Ordinanza ingiunzione nei confronti di UniCredit S.p.A. - 10 giugno 2020 [9429195]

VEDI ANCHE Newsletter del 26 giugno 2020

[doc. web n. 9429195]

Ordinanza ingiunzione nei confronti di UniCredit S.p.A. - 10 giugno 2020

Registro dei provvedimenti
n. 99 del 10 giugno 2020

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, alla quale hanno preso parte il dott. Antonello Soro, presidente, la dott.ssa Augusta Iannini, vicepresidente, la dott.ssa Giovanna Bianchi Clerici e la prof.ssa Licia Califano, componenti e il dott. Giuseppe Busia, segretario generale;

VISTA la legge 24 novembre 1981, n. 689, e successive modificazioni e integrazioni, con particolare riferimento all'art. 1, comma 2;

RILEVATO che l'Ufficio del Garante, con atto n. 15976/119444 del 14 maggio 2019 che qui deve intendersi integralmente richiamato, ha contestato a UniCredit S.p.A. (di seguito "la Società"), in persona del legale rappresentante pro-tempore, con sede legale in Milano, Piazza Gae Aulenti n. 3, P.I. 00348170101, le violazioni amministrative previste dagli artt. 162, comma 2-bis, 162, comma 2-ter, e 164-bis, comma 2, del Codice in materia di protezione dei dati personali (d.lgs. 196/2003, di seguito denominato "Codice", nella formulazione antecedente alle modifiche intervenute a seguito dell'entrata in vigore del d.lgs. 101/2018), in relazione agli artt. 33 e 154, comma 1, lett. c), del medesimo Codice;

RILEVATO che, dall'esame degli atti del procedimento sanzionatorio, avviato con l'atto di contestazione di cui sopra, è emerso che:

- la Società, in data 25 luglio 2017, ha comunicato a questa Autorità di aver subito un'intrusione informatica, verificatasi in due momenti distinti in un arco temporale compreso tra aprile 2016 e luglio 2017, che ha determinato accessi non autorizzati a dati personali riferiti a circa 762.000 interessati; tali accessi abusivi sono stati effettuati con le utenze di alcuni dipendenti di un partner commerciale esterno (la società Penta Finanziamenti Italia S.r.l., di seguito "Penta") attraverso un applicativo denominato Speedy Arena. In particolare, è risultato che i dati, oggetto della violazione, consistevano in: dati anagrafici e di contatto, professione, livello di studio, estremi identificativi di un documento di riconoscimento e informazioni relativi a datore di lavoro, salario, importo del prestito, stato del pagamento, "approssimazione della classificazione creditizia del cliente" e codice Iban;

- l'Ufficio ha avviato una complessa attività istruttoria nei confronti della Società, culminata in un accertamento ispettivo che si è svolto in data 22, 23 e 24 ottobre 2018;

- all'esito dell'istruttoria svolta dall'Ufficio, il Garante ha adottato, in data 28 marzo 2019, il provvedimento n. 87 (reperibile in www.gpdp.it, doc. web n. 9104006, di seguito "provvedimento"), al quale si fa integralmente richiamo, con il quale ha dichiarato illecito il trattamento dei dati personali posto in essere da Unicredit, in qualità di titolare del trattamento, perché effettuato in violazione delle misure minime di sicurezza previste dagli artt. 33 e ss. del Codice e dal disciplinare tecnico di

cui all'All. B) al Codice stesso e delle misure prescritte con il provvedimento n. 192 del 12 maggio 2011, recante "Prescrizioni in materia di circolazione delle informazioni in ambito bancario e di tracciamento delle operazioni bancarie" (doc. web n. 1813953);

- la violazione delle misure minime di sicurezza ex art. 33 del Codice è stata accertata con riferimento all'inosservanza delle regole nn. 12 e 13 del disciplinare tecnico di cui all'All. B) al Codice, in relazione all'utilizzo di un non idoneo sistema di autorizzazione dell'applicativo Speedy Arena e all'assenza del "limite di accesso" dei profili di autorizzazione ai soli dati necessari per effettuare le operazioni di trattamento;

