Ordinanza ingiunzione nei confronti di Agenzia regionale protezione ambientale Campania (ARPAC) - 14 gennaio 2021 [9538748]

[doc. web n. 9538748]

Ordinanza ingiunzione nei confronti di Agenzia regionale protezione ambientale Campania (ARPAC) - 14 gennaio 2021

Registro dei provvedimenti
n. 5 del 14 gennaio 2021

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, il dott. Agostino Ghiglia e l'avv. Guido Scorza, componenti, e il cons. Fabio Mattei, segretario generale;

VISTO il Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE, "Regolamento generale sulla protezione dei dati" (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");

VISTO il regolamento n. 1/2019 concernente le procedure interne aventi rilevanza esterna, finalizzate allo svolgimento dei compiti e all'esercizio dei poteri demandati al Garante per la protezione dei dati personali, approvato con deliberazione n. 98 del 4 aprile 2019, pubblicato in G.U. n. 106 dell'8 maggio 2019 e reperibile sul sito www.garanteprivacy.it, doc. web n. 9107633 (di seguito "regolamento del Garante n. 1/2019");

VISTA la documentazione in atti;

VISTE le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000 sull'organizzazione e il funzionamento dell'Ufficio del Garante per la protezione dei dati personali (doc. web n. 1098801);

Relatore il prof. Pasquale Stanzione;

PREMESSO

1. La violazione dei dati personali.

Con note ricevute in data XX e XX (rispettivamente, ns. prot. nn. XX e XX), l'Agenzia regionale protezione ambientale Campania (di seguito, "ARPAC" o "Agenzia") ha notificato a questa Autorità la violazione dei dati personali di cui all'art. 33 del Regolamento, consistente nella perdita di un dispositivo contenente dati personali.

Sulla base di quanto dichiarato dall'ARPAC nelle predette note:

- la violazione ha riguardato il furto di un hard disk esterno, avvenuto in data XX, presso i locali della U.O.C. Siti contaminati e Bonifiche dell'Agenzia;

- in tale dispositivo erano contenuti dati personali quali copie di documenti di riconoscimento, documenti di tipo fiscale (CUD, modelli F24 e 730), buste paga, pratiche di rimborso e un elenco contenente dati analitici riferiti a procedimenti giudiziari;

- non viene escluso "che il data breach sia stato doloso", e viene ritenuto che tale violazione "abbia comportato una illecita sottrazione e possibile divulgazione non autorizzata dei dati contenuti nell'hard disk esterno", e quindi che essa, "in virtù del numero degli interessati, della natura, numero e grado di sensibilità dei dati personali violati possa determinare un conseguente rischio per le libertà e i diritti degli interessati";

- tale violazione, inoltre, avrebbe compromesso sia la riservatezza dei summenzionati dati che la loro disponibilità, in quanto "il salvataggio di backup non [era] andato a buon fine, di conseguenza i dati [erano] andati quasi tutti irreparabilmente persi". Come specificato nella denuncia al Comando dei carabinieri effettuata in data XX, "I dati in questione erano stati oggetto di backup il XX, pertanto quelli salvati successivamente alla citata data sono andati persi";

- l'hard disk oggetto di sottrazione sarebbe stato "collegato al server installato in una stanza alla quale può accedere qualsiasi dipendente", nonché i dipendenti dell'ARPAC Multiservizi, società in house dell'Agenzia.

2. L'attività istruttoria.

L'Ufficio, con atto n. XX del XX (notificato in pari data mediante posta elettronica certificata), che qui deve intendersi integralmente riprodotto, ha avviato, ai sensi dell'art. 166, comma 5, del Codice, con riferimento alle specifiche situazioni di illiceità in esso richiamate, un procedimento per l'adozione dei provvedimenti di cui all'art. 58, par. 2, del Regolamento nei confronti dell'ARPAC, per la violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento.

Con nota del XX (ns. prot. n. XX del XX), l'ARPAC ha fatto pervenire le proprie memorie difensive, ai sensi dell'art. 166, comma 6, del Codice, ove ha rappresentato, in particolare, che:

- all'interno del più generale processo di adeguamento ai principi e alle regole del Regolamento, si è dotata, tra le altre cose, "di un sistema di gestione della sicurezza delle informazioni idoneo alla individuazione di eventuali vulnerabilità nell'architettura dei dati di ARPAC, aderendo al Contratto Quadro Consip relativo ai "Servizi di gestione delle identità digitali e sicurezza applicativa" -Deliberazione XX del XX" (descrivendo i servizi contrattualizzati), nonché, con riferimento alle risorse presenti sulla rete internet, di una serie misure di sicurezza a più livelli (protezione Firewall, misure di sicurezza per le singole postazioni di lavoro, misure di sicurezza per i server);

