Time Password (OTP);
>
> analisi comportamentale e monitoraggio delle transazioni per individuare frodi a scapito dei clienti;
>
> esecuzione di VA/PT periodici […] sull'infrastruttura e l'applicazione di internet/banking;
>
> 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" o "la società") 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 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 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 NTT Data Italia 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 da NTT Data, responsabile del trattamento di UniCredit, (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:

NTT Data ha affidato l’esecuzione delle attività di vulnerability assessment e penetration testing del Portale di mobile banking in questione ad una società terza (Truel IT) in assenza di preventiva autorizzazione scritta da parte del titolare del trattamento, in violazione dell’art. 28, par. 2, del Regolamento;

NTT Data ha informato tardivamente UniCredit dell’avvenuta violazione dei dati personali e, pertanto, non ha ottemperato all’obbligo di cui all’art. 33, par. 2, del Regolamento.

Tenuto conto di quanto sopra, l’Ufficio, con nota del 5 febbraio 2020, ha notificato a NTT Data Italia S.p.A., responsabile del trattamento di UniCredit, 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 delle disposizioni che disciplinano il ricorso ad altro responsabile del trattamento e dell’obbligo di informazione del titolare del trattamento in caso di violazione dei dati personali di cui agli artt. 28, par. 2, e 33, par. 2 del Regolamento.

Con la medesima nota NTT Data 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 20 marzo 2020, NTT Data Italia ha fatto pervenire la memoria difensiva, che qui si richiama integralmente, con la quale, nel formulare richiesta di audizione, ha fornito gli elementi di valutazione (con relativa documentazione allegata) di seguito indicati. In particolare:

a) "le attività di VA e PT oggetto dell'odierna verifica da parte del Garante sono state svolte da NTT Data, su incarico di UBIS (non di UniCredit), nel periodo 1° ottobre 2018 – 12 ottobre 2018, in esecuzione del contratto del 5 giugno 2017 relativo a "Banking Application Penetration Test & Vulnerability Assessment" e, in forza del quale, è stato emesso da UBIS uno specifico ordine di acquisto per NTT Data". Dunque "È UBIS, e solo UBIS, la società del Gruppo UniCredit con la quale NTT Data ha avuto rapporti contrattuali. Infatti:

il Contratto è stato sottoscritto da UBIS e NTT Data;

l'ultima designazione di NTT Data quale subprocessor o sub-responsabile (non responsabile) del trattamento è stata eseguita da UBIS, nella sua qualità di processor o responsabile del trattamento, il 18 ottobre 2018 (Data Processing Agreement o DPA);

è espressamente previsto che le obbligazioni del DPA prevalgano, in caso di contrasto, su quelle del Contratto (art. 12.1. del DPA), con la conseguenza che, a far data dal 18 ottobre 2018, la nomina di NTT Data quale responsabile del trattamento per UniCredit di cui all'art. 13 del Contratto deve ritenersi superata e sostituita dal DPA;

UBIS (non UniCredit) risulta, nel DPA, come l'unico soggetto al quale comunicare eventuali data breaches o violazioni di dati personali (v. Appendix 1 del DPA – p. 8;

le lettere di autorizzazione specifica allo svolgimento delle attività di VA e PT sui sistemi di mobile banking (Android e iOS) di UniCredit oggetto di verifica da parte del Garante sono state sottoscritte da UBIS […].

Fermo restando quanto sopra, è del pari vero che l'Allegato 1 del Contratto […] prevede che NTT Data svolga le attività di VA e PT su sistemi di diverse società del Gruppo UniCredit: ma è altrettanto vero che tali attività sarebbero, e sono state svolte sempre su incarico di UBIS, e non di UniCredit";

b) "NTT Data non aveva alcuna obbligazione nei confronti di UniCredit: ogni suo obbligo era nei confronti di UBIS, con la conseguenza che non può esserle addebitato alcun ritardo nella comunicazione di alcunché a UniCredit. Quanto alle obbligazioni assunte da NTT Data con il Contratto e il DPA, si citano quelle che rilevano ai fini del presente procedimento:

svolgere, su incarico di UBIS, attività di VA e PT (artt. 3.1. e 3.2. del Contratto);

comunicare immediatamente a UBIS eventuali vulnerabilità di livello critico o alto (v. p. 4 dell'Allegato 3 del Contratto);

comunicare a UBIS, senza ingiustificato ritardo, ogni eventuale violazione dei dati personali (art. 6.1. del DPA);

comunicare immediatamente a UBIS e, in ogni caso, entro 4 ore dall'esserne venuta a conoscenza, ogni violazione dei dati personali (art. 6.2. del DPA);

richiedere l'autorizzazione preventiva di UBIS per l'ingaggio di eventuali ulteriori sub-responsabili del trattamento (art. 9.1. del DPA)";

c) “il motivo per cui è stato necessario il coinvolgimento di Truel It è lo stesso motivo alla base della mancata acquisizione dell’autorizzazione preventiva di UBIS: far fronte a un improvviso e inatteso picco di lavoro. Il coinvolgimento di Truel It è, comunque, stato limitato a un solo caso, quello dell’esecuzione dei VA e PT oggi all’esame del Garante. Il riferito picco di lavoro non è, comunque, stato tale da pregiudicare la posizione di UBIS o degli interessati […]. Infatti, Truel It è stata coinvolta unicamente quale fornitore censito nell’albo di NTT Data, ossia in quanto ne erano già state verificate la professionalità e affidabilità mediante raccolta dei dovuti documenti e delle dovute autocertificazioni/autodichiarazioni, compresa quella relativa alle misure di sicurezza organizzative e tecniche implementate”;

d) “lo svolgimento delle attività di VA e PT tra il 1° ottobre 2018 e il 12 ottobre 2018 è avvenuto in adempimento a una specifica richiesta di UBIS. Le verifiche svolte da NTT Data (anche attraverso Truel It) sono consistite, nello specifico, nella simulazione di scenari di intrusione verso l’applicazione target per verificarne la resistenza a potenziali azioni finalizzate alla creazione di condizioni di disservizio e/o di sottrazione di dati/informazioni critiche (c.d. data exfiltration). Tutte queste attività sono state costantemente monitorate da UBIS attraverso il proprio Security Operation Center. Il perimetro di intervento concordato con UBIS, la natura stessa delle attività commissionate a NTT Data da UBIS e gli strumenti utilizzati dal personale NTT Data e di Truel It nello svolgimento di tali attività, non hanno consentito – né avrebbero potuto consentire - in alcun modo la rilevazione di tentativi di intrusione (effettivi e non simulati) realizzati da terzi. In particolare, la rilevazione di un tentativo di accesso ai sistemi di UBIS da parte di terzi può avvenire tramite […]” una serie di attività “non comprese nell’incarico conferito a NTT Data (e, di conseguenza, Truel It) […] le uniche […] che avrebbero consentito la rilevazione di tentativi di accesso ai sistemi di UBIS. […]. NTT Data, anche attraverso Truel It, si è limitata alle attività necessarie per adempiere l’incarico ricevuto: esecuzione di VA e PT. In tale contesto, Truel It ha prodotto (in data 19 ottobre 2018) un report provvisorio, che NTT Data ha provveduto a verificare secondo le proprie prassi interne, quale garanzia di qualità”;

e) con specifico riferimento alle contestazioni mosse dall’Autorità, la Società ha innanzitutto evidenziato due circostanze: la prima è che “NTT Data non ha avuto alcun rapporto con, né alcun obbligo verso, UniCredit: pertanto, non sembra possibile contestarle di aver comunicato con ritardo alcunché a UniCredit; la seconda è che “NTT Data non ha avuto alcuna possibilità di rilevare (per conto di UBIS) i tentativi di accesso ai sistemi di UniCredit, culminati con il data breach notificato da quest’ultima al Garante. L’incarico che ha svolto (anche con Truel It) era relativo a tutt’altro, vale a dire vulnerability assessment e penetration test e, in quel contesto, non ha avuto accesso agli strumenti che le avrebbero potuto consentire di avvedersi (per conto di UBIS) di tentativi di accesso non autorizzato ai sistemi di UniCredit”. Ciò premesso, va evidenziato che:

1. “per quanto concerne la violazione dell’art. 28, comma 2, del Regolamento:

> la stessa si è verificata nel “periodo di prima applicazione del GDPR, 8 mesi decorrenti dal 19 settembre 2018 al 19 maggio 2019”, periodo di cui - ai sensi “dell’art. 22, comma 13 del D.Lgs. 101/2018 - il Garante […] tiene conto, ai fini dell'applicazione delle sanzioni amministrative e nei limiti in cui risulti compatibile con le disposizioni del Regolamento […]”. Dunque “il fatto che NTT Data, in buona fede, per una scusabile leggerezza (e non certo per dolo o colpa grave), abbia omesso di richiedere la preventiva autorizzazione di UBIS all’ingaggio di Truel It dovrà, quindi, essere valutato in quest’ottica […]”:
>
> “né UBIS, né gli interessati, hanno subito alcun danno dal coinvolgimento di Truel It nell’esecuzione di VA e PT”; questi “sono stati eseguiti (non da NTT Data, ma) da Truel It, ma pur sempre a regola d’arte e secondo le specifiche contrattualmente pattuite con

UBIS […] In buona sostanza, se NTT Data avesse eseguito le attività di VA e PT direttamente, le avrebbe eseguite nello stesso modo di Truel It […]"; quindi "[…] Anche sotto questo profilo, l'omissione di NTT Data risulta una semplice leggerezza, come tale del tutto priva (sotto ogni profilo) del carattere dell'offensività";

"le modalità di esecuzione di VA e PT da parte di Truel It, così come descritte nel report consegnato da Truel It a NTT Data" hanno comportato che "gran parte dei test richiesti da UBIS sono stati "condotti su credenziali e conti correnti di test"; ciò ha "ha escluso l'interazione massiva (di NTT Data e/o di Truel It) con altri conti correnti associati a clienti reali, con la conseguenza che l'integrità e la confidenzialità dei dati di questi ultimi è stata preservata". In particolare l'Autorità, nel decider se comminare o meno una sanzione, dovrebbe tener conto anche del fatto che nell'esecuzione dei VA e PT Truel It è venuta a conoscenza, per un arco temporale estremamente limitato (1-12 ottobre 2018), di meri dati identificativi (nome, cognome e codice fiscale) e che gli stessi, "in applicazione dei principi di minimizzazione, finalità e limitazione della conservazione, laddove visualizzati dai sistemi UniCredit all'esito dell'interrogazione – sono stati tempestivamente cancellati dai sistemi di Truel It";

NTT Data "non è mai stata oggetto, prima d'ora, di controlli e/o di sanzioni da parte dell'Autorità; ciò è indubbiamente un chiaro indice del buon (se non, addirittura, ottimo) livello di compliance raggiunto dalla società […]" come dimostrano le diverse "misure di compliance già in essere al 22 ottobre 2018" e quelle adottate successivamente al 22 ottobre 2018 e in corso di implementazione (delle quali è stata fornita ampia descrizione in allegato alla memoria difensiva). "Ad ulteriore conferma e conforto di quanto sopra, si deve considerare anche che NTT Data, agendo spesso quale (sub)responsabile del trattamento, è altrettanto spesso sottoposta ad audit da parte dei propri clienti (titolari o responsabili del trattamento): tali audit hanno sempre esito positivo";

"un'eventuale sanzione per la violazione dell'art. 28, comma 2 GDPR (norma che disciplina il rapporto tra responsabile e titolare e, quindi, tra NTT Data e i propri clienti)" avrebbe come conseguenza un danno reputazionale (ovvero "la perdita della fiducia dei clienti e, quindi, la perdita di incarichi") "di gravità, francamente, sproporzionata rispetto alla lievità della violazione contestata";

2. quanto alla contestata violazione dell'art. 33, par. 2 del Regolamento si ribadisce nuovamente che "NTT Data non ha avuto, né poteva avere, alcuna conoscenza della violazione dei dati personali subita da UniCredit il 21 ottobre 2018"; ciò in quanto:

"l'incarico di NTT Data era quello di condurre vulnerability assessment e penetration test: nient'altro;

l'odierna esponente non era, in particolare, responsabile del monitoraggio dei sistemi informatici di UniCredit: non aveva, quindi, alcun modo di rilevare attacchi e/o data breach (circostanza confermata anche dalla Relazione Tecnica: v. pp. 5 ss.);

inoltre, gli accessi ai sistemi di UniCredit si sono arrestati il 12 ottobre 2018, quando Truel.it ha concluso le attività ed iniziato la stesura del report di vulnerability assessment e penetration test: ben prima, quindi, che il data breach del 21 ottobre 2018 si verificasse".

