filodiritto
APPROFONDISCI SEMPRE
Tribunale Bologna 24.07.2007, n.7770 - ISSN 2239-7752
Direttore responsabile: Antonio Zama

Misure urgenti prescritte dal Garante Privacy per la sicurezza del servizio PEC

07 Aprile 2020
Simona Loprete

1. Premessa

Il Garante privacy adotta un provvedimento d'urgenza (Provvedimento correttivo d'urgenza n. 228 del 18 dicembre 2019) a tutela degli utenti dopo aver rilevato che le procedure informatiche della società Aruba PEC non erano capaci di assicurare la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento così come richiesto dall'articolo 32 del GDPR e che gli interessati erano gravemente esposti al rischio di trattamenti non autorizzati o illeciti.

Venerdì 6 marzo 2020, il Garante per la protezione dei dati personali ha reso noto per la prima volta un provvedimento che aveva adottato d'urgenza in data 18 dicembre 2019 nei confronti di Aruba Posta Elettronica Certificata S.p.a. al fine di **dettare misure di sicurezza relative al servizio PEC fornito**. L'intenzionale tarda pubblicazione da parte dell'Autorità si era resa necessaria in considerazione delle **rilevate vulnerabilità del servizio e del rischio di sfruttamento delle stesse da parte di eventuali aggressori**.

Il servizio PEC di Aruba è particolarmente noto e il suo utilizzo è largamente diffuso non solo tra i professionisti e le società private ma anche tra soggetti pubblici, quali amministrazioni centrali e locali dello Stato. Va da sè che gli interessati esposti ad un potenziale trattamento illecito dei loro dati personali appartenessero alle categorie più disparate e che l'obiettivo che si poneva come prioritario ed urgente consistesse nell'**implementazione da parte della società Aruba delle misure di sicurezza ritenute dall'Autorità assenti, ridotte o compromesse, al fine di tutelare i diritti e le libertà dei suddetti interessati**.

Aruba ha informato di aver attuato, nei termini individuati nel provvedimento, tutte le misure correttive impartite ma si attende un ulteriore intervento del Garante nel quale si valutino ulteriori aspetti relativi al trattamento dei dati svolto da Aruba e alle eventuali rispettive violazioni, comprese le determinazioni sanzionatorie.

2. Accertamento ispettivo del Garante

Nel settembre del 2019 il Garante privacy aveva avviato un accertamento ispettivo nei confronti di Aruba Posta Elettronica Certificata S.p.a. **per verificare** la conformità della gestione del servizio PEC offerto dalla società alle disposizioni applicabili in materia di protezione dei dati personali.

L'intervento dell'Autorità era stato **sollecitato dalle notifiche, ricevute da diversi titolari di caselle PEC, di numerosi casi di violazione dei dati personali relativi alla perdita o all'intervenuta indisponibilità di dati a seguito della ricezione di messaggi PEC contenenti allegati infetti da virus informatici**.

Nel corso dell'istruttoria, il Garante aveva appreso in via preliminare che la società si avvaleva di un'ingente rete di partner per la commercializzazione e l'attivazione del servizio PEC. Tali partner, mediante un'applicazione web denominata "Area Clienti" resa disponibile da Aruba, potevano attivare e gestire le nuove caselle di PEC e in particolare fino al 24 settembre 2019 provvedevano a impostare e assegnare ai titolari delle nuove caselle di PEC delle credenziali di autenticazione per consentirne l'accesso, inviando poi tali password in chiaro, tramite la medesima applicazione, all'indirizzo di posta elettronica ordinaria del titolare della casella PEC.

La procedura di generazione e consegna delle credenziali non prevedeva altresì
né requisiti di complessità nella composizione (se non almeno 8 caratteri)
né l'aggiornamento periodico
né l'obbligo (bensì solo il consiglio) di modificare la password fornita nel momento dell'attivazione della casella.
Una procedura così debole in termini di applicazione dei principi privacy di protezione e sicurezza dei dati e utilizzata dalla Società per ben 559.151 attivazioni senza effettiva successiva modifica della password, è stata ritenuta **pericolosa dal Garante perché capace di esporre innumerevoli interessati a utilizzi impropri o furti d'identità**.
Il Garante privacy, in secondo luogo, rilevava che **i log dei messaggi PEC inviati o ricevuti** (da 6.5 milioni di caselle PEC nel corso dei 30 mesi precedenti) **erano accessibili e trasferibili non solo dai titolari delle caselle di PEC ma anche da diversi soggetti coinvolti a vario titolo nella gestione del servizio mediante un'unica utenza condivisa e le medesime credenziali** all'interno di una applicazione web denominata "PEC Log".

Fermo restando l'obbligo di conservazione dei log dei messaggi PEC, l'Autorità contestava le modalità con cui si effettuavano, da rete internet, le operazioni di consultazione e di esportazione dei log dei messaggi inviati o ricevuti da tutte le caselle PEC gestite da Aruba, soprattutto dal momento che l'accesso avveniva tramite un'unica utenza, con elevati privilegi di amministrazione, tramite credenziali condivise da più operatori e che, di conseguenza, non consentiva di identificare e

controllare chi tra gli loro avesse compiuto le azioni.