- con riferimento alla specifica vicenda, il server a cui era collegato l'hard disk sottratto "viene di norma utilizzato come "Server di Area Condivisa ad uso interno" in cui il personale tecnico dell'Area Analitica inserisce, nei files dei Rapporti di Prova Provvisori (Certificati di Analisi Provvisori) i dati derivanti dall'elaborazione dei parametri analitici determinati nei campioni in corso di analisi. […] Dall'istruttoria successiva compiuta […] si è riscontrato che nel suddetto server sono altresì memorizzati fogli di calcolo (in formato .xls), metodi di analisi, lettere di trasmissione di documentazione in formato word non firmate, proposte di deliberazioni o determinazione non firmate (trattasi di meri brogliacci in word, di lavoro in fase di studio ed elaborazione e non di "dati giudiziari" come erroneamente individuato nel Modulo preventivo di Segnalazione del Data Breach) documentazione a corredo delle stesse deliberazioni e/o determinazioni, quali richieste, offerte e dichiarazioni di fornitori", nonché copia dei documenti di identità dei rappresentanti legali di questi ultimi;

- all'interno del dispositivo si trovavano altresì "dati personali dei dipendenti abilitati all'accesso all'hard disk in questione, comunque protetto da password di accesso, nonché quelli dei propri familiari, [i quali] non sono mai stati richiesti da ARPAC. Difatti si precisa che tali dati sono stati impropriamente memorizzati direttamente dal suddetto personale e di volontaria iniziativa su tale supporto condiviso nelle proprie cartelle personali";

- tutti gli interessati sopra individuati (rappresentanti legali di fornitori, dipendenti, loro familiari e collaboratori esterni) sarebbero stati contattati al fine di essere informati "dell'avvenuto furto/smarrimento, a loro tutela", tramite comunicazioni effettuate via email, "esortando ad attivare ogni eventuale precauzione tesa alla protezione di potenziali conseguenze negative a causa della violazione subita";

- inoltre, "al fine di mitigare, sotto il profilo organizzativo, ulteriori e potenziali simili episodi", nonché "nelle more

dell'attuazione della Delibera n.XX del XX di adesione al Contratto Quadro Consip precedentemente citata", sono state adottate anche particolari misure di sicurezza fisiche. "Nel contempo tutto il personale è stato esortato a non utilizzare tutti gli strumenti agenziali informatici e non per scopi personali, come da Regolamento ICT";

- infine, "da ulteriori approfondimenti effettuati non risultano verificatesi conseguenze negative, che appaiono del tutto improbabili, relativamente all'eventuale utilizzo improprio dei dati personali sia dei dipendenti che degli esterni".

In relazione ad alcuni aspetti non ancora chiariti, in risposta alla richiesta di informazioni inviata dall'Ufficio, ai sensi dell'art. 157 del Codice, il XX (prot. n. XX), l'ARPAC ha fornito il riscontro richiesto, con note del XX e XX (rispettivamente, ns. prot. nn. XX e XX):

- allegando copia delle comunicazioni della violazione effettuate nei confronti degli interessati, ai sensi degli artt. 33 e 34 del Regolamento (risalenti al XX);

- producendo l'"auto dichiarazione dei dipendenti circa la volontaria memorizzazione dei propri dati personali all'interno dell'hard disk" (datata XX), in cui viene riconosciuto, dagli stessi "l'utilizzo improprio dei dati nonché dei danni che ne potrebbero conseguire";

- confermando l'avvenuto allestimento delle già citate misure di sicurezza fisiche;

- descrivendo l'"attuazione delle misure di sicurezza che il Servizio SINF ha inteso adottare, con particolare riferimento agli aspetti concernenti l'analisi dei rischi e le misure previste per eliminarli, o quantomeno mitigarli", allo stato in corso;

- trasmettendo, a mezzo corriere, un CD contenente "copia dei Rapporti di Prova relativi all'anno XX in formato .pdf e copia dei rispettivi fogli di calcolo in formato excel (brogliacci di lavoro), contenuti nell'Hard Disk oggetto di sottrazione, come prova evidente che gli stessi non contengono dati personali relativi alle condanne penali e ai reati o a connesse misure di sicurezza, di cui all'art. 10 del Regolamento";

- comunicando, infine, la richiesta effettuata al Comando dei carabinieri, volta ad acquisire informazioni circa gli eventuali sviluppi delle indagini avviate sulla vicenda.

3. Esito dell'attività istruttoria.

L'art. 5, par. 1, lett. f), del Regolamento pone il principio di integrità e riservatezza, ai sensi del quale i dati personali sono "trattati in maniera da garantire un'adeguata sicurezza dei dati personali, compresa la protezione, mediante misure tecniche e organizzative adeguate, da trattamenti non autorizzati o illeciti e dalla perdita, dalla distruzione o dal danno accidentali".