La Società ha quindi nuovamente evidenziato che "l'unica cosa che NTT Data poteva rilevare, e ha rilevato, è stata una vulnerabilità di livello alto che ha provveduto a comunicare a UBIS con tempestività rispetto al momento nel quale ne è venuta a conoscenza. […] NTT Data non

conosceva, e non poteva conoscere, il data breach di UniCredit del 21 ottobre 2018: gli artt. 6.1. e 6.2. del DPA non sono, quindi, stati violati. L'unica cosa della quale NTT Data è venuta a conoscenza, è stata la vulnerabilità sfruttata dai terzi ai quali è imputabile il data breach subito da UniCredit: cosa ben diversa dal data breach stesso. E non è stato contestato a NTT Data di aver comunicato in ritardo tale vulnerabilità: né avrebbe potuto esserlo, perché tale vulnerabilità è stata comunicata con tempestività.

Il Contratto, sotto questo punto di vista, prevedeva che la comunicazione [fosse] immediata. Il concetto di immediatezza sconta, naturalmente, l'effettiva conoscenza che NTT Data può aver avuto della vulnerabilità: tale momento non è antecedente il 19 marzo 2018, i.e. il giorno in cui NTT Data ha ricevuto il report preliminare di Truel It ([…] allegato alla Relazione Tecnica), e non è nemmeno coincidente. Il Working Party Art. 29, nelle sue linee guida sulla notifica delle violazioni di dati personali, ha avuto modo di precisare che il termine per detta notifica decorre dal momento in cui il titolare o il responsabile del trattamento (a seconda dei casi) acquisisce effettiva conoscenza della violazione stessa, e che l'effettiva conoscenza necessariamente consegue alle dovute verifiche. Tale principio è chiaramente applicabile anche al caso di NTT Data, sulla base di un principio di ragionevolezza: se una circostanza grave come un data breach deve essere verificato, prima di essere notificato, non si vede perché una circostanza meno grave, come una vulnerabilità, debba essere comunicata prima di aver verificato che sia effettiva.

Nessun ritardo è, quindi, contestabile a NTT Data: né in relazione alla comunicazione del data breach di UniCredit, che non poteva conoscere; né in relazione alla vulnerabilità, che ha comunicato non appena conosciuta".

La Società ha quindi evidenziato che, in estrema sintesi, dagli elementi di fatto risulta che:

> "NTT Data non aveva, né avrebbe potuto avere, alcuna conoscenza del data breach (e dei precedenti tentativi di terzi di accedere ai sistemi) di UniCredit;
>
> NTT Data non poteva, né avrebbe potuto, comunicare il data breach a UniCredit;
>
> l'unico fatto del quale NTT Data ha avuto conoscenza, è stata una vulnerabilità ai sistemi di UniCredit […] che è stata tempestivamente comunicata da NTT Data, in quanto UBIS ne ha ricevuto notizia non appena NTT Data ha concluso le verifiche finalizzate ad assicurare che il report di Truel It fosse corretto";
>
> anche qualora NTT avesse trasmesso il report di Truel IT "subito, cioè già il 19 ottobre 2018 senza aspettare di averlo verificato", UBIS non avrebbe potuto evitare la violazione dei dati personali "perché tra il 19 ottobre e il 21 ottobre è trascorso un lasso di tempo veramente ridotto".