-la violazione delle misure prescritte con il provvedimento n. 192 del 12 maggio 2011 è stata accertata in relazione alla inadeguatezza e alla non corretta conservazione dei log di tracciamento delle operazioni svolte sull'applicativo Speedy Arena, alla mancata implementazione di alert per le operazioni svolte attraverso il citato applicativo e alla mancata esecuzione di attività di audit interni di controllo;

RILEVATO che, con il citato atto del 14 maggio 2019, sono state contestate alla Società, in qualità di titolare del trattamento ai sensi degli artt. 4, comma 1, lett. f), e 28 del Codice:

- la violazione amministrativa prevista dall'art. 162, comma 2-bis, del Codice, in relazione all'art. 33, con riferimento alla mancata adozione delle misure minime di sicurezza;

- la violazione amministrativa prevista dall'art. 162, comma 2-ter, del Codice, in relazione all'art. 154, comma 1, lett. c), con riferimento all'inosservanza delle prescrizioni impartite dal Garante con il provvedimento n. 192 del 12 maggio 2011;

- infine, la violazione prevista dall'art. 164-bis, comma 2, del Codice, in riferimento alla circostanza che le violazioni commesse sono riferite a banche date di particolare rilevanza o dimensioni;

RILEVATO dal rapporto predisposto dall'Ufficio ai sensi dell'art. 17 della legge n. 689/1981 che non risulta effettuato il pagamento in misura ridotta in relazione alle violazioni di cui agli artt. 162, comma 2-bis, e 162, comma 2-ter, del Codice;

VISTI gli scritti difensivi, inviati in data 12 giugno 2019 ai sensi dell'art. 18 della legge n. 689/1981, che qui si richiamano integralmente, con cui la Società ha illustrato le ragioni per le quali non sussisterebbero i presupposti per l'applicazione delle sanzioni in relazione alle violazioni oggetto di contestazione e ha, in sintesi, dichiarato che:

- con riferimento alla violazione delle misure di sicurezza di cui all'art. 33 del Codice, il sistema di autorizzazione adottato, rispetto all'applicativo Speedy Arena, era pienamente conforme alle disposizioni contenute nella regola 12 del Disciplinare tecnico di cui all'All. B) al Codice, vigente all'epoca dei fatti, posto che "non si è verificato alcun errore nella definizione dei profili di autorizzazione che erano correttamente impostati ed operativi". Invece, "l'accesso indebito ai dati personali è stato possibile solo a causa della gestione scorretta delle credenziali di accesso da parte di Penta che hanno consentito il successivo sfruttamento di un baco dell'applicativo". L'applicativo Speedy Arena poteva essere utilizzato solo attraverso Extranet, ovvero un'estensione della rete aziendale idonea a consentire ai soggetti operanti all'esterno della Società di accedere alle informazioni o ai servizi della Società stessa, il cui accesso (analiticamente descritto al punto 3.1, lett. a) e b), dello scritto difensivo) era possibile attraverso un canale criptato e previo superamento di una doppia procedura di autenticazione informatica da parte dell'utente;

- a differenza di quanto rilevato nel Provvedimento e successivamente oggetto di contestazione, "i profili di autorizzazione per ciascun incaricato o per classi omogenee di incaricati di UniCredit sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento". La Società, pertanto, sostiene di aver definito correttamente i livelli di accesso all'applicativo Speedy Arena, ma che, a causa di un utilizzo improprio delle credenziali di accesso da parte degli utenti di Penta, cui ha fatto seguito lo sfruttamento di un bug informatico dei sistemi di back-end del citato applicativo, è stato possibile superare le restrizioni di visibilità e le segregazioni degli accessi, che invece erano state poste in essere correttamente;