In attuazione di tale principio, il successivo art. 32 stabilisce 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, che comprendono, tra le altre, se del caso: a) la pseudonimizzazione e la cifratura dei dati personali; b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento; c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico; d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento" (par. 1) e 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" (par. 2).

Il caso in trattazione attiene, quindi, a una violazione di dati personali, intendendosi per essa una "violazione di sicurezza che comporta accidentalmente o in modo illecito la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso ai dati personali trasmessi, conservati o comunque trattati" (art. 4, n. 12), del Regolamento), essendosi realizzata "una illecita sottrazione e possibile divulgazione non autorizzata dei dati contenuti nell'hard disk esterno", come notificata da parte dell'ARPAC a questa Autorità ai sensi dell'art. 33 del Regolamento.

Rispetto al citato quadro giuridico, è emerso come la segnalata violazione dei dati personali sia stata resa possibile in ragione

dell'assenza delle misure necessarie per garantire un livello di sicurezza adeguato al rischio, richieste dall'art. 32 del Regolamento. Invero, dalla documentazione in atti risulta che non fossero stati adottati:

- accorgimenti necessari a consentire la continuità, su base permanente, e il ripristino della disponibilità dei dati personali sottratti, essendo stato riconosciuto, da parte dell'ARPAC, come le operazioni di backup non abbiano dato buon esito e quindi, anche solo volendo considerare quelli registrati fino al XX, "i dati [siano] andati quasi tutti irreparabilmente persi";

- tecniche in grado di assicurare la non identificabilità degli interessati ai quali i dati personali contenuti nel dispositivo si riferivano, per limitare il rischio della loro consultazione da parte di soggetti non debitamente autorizzati (come la pseudonimizzazione o la cifratura dei dati), tenuto anche conto che, presso il locale in cui era custodito il dispositivo sottratto, poteva accedere qualsiasi dipendente;

- procedure idonee a testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

Quanto addotto dal titolare del trattamento negli scritti difensivi pertiene le misure adottate successivamente all'episodio che ha causato la perdita dell'hard disk, o comunque in corso di predisposizione in quel periodo. Le iniziative descritte, seppur meritevoli di considerazione nei termini che si andranno di seguito ad esporre, non eliminano il fatto che, nel momento in cui si è verificata la perdita del dispositivo contenente i dati personali, non fossero state adottate misure tecniche e organizzative adeguate per assicurare la protezione da trattamenti non autorizzati o illeciti o dalla perdita, e per garantire un livello di sicurezza adeguato al rischio.

Per tali ragioni, sulla base degli elementi acquisiti e dei fatti emersi nell'ambito dell'attività istruttoria, risulta accertato che l'ARPAC, in relazione ai fatti in esame al momento della perdita dell'hard disk, si è resa responsabile della violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento.

4. Conclusioni.

Alla luce delle valutazioni sopra richiamate, tenuto conto delle dichiarazioni rese dal titolare del trattamento nel corso dell'istruttoria – della cui veridicità si può essere chiamati a rispondere ai sensi dell'art. 168 del Codice – si rappresenta che gli elementi forniti dal titolare del trattamento nelle memorie difensive, nonché negli elementi forniti a seguito della successiva richiesta di informazioni, seppure meritevoli di considerazione, non consentono di superare i rilievi notificati dall'Ufficio con l'atto di avvio del procedimento e risultano insufficienti a consentire l'archiviazione del procedimento, non ricorrendo, peraltro, alcuno dei casi previsti dall'art. 11 del regolamento del Garante n. 1/2019.

Pertanto, si confermano le valutazioni preliminari dell'Ufficio e si rileva l'illiceità del trattamento di dati personali effettuato da ARPAC, per non aver adottato misure tecniche e organizzative adeguate per assicurare la protezione da trattamenti non autorizzati o illeciti o dalla perdita, e per garantire un livello di sicurezza adeguato al rischio, in violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento.

La violazione delle predette disposizioni rende applicabile la sanzione amministrativa prevista dall'art. 83, par. 5, del Regolamento, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento medesimo.

5. Adozione dell'ordinanza ingiunzione per l'applicazione della sanzione amministrativa pecuniaria e delle sanzioni accessorie (artt. 58, par. 2, lett. i), e 83 del Regolamento; art. 166, comma 7, del Codice).

Il Garante, ai sensi ai sensi degli artt. 58, par. 2, lett. i), e 83 del Regolamento nonché dell'art. 166 del Codice, ha il potere di "infliggere una sanzione amministrativa pecuniaria ai sensi dell'articolo 83, in aggiunta alle [altre] misure [correttive] di cui al presente paragrafo, o in luogo di tali misure, in funzione delle circostanze di ogni singolo caso" e, in tale quadro, "il Collegio [del Garante] adotta l'ordinanza ingiunzione, con la quale dispone altresì in ordine all'applicazione della sanzione amministrativa accessoria della sua pubblicazione, per intero o per estratto, sul sito web del Garante ai sensi dell'articolo 166, comma 7, del Codice" (art. 16, comma 1, del regolamento del Garante n. 1/2019).