Il 19 gennaio 2021, si è svolta l'audizione di NTT Data, nel corso della quale la stessa, nel ribadire integralmente quanto già esposto nella memoria difensiva, ha chiesto che l'Autorità, ai fini della valutazione del caso, tenga in particolare considerazione le seguenti circostanze:

> a) "nessun danno si è realizzato in conseguenza dell'attività posta in essere dalla società";
>
> b) "i fatti si sono verificati in un periodo particolarmente impegnativo che ha determinato la necessità di ricorrere a un soggetto terzo, peraltro in una fase di prima applicazione del GDPR";
>
> c) "la società si è mostrata collaborativa nei confronti dell'Autorità, fornendo ogni elemento utile ai fini della ricostruzione dell'incidente";
>
> d) "l'eventuale applicazione di una sanzione pecuniaria e soprattutto la pubblicazione del

provvedimento sarebbe fortemente lesiva degli interessi della società e vanificherebbe ogni sforzo posto in essere finora, in termini di compliance, laddove tale aspetto è un elemento di concorrenza tra i soggetti operanti nel settore".

La Società ha altresì evidenziato di essere impegnata nell'adozione di ulteriori misure "al fine di continuare ad innalzare il livello di compliance, alcune delle quali sono ancora in fase di implementazione (fase che si prevede di concludere […] entro il 31 marzo 2021). […] tra le altre, il privacy dashboard, che consente alla società (e, in particolare, al suo privacy office) di (i) monitorare costantemente gli aspetti privacy anche al fine di individuare aree di miglioramento in conformità al principio di accountability, e di (ii) predisporre dei report periodici sul livello di compliance privacy, da condividere con il top management".

3. La normativa in materia di protezione dei dati personali.

A norma dell'art. 28, par. 2 del Regolamento "il responsabile del trattamento non ricorre a un altro responsabile senza previa autorizzazione scritta, specifica o generale, del titolare del trattamento […]".

Il successivo par. 3, del medesimo art. 28 del Regolamento, nel disporre che "i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da altro atto giuridico", precisa, alla lett. f), che tale contratto o altro atto giuridico deve prevedere che il responsabile del trattamento "assista il titolare del trattamento nel garantire il rispetto degli obblighi di cui agli articoli da 32 a 36, tenendo conto della natura del trattamento e delle informazioni a disposizione del responsabile del trattamento".

Inoltre, l'art. 28, par. 4, del Regolamento dispone che "quando un responsabile del trattamento ricorre a un altro responsabile del trattamento per l'esecuzione di specifiche attività di trattamento per conto del titolare […], su tale altro responsabile del trattamento sono imposti, mediante un contratto o un altro atto giuridico a norma del diritto dell'Unione o degli Stati membri, gli stessi obblighi in materia di protezione dei dati contenuti nel contratto o in altro atto giuridico tra il titolare del trattamento e il responsabile del trattamento di cui al paragrafo 3, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del […] regolamento. Qualora l'altro responsabile del trattamento ometta di adempiere ai propri obblighi in materia di protezione dei dati, il responsabile iniziale conserva nei confronti del titolare del trattamento l'intera responsabilità dell'adempimento degli obblighi dell'altro responsabile".

L'art. 33 del Regolamento, in tema di violazione dei dati personali, al par. 2 dispone che, in siffatta ipotesi, "il responsabile del trattamento informa il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione".

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.

Per quanto attiene la contestata violazione della disposizione di cui all'art. 28, par. 2, del Regolamento, si prende atto che NTT Data ha affidato alla società Truel IT lo svolgimento delle attività di vulnerability assessment e penetration testing senza aver ottenuto la necessaria preventiva autorizzazione scritta, specifica o generale, da parte del titolare del trattamento.

Peraltro, lo stesso atto di designazione di NTT Data quale responsabile del trattamento conteneva

il divieto espresso di affidare a terze parti l'esecuzione, parziale o totale, delle attività di vulnerability assessment e penetration testing.