Inoltre, veniva constatato che, da un lato, **i log di tracciamento degli accessi e delle operazioni compiute** sull'applicazione "Area Clienti" **riportavano in chiaro le credenziali di utenze tecniche** che servivano a gestire alcuni servizi informatici aumentando così in maniera esponenziale la possibilità di accessi illeciti non solo da parte di soggetti interni non autorizzati ma anche in caso di attacchi esterni.

D'altro lato, **nei suddetti log erano anche presenti informazioni non necessarie riferite ai soggetti** per cui veniva richiesta l'attivazione di una casella PEC o di un altro servizio, quali il nome, il cognome, il codice fiscale, il numero di telefono, l'indirizzo di posta elettronica ordinaria, la denominazione della casella PEC, la username e la relativa password.

3. L'intervento d'urgenza e le ingiunzioni ad Aruba

Il Garante privacy, dunque, in considerazione delle diverse criticità rilevate e dei conseguenti profili di rischio configurati a carico degli interessati, **è intervenuto d'urgenza per sopperire alla mancata protezione dei dati all'interno dei sistemi informatici di Aruba che, in qualità di titolare del trattamento, sarebbe stato obbligato a garantirne la sicurezza e a evitare trattamenti non autorizzati, illeciti o anche la perdita, la distruzione o i danni accidentali ai sensi degli articoli 5, paragrafo 1, lettera f) e 32 del Regolamento UE 2016/679 ("GDPR")**.

L'Autorità, in particolare, ha ingiunto ad Aruba, ai sensi dell'articolo 58, paragrafo 2, lettera d) del GDPR, di adottare le seguenti misure:

1. inviare alle 559.151 caselle PEC, che per l'accesso utilizzavano ancora la password di attivazione del servizio impostata e rilasciata in modo non sicuro da uno dei partner della società, una comunicazione in cui si avvisavano i titolari che in caso di mancata modifica della password entro un termine congruo (individuato da Aruba) sarebbe stata adottata una **procedura di modifica obbligatoria**, che Aruba doveva implementare che entro 30 giorni dalla ricezione del provvedimento. **L'obbligo di modifica**, rileva infatti il Garante, **avrebbe dovuto essere imposto al primo accesso del titolare della nuova casella di PEC**;
2. **relativamente alle operazioni di consultazione ed esportazione dei log dei messaggi** inviati e ricevuti da tutte le caselle gestiste da Aruba PEC, l'inibizione dell'accesso all'applicazione web "PEC Log" agli operatori e **l'assegnazione a un solo soggetto autorizzato delle credenziali di autenticazione dell'utenza, previa modifica della password**. Tali operazioni venivano svolte infatti in evidente violazione dei principi di sicurezza del trattamento e senza un'adeguata valutazione dei rischi connessi alla possibilità di accedere a queste informazioni e il Garante ha quindi anche **imposto che tutti gli utenti dell'applicazione web denominata "PEC Log" siano dotati di credenziali di autenticazione ad uso esclusivo degli stessi;**
3. per la memorizzazione all'interno dei file di log prodotti dall'applicazione web denominata "Area Clienti", di credenziali di autenticazione di utenze tecniche e di informazioni non necessarie al perseguimento delle finalità di controllo e sicurezza connesse al tracciamento, la **ridefinizione delle modalità di tracciamento degli accessi e delle operazioni** compiute sull'applicazione web "Area Clienti" e su ogni altra applicazione web che produca file di log, **prevedendo che questi non contengano credenziali di autenticazione di utenze tecniche, né ogni altra informazione non indispensabile per le finalità di controllo e sicurezza connesse al tracciamento alla luce del principio di minimizzazione** e la modifica delle password utilizzate dalle utenze tecniche riportate all'interno dei file di log.

TAG: *GDPR, PEC, riservatezza, dati personali*

Avvertenza
La pubblicazione di contributi, approfondimenti, articoli e in genere di tutte le opere dottrinarie e di commento (ivi comprese le news) presenti su Filodiritto è stata concessa (e richiesta) dai rispettivi autori, titolari di tutti i diritti morali e patrimoniali ai sensi della legge sul diritto d'autore e sui diritti connessi (Legge 633/1941). La riproduzione ed ogni altra forma di diffusione al pubblico delle predette opere (anche in parte), in difetto di autorizzazione dell'autore, è punita a norma degli articoli 171, 171-bis, 171-ter, 174-bis e 174-ter della menzionata Legge 633/1941. È consentito scaricare, prendere visione, estrarre copia o stampare i documenti pubblicati su Filodiritto nella sezione Dottrina per ragioni esclusivamente personali, a scopo informativo-culturale e non commerciale, esclusa ogni modifica o alterazione. Sono parimenti consentite le citazioni a titolo di cronaca, studio, critica o recensione, purché accompagnate dal nome dell'autore dell'articolo e dall'indicazione della fonte, ad esempio: Luca Martini, La discrezionalità del sanitario nella qualificazione di reato perseguibile d'ufficio ai fini dell'obbligo di referto ex. art 365 cod. pen., in "Filodiritto" (https://www.filodiritto.com), con relativo collegamento ipertestuale. Se l'autore non è altrimenti indicato i diritti sono di Inforomatica S.r.l. e la riproduzione è vietata senza il consenso esplicito della stessa. È sempre gradita la comunicazione del testo, telematico o cartaceo, ove è avvenuta la citazione.