- "la circostanza che non sia stato possibile accedere ai log di tracciamento delle operazioni effettuate (…) e che tali log non riportassero la registrazione del codice del cliente interessato dall'operazione di accesso ai dati bancari da parte dell'incaricato non implica la totale inadeguatezza delle misure di sicurezza adottate". Infatti, la Società aveva adottato un

sistema di tracciamento delle operazioni bancarie, ad integrazione e complemento dei sistemi di raccolta dei log per singoli applicativi, che le ha permesso di ricostruire gli eventi legati al data breach. In particolare, è stato possibile individuare la data di inizio della violazione e la sua portata, grazie al sistema di collezione dei log che raccoglieva i log del firewall, il quale includeva: il numero della pratica, il codice utenza dell'operatore che ha effettuato l'operazione di accesso, l'indirizzo IP da cui viene effettuata l'operazione, la data e l'ora di esecuzione dell'operazione e la tipologia di operazione posta in essere conformemente alle misure prescritte al punto 1, lett. b), del provvedimento del 12 maggio 2011;

- infine, per quanto riguarda la contestazione relativa alla mancata implementazione di alert, la società ha dichiarato che, già all'epoca degli eventi contestati, era presente un sistema di firewall che filtrava e valutava l'ammontare del traffico sul complesso degli applicativi della società che, al superamento di soglie particolarmente elevate di traffico, inviava un alert "senza riuscire a identificare un numero di interrogazioni come quelle del caso in esame che, benché elevate per il singolo applicativo, non erano rilevanti rispetto al traffico informatico che un istituto di credito come Unicredit gestisce quotidianamente";

LETTO il verbale di audizione, svoltasi in data 6 novembre 2019, ai sensi dell'art. 18 della legge n. 689/1981, con cui la parte ha ribadito quanto già dichiarato nelle memorie difensive, chiedendo l'archiviazione del procedimento sanzionatorio o, in subordine, l'applicazione delle sanzioni nella misura del minimo edittale, in considerazione del fatto che gli interessati non hanno subito alcun pregiudizio e che la Società ha ulteriormente rafforzato le proprie misure di sicurezza;

CONSIDERATO che, salvo che il fatto non costituisca più grave reato, chiunque, in un procedimento dinanzi al Garante, dichiara o attesta falsamente notizie o circostanze o produce atti o documenti falsi ne risponde ai sensi dell'art. 168 del Codice "Falsità nelle dichiarazioni al Garante e interruzione dell'esecuzione dei compiti o dell'esercizio dei poteri del Garante";

CONSIDERATO altresì che i rilevanti profili di illiceità del trattamento emersi nel caso di specie, quale conseguenza della mancata adozione di misure tecniche e organizzative adeguate, esigono comunque l'intervento correttivo di questa Autorità nei termini odierni, al fine di salvaguardare i diritti e le libertà fondamentali degli interessati a prescindere dalla notificazione della violazione di dati personali effettuata dal titolare del trattamento;

CONSIDERATO che le argomentazioni addotte non sono idonee ad escludere la responsabilità della parte in relazione a quanto contestato. Infatti, nei propri scritti difensivi, la parte ha chiarito molti aspetti legati all'impostazione dei sistemi di autenticazione informatica che, sulla base degli accertamenti eseguiti dall'Ufficio, risultavano effettivamente conformi alle disposizioni indicate nel Disciplinare tecnico. Diversamente, hanno formato oggetto di contestazione, perché ritenuti posti in essere in violazione della disciplina vigente all'epoca dei fatti, gli aspetti legati alla impostazione dei sistemi di autorizzazione degli incaricati del trattamento, di cui alle regole n. 12 e n. 13 del citato Disciplinare tecnico. La documentazione acquisita durante la fase istruttoria e, soprattutto, le verifiche effettuate nel corso dell'accertamento ispettivo, hanno evidenziato un'errata progettazione del sistema di autorizzazione dell'applicativo Speedy Arena che risultava particolarmente debole sia a livello di front-end che di back-end. D'altra parte, la stessa Società aveva rappresentato, nell'audit report del 30 novembre 2017, come l'applicativo Speedy Arena fosse stato sviluppato per essere utilizzato solo dai dipendenti interni (i quali non hanno restrizione sulla visibilità delle pratiche) e che fosse stato successivamente esteso anche a soggetti esterni alla Società, implementando una segregazione degli accessi che poi non si è rivelata sicura. Infatti, "sfruttando alcune debolezze della sicurezza dell'applicativo in questione, soggetti ignoti, attraverso le credenziali assegnate al personale Penta, hanno avuto accesso ai dati personali presenti in pratiche di finanziamento che non rientravano nell'ambito del mandato di Penta, determinando in questo modo il data breach oggetto della comunicazione del 25 luglio 2017" (verbale del 22 ottobre 2018, p. 3). L'accertata presenza di alcune debolezze dell'applicativo Speedy Arena, ancorché causate da un bug informatico (circostanza che non è stata mai rappresentata dalla Società nel corso dell'istruttoria), resta comunque riconducibile alla sfera di responsabilità del titolare del trattamento che, nell'approntare le misure di cui all'All. B) al Codice, volte ad assicurare un livello minimo di protezione dei dati personali, deve garantirne l'efficacia nel tempo e non può, quindi, essere imputata a Penta. È risultato, infatti, che gli operatori di Penta, dopo aver superato le procedure di autenticazione informatica, potevano accedere a una qualsiasi pratica di finanziamento (sia di "prestito al consumo" che di "cessione del quinto dello stipendio"), sfruttando le citate debolezze dell'applicativo Speedy Arena, semplicemente modificando il numero identificativo della pratica e, soprattutto, indipendentemente dal profilo di autorizzazione a loro attribuito. Laddove, invece, i profili di autorizzazione fossero stati correttamente impostati e configurati con le limitazioni di accesso, ciascun operatore di Penta avrebbe potuto consultare solo i dati relativi alle pratiche di propria competenza, in quanto il sistema di autorizzazione avrebbe bloccato ogni accesso su pratiche gestite da altri soggetti. È stato, invece, verificato che le limitazioni di accesso, associate ai profili di autorizzazione, non funzionassero correttamente. Si rileva, diversamente da quanto dedotto dal titolare, che la possibilità di