Con riferimento al secondo profilo oggetto di contestazione, tenuto conto di quanto ampiamente rappresentato nel corso dell'istruttoria da UniCredit e da NTT Data, risulta accertato che:

a) le due vulnerabilità sopra citate, identificate "con gravità di livello high", sono esattamente quelle utilizzate dall'attaccante nel corso dell'attacco informatico che è stato condotto, in maniera massiva, per individuare le User ID (REB code) valide per l'accesso al Portale di mobile banking e per acquisire illecitamente i dati personali ad esse associate;

b) Truel IT era "a conoscenza" della violazione dei dati personali dal momento in cui ha rilevato la vulnerabilità di tipo "User Data Disclosure" (ovvero, come si evince dai report tecnici, dal 10 ottobre 2018), in quanto in quel momento vi era la ragionevole certezza del fatto che si fosse verificata una violazione della riservatezza dei dati personali trattati nell'ambito del Portale di mobile banking. Inoltre, l'individuazione, da parte della medesima Società, nel giorno immediatamente successivo (11 ottobre 2018), della vulnerabilità di tipo "Lack of Reverse Bruteforce Protection" metteva in evidenza la circostanza che la vulnerabilità di tipo "User Data Disclosure" potesse essere sfruttata in modo massivo, producendo effetti negativi su un numero elevato di interessati;

c) Truel IT ha informato NTT Data delle anzidette vulnerabilità soltanto il 19 ottobre 2018, mediante l'invio della bozza del report contenente gli esiti delle attività di vulnerability assessment e penetration testing e solo il 22 ottobre 2018, giorno successivo all'attacco informatico, NTT Data ha informato UniCredit (quando la Banca ne aveva già autonomamente avuto conoscenza, in quanto i suoi sistemi di monitoraggio avevano rilevato l'attacco informatico del 21 ottobre 2018 e di conseguenza aveva adottato un primo insieme di misure tecniche e organizzative per porre rimedio alla violazione dei dati personali).

Tanto considerato, nel rilevare preliminarmente come le attività che la banca ha affidato a NTT Data siano riconducibili a quelle che un titolare del trattamento effettua per "testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" (cfr. art. 32, par. 1, lett. d), del Regolamento), ne deriva che nel caso in cui si verifichi una violazione dei dati personali, sebbene il titolare conservi la responsabilità generale per la protezione dei dati personali, il responsabile del trattamento svolge comunque un ruolo fondamentale per consentire al titolare di adempiere tempestivamente e adeguatamente agli obblighi previsti dagli articoli da 32 a 36 del Regolamento (cfr. art. 28, par. 3, lett. f)), compresi quelli, in materia di notifica delle violazioni dei dati personali.

In particolare, ai sensi dell'art. 33, par. 2, del Regolamento, in caso di violazione dei dati personali, il responsabile del trattamento è tenuto ad informare "il titolare del trattamento senza ingiustificato ritardo dopo essere venuto a conoscenza della violazione".

Al riguardo, con riferimento all'espressione "senza ingiustificato ritardo", le "Linee guida 9/2022 sulla notifica delle violazioni dei dati personali ai sensi del RGPD", adottate dal Comitato europeo per la protezione dei dati il 28 Marzo 2023 (che hanno sostituito le precedenti "Linee guida sulla notifica delle violazioni dei dati personali ai sensi del Regolamento (UE) 2016/679" adottate dal Gruppo di Lavoro Articolo 29 per la Protezione dei Dati, da ultimo il 6 febbraio 2018 e fatte proprie dal Comitato europeo per la protezione dei dati il 25 maggio 2018), raccomandano al responsabile di "effettuare la notifica al titolare del trattamento tempestivamente, fornendo successivamente le eventuali ulteriori informazioni sulla violazione di cui venga a conoscenza"; ciò è "importante al fine di aiutare il titolare del trattamento a soddisfare l'obbligo di notifica all'autorità di controllo entro 72 ore".

Ciò anche quando, come è avvenuto nel caso di specie, un responsabile del trattamento ricorra a un subresponsabile per l'esecuzione di specifiche attività di trattamento per conto di un titolare; l'obbligo di informare il titolare del trattamento previsto dall'art. 33, par. 2, rimane in capo al responsabile iniziale, il quale non è tenuto a valutare il rischio derivante dalla violazione, prima di darne comunicazione al titolare del trattamento; al responsabile spetta soltanto stabilire se si è verificata una violazione dei dati personali e, in tal caso, informare tempestivamente il titolare; grava su quest'ultimo il compito di effettuare la predetta valutazione, nel momento in cui sia venuto a conoscenza della violazione.