Al riguardo, tenuto conto dell'art. 83, par. 3, del Regolamento, nel caso di specie, la violazione delle disposizioni citate è soggetta all'applicazione della stessa sanzione amministrativa pecuniaria prevista dall'art. 83, par. 5, del Regolamento.

La predetta sanzione amministrativa pecuniaria inflitta, in funzione delle circostanze di ogni singolo caso, va determinata nell'ammontare tenendo in debito conto gli elementi previsti dall'art. 83, par. 2, del Regolamento.

In relazione ai predetti elementi, è stato considerato anche che la violazione ha riguardato dati personali che, per qualità e quantità, non denotano particolare rilievo – peraltro, stando a quanto dichiarato, in parte memorizzati impropriamente da parte degli interessati stessi – e da cui risultano esclusi categorie particolari di dati personali e dati personali relativi a condanne penali e reati, di cui agli artt. 9 e 10 del Regolamento, ed è emersa solamente in seguito ad un'azione presumibilmente criminosa posta in essere da parte di soggetti da identificare (in relazione alla quale l'Agenzia ha sporto immediatamente apposita denuncia presso le autorità competenti all'accertamento di eventuali responsabilità di carattere penale).

Inoltre, si è tenuto favorevolmente conto delle misure tecniche e organizzative che l'Agenzia ha dichiarato di aver già predisposto in via transitoria e di quelle in corso di predisposizione, nonché della piena cooperazione dimostrata nei confronti dell'Autorità nel fornire elementi per la ricostruzione dell'accaduto e per l'attenuazione dei possibili effetti negativi della violazione (compresa la comunicazione della violazione agli interessati ai sensi dell'art. 34 del Regolamento).

In ragione dei suddetti elementi, valutati nel loro complesso, si ritiene di determinare l'ammontare della sanzione pecuniaria nella misura di euro 8.000,00 (ottomila) per la violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento, quale sanzione amministrativa pecuniaria ritenuta, ai sensi dell'art. 83, par. 1, del Regolamento, effettiva, proporzionata e dissuasiva.

Tenuto conto che la violazione è emersa in occasione di una condotta presumibilmente criminosa che potrebbe presentare aspetti di carattere penale, stante peraltro la denuncia presentata dall'Agenzia alle autorità competenti, si ritiene altresì che debba applicarsi la sanzione accessoria della pubblicazione sul sito del Garante del presente provvedimento, prevista dall'art. 166, comma 7, del Codice e art. 16 del regolamento del Garante n. 1/2019.

Si rileva, infine, che ricorrono i presupposti di cui all'art. 17 del regolamento del Garante n. 1/2019.

TUTTO CIÒ PREMESSO IL GARANTE

rilevata l'illiceità del trattamento effettuato dall'Agenzia regionale protezione ambientale Campania (ARPAC) per violazione degli artt. 5, par. 1, lett. f), e 32 del Regolamento, nei termini di cui in motivazione,

ORDINA

all'Agenzia regionale protezione ambientale Campania (ARPAC), in persona del legale rappresentante pro tempore, con sede a Napoli, Via Vicinale S. Maria Del Pianto – Centro Polifunzionale, Torre 1, C.F. 07407530638, ai sensi degli artt. 58, par. 2, lett. i), e 83, par. 5, del Regolamento, di pagare la somma di euro 8.000,00 (ottomila) a titolo di sanzione amministrativa pecuniaria per le violazioni indicate in motivazione. Si rappresenta che il contravventore, ai sensi dell'art. 166, comma 8, del Codice, ha facoltà di definire la controversia mediante pagamento, entro il termine di 30 giorni, di un importo pari alla metà della sanzione comminata;

INGIUNGE

alla predetta Agenzia, in caso di mancata definizione della controversia ai sensi dell'art. 166, comma 8, del Codice, di pagare la somma di euro 8.000,00 (ottomila) 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 l. 689/1981;

DISPONE

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

b) ai sensi dell'art. 17 del regolamento del Garante n. 1/2019, l'annotazione nel registro interno dell'Autorità delle violazioni e delle misure adottate, ai sensi dell'art. 58, par. 2, del Regolamento, con il presente provvedimento.

Ai sensi degli artt. 78 del Regolamento, 152 del Codice e 10 del d.lgs. 150/2011, avverso il presente provvedimento è

possibile proporre ricorso dinnanzi 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, 14 gennaio 2021

IL PRESIDENTE
Stanzione

IL RELATORE
Stanzione

IL SEGRETARIO GENERALE
Mattei