visionare anche pratiche non di propria competenza è una circostanza che prescinde dall'uso improprio delle utenze in uso agli incaricati. Pertanto, devono essere confermate le violazioni delle misure di sicurezza di cui all'art. 33 del Codice.

Per quanto riguarda la violazione relativa alla inosservanza del provvedimento n. 192 del 12 maggio 2011, si rileva che, indipendentemente dalla circostanza che la Società sia riuscita a individuare gli aspetti fondamentali legati al data breach e ad adottare le necessarie misure, è indubbio che i log di tracciamento non fossero stati correttamente implementati, sia con riferimento ai tempi di conservazione dei log (che era inferiore a 24 mesi a decorrere dalla data di registrazione dell'operazione) sia con riferimento alla mancata indicazione del codice del cliente interessato dall'operazione di accesso ai dati bancari. Con riferimento al primo aspetto, la stessa Società ha rappresentato che "non essendo disponibili file di log anteriori al 28 aprile 2016, la portata esatta della violazione dei dati non può essere determinata" (audit report del 30 novembre 2017), per l'impossibilità di individuare elementi utili. Con riferimento, invece, al secondo aspetto, si osserva che il Garante ha ritenuto che la registrazione nei log di tracciamento del codice del cliente (unitamente alle altre informazioni individuate al punto 4.2.1 del provvedimento n. 192) sia fondamentale al fine di assicurare un effettivo controllo delle attività svolte sui dati dei clienti da parte di ciascun incaricato del trattamento. Tra l'altro, tale misura prescrittiva è funzionale alle altre indicate nel provvedimento, tra cui quella relativa all'attivazione di specifici alert volti a rilevare intrusioni o accessi anomali e abusivi ai sistemi informativi, analizzando e correlando tra loro i log di tracciamento relativi a tutti gli applicativi utilizzati dagli incaricati del trattamento. La circostanza che all'interno dei log fosse presente il numero della pratica, in luogo del codice del cliente, non avrebbe reso possibile, se non mediante una complessa e articolata operazione di incrocio dei dati presenti nei log con i dati della clientela (anche considerando che una stessa pratica può riferirsi a più clienti o che pratiche diverse possono riferirsi al medesimo cliente) correlare tra loro i log di tracciamento generati da applicativi diversi della Società. La Società stessa ha dichiarato, nel corso dell'istruttoria, che all'epoca in cui si sono verificati gli accessi illegittimi, non esisteva un meccanismo di alert utile a rilevare comportamenti anomali, a fronte di operazioni di accesso eseguite da utenti esterni alla Società (quali gli operatori Penta). Infatti, rispetto allo specifico episodio di data breach oggetto del presente procedimento, è emerso che "le pratiche dei clienti sono state consultate con una frequenza sino a 10 al secondo, in ordine consecutivo da un singolo utente", senza che tale comportamento anomalo venisse rilevato, e che la mancata attivazione di alert è stata una delle condizioni che hanno "contribuito all'esfiltrazione dei dati, la quale è perdurata per almeno 14 mesi senza che venisse individuata" (audit report del 30 novembre 2017). Per quanto sopra, si ritiene che sussistano in capo alla Società responsabilità in ordine alla mancata adozione delle misure prescritte con il provvedimento n. 192;