Nel caso in esame, pertanto, NTT Data avrebbe dovuto informare il titolare del trattamento della violazione dei dati personali, senza ritardo, ovvero sin dall'11 e 12 ottobre 2018, data in cui ne aveva avuto contezza per il tramite di Truel IT.

Ciò al fine di consentire al titolare medesimo di:

di adottare tempestivamente le misure necessarie a rimuovere le vulnerabilità sopra citate, evitando così che le stesse potessero essere sfruttate da un eventuale attaccante;

verificare se le vulnerabilità fossero state già sfruttate per acquisire illecitamente dati personali e quindi contenere la portata dell'attacco informatico;

adempiere, se del caso, agli obblighi di notifica all'Autorità e di comunicazione agli interessati previsti dagli artt. 33 e 34 del Regolamento.

Si aggiunge altresì che la scelta della Società di esternalizzare l'esecuzione delle attività di vulnerability assessment e penetration testing ha verosimilmente contribuito al ritardo nella comunicazione della violazione al titolare, circostanza che ha poi inciso negativamente sulla tempestività delle misure correttive adottate dal titolare medesimo per rimuovere le citate vulnerabilità.

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 da NTT Data 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, alla luce delle considerazioni di cui al par. 4, si dichiara che NTT Data, in relazione alla violazione di dati personali in questione – a latere delle considerazioni sui profili di responsabilità di UniCredit S.p.a. quale titolare del trattamento che sono oggetto di un distinto e separato provvedimento – ha posto in essere una condotta illecita in violazione degli artt. 28, par. 2, e 33, par. 2, del Regolamento.

Pertanto, considerata la natura delle violazioni, 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, par. 4, lett. a), del Regolamento.

Con riferimento agli elementi elencati dall'art. 83, par. 2, del Regolamento ai fini dell'applicazione della sanzione amministrativa pecuniaria e della relativa quantificazione, tenuto conto che la sanzione deve essere "in ogni singolo caso effettiva, proporzionata e dissuasiva" (art. 83, par. 1 del Regolamento), si rappresenta che, nel caso di specie, sono state tenute in considerazione le circostanze sotto riportate:

a) con riferimento alla natura, alla gravità e alla durata delle violazioni (art. 83, par. 2, lett. a), del Regolamento) è stata considerata rilevante la circostanza che la Società ha avuto contezza delle stesse solo a seguito dell'avvenuta violazione dei dati personali e delle richieste di elementi da parte del titolare del trattamento;

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 negligente della Società quale responsabile del trattamento che non si è conformata alla disciplina in materia di protezione dei dati personali, sia relativamente agli obblighi che incombono al responsabile medesimo (artt. 28, par. 2 e 33, par. 2 del Regolamento), sia con riferimento alle legittime istruzioni del titolare del trattamento (divieto di affidare a terze parti l'esecuzione, parziale o totale, delle attività di vulnerability assessment e penetration testing);

c) l'assenza di precedenti provvedimenti dell'Autorità nei confronti della società (art. 83, par. 2, lett. e), del Regolamento);

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

e) con riferimento alle categorie di dati personali interessate dalla violazione (art. 83, par. 2, lett. g), del Regolamento), è stato che i dati oggetto di violazione erano costituiti da dati comuni degli interessati.

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 800.000 (ottocentomila) per la violazione degli artt. 28, par. 2, e 33, par. 2, del Regolamento.

In tale quadro, anche in considerazione della tipologia di violazione accertata, 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. 28, par. 2, e 33, par. 2, del Regolamento.

ORDINA

a NTT Data Italia S.p.a., con sede legale in legale in Milano, Via Ernesto Calindri, 4, C.F./P.I. 00513990010, ai sensi dell'art. 58, par. 2, lett. i), del Regolamento, di pagare la somma di euro 800.000 (ottocentomila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate nel presente provvedimento;

INGIUNGE

alla medesima NTT Data Italia S.p.a. di pagare la somma di euro 800.000 (ottocentomila) 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