RILEVATO, quindi, che UniCredit S.p.A., in qualità di titolare del trattamento ai sensi degli artt. 4, comma 1, lett. f) e 28 del Codice, risulta aver commesso le violazioni di cui agli artt. 162, comma 2-bis, e 162, comma 2-ter, del medesimo Codice, come indicate nell'atto di contestazione n. 15976/119444 del 14 maggio 2019, nonché la violazione di cui all'art. 164-bis, comma 2, per aver commesso le suddette violazioni in relazione a banche dati di particolare rilevanza e dimensione;

CONSIDERATO che, ai fini dell'ammontare delle sanzioni pecuniarie, occorre tener conto, ai sensi dell'art. 11 della legge n. 689/1981, dell'opera svolta dall'agente per eliminare o attenuare le conseguenze della violazione, della gravità della violazione, della personalità e delle condizioni economiche del contravventore;

CONSIDERATO che, nel caso in esame:

- in ordine all'aspetto della gravità, gli elementi relativi all'intensità dell'elemento psicologico e all'entità del pericolo e del pregiudizio vanno valutati tenendo conto che le violazioni risultano commesse in relazione a un rilevante numero di interessati;

- ai fini della valutazione dell'opera svolta dall'agente, deve evidenziarsi che la Società, successivamente al data breach in esame, ha adottato diverse misure e ha avviato iniziative volte a rafforzare la sicurezza dei propri sistemi informatici;

- circa la personalità dell'autore della violazione, deve essere considerata la circostanza che non risultano precedenti procedimenti sanzionatori nei confronti di UniCredit S.p.A.;

- in merito alle condizioni economiche dell'agente, è stato preso in considerazione il bilancio di esercizio per l'anno 2018;

RITENUTO, quindi, di dover determinare, ai sensi dell'art. 11 della legge n. 689/1981, l'importo delle sanzioni pecuniarie, in ragione dei suddetti elementi valutati nel loro complesso, nella misura di:

- euro 120.000,00 (centoventimila) per la violazione di cui all'art. 162, comma 2-bis, del Codice, in relazione all'art. 33;

- euro 180.000,00 (centottantamila) per la violazione di cui all'art. 162, comma 2-ter, del Codice, in relazione all'art. 154, comma 1, lett. c);

- euro 300.000,00 (trecentomila) per la violazione di cui all'art. 164-bis, comma 2, del Codice;

per un importo complessivo pari a euro 600.000,00 (seicentomila);

VISTA la documentazione in atti;

VISTA la legge n. 689/1981 e successive modificazioni e integrazioni;

VISTE le osservazioni formulate dal Segretario generale ai sensi dell'art. 15 del regolamento del garante n. 1/2000, adottato con deliberazione del 28 giugno 2000;

RELATORE la dott.ssa Augusta Iannini;

ORDINA

a UniCredit S.p.A., in persona del legale rappresentante pro-tempore, di pagare la somma di euro 600.000,00 (seicentomila), a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione;

INGIUNGE

alla predetta società di pagare la somma di euro 600.000,00 (seicentomila), secondo le modalità indicate in allegato, entro 30 giorni dalla notificazione del presente provvedimento, pena l'adozione dei conseguenti atti esecutivi a norma dall'art. 27 della legge 24 novembre 1981, n. 689.

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

Roma, 10 giugno 2020

IL PRESIDENTE
Soro

IL RELATORE
Iannini

IL SEGRETARIO GENERALE
Busia