DIRITTIFONDAMENTALI.IT
rivista on-line

Criticità nel trattamento dei dati personali da parte della "Piattaforma Rousseau" (Garante per la protezione dei dati personali, Provvedimento n. 83 del 4 aprile 2019)

***

AUTORITÁ GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Provvedimento su data breach - 4 aprile 2019

Registro dei provvedimenti
n. 83 del 4 aprile 2019

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

NELLA riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vicepresidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, 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 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 (d.lgs. 30 giugno 2003, n. 196, come modificato dal d.lgs. n. 101 del 10 agosto 2018, di seguito "Codice");

VISTO il provvedimento n. 548 del 21 dicembre 2017, doc. web n. 7400401 (di seguito "provvedimento" o "provvedimento n. 548"), con il quale l'Autorità, a conclusione dell'istruttoria relativa alla violazione dei sistemi informatici riferiti alla Piattaforma Rousseau e ad altri siti connessi al Movimento 5 Stelle, ha prescritto nei confronti dei relativi titolari del trattamento, ai sensi dell'art. 154, comma 1, lett. a), b) e c) del

Codice, l'adozione di misure necessarie e opportune al fine di rendere i trattamenti dei dati personali degli utenti dei predetti siti web conformi ai princìpi della disciplina in materia di protezione dei dati personali;

VISTI i successivi provvedimenti del 16 maggio 2018 (doc. web 8999795) e 4 ottobre 2018 (doc. web 9048594) con i quali l'Autorità ha prorogato i termini stabiliti con il provvedimento n. 548 fissando al 15 ottobre 2018 il termine ultimo per "dare completo adempimento alle prescrizioni contenute nel paragrafo 7 del provvedimento n. 548 del 21 dicembre 2017";

ESAMINATA la documentazione in atti;

VISTI gli atti d'ufficio e le osservazioni formulate dal segretario generale ai sensi dell'art. 15 del regolamento del Garante n. 1/2000;

RELATORE la dott.ssa Giovanna Bianchi Clerici;

PREMESSO

1. L'iter istruttorio relativo alla verifica dell'adempimento del provvedimento n. 548 del 21 dicembre 2017.

A conclusione dell'istruttoria relativa alla violazione dei sistemi informatici riferiti ai diversi siti web connessi al Movimento 5 Stelle (www.movimento5stelle.it, www.rousseau.movimento5stelle.it, www.beppegrillo.it) verificatasi nell'estate 2017, l'Autorità ha prescritto, nei confronti dei relativi titolari del trattamento, ai sensi dell'art. 154, comma 1, lett. a), b) e c) del Codice, l'adozione di misure necessarie e opportune al fine di rendere i trattamenti dei dati personali degli utenti dei predetti siti web conformi ai princìpi della disciplina in materia di protezione dei dati personali.

1.1. Le prescrizioni relative all'adozione delle misure necessarie, oltre a quelle concernenti i profili di sicurezza informatica (come delineati nel paragrafo 7 del provvedimento, lett. da A) a F)) impartite a tutti i titolari del trattamento dei predetti siti web (cfr. punto 1.2), riguardavano anche la riformulazione delle informative rese ai sensi dell'art. 13 del Codice, sia nel senso di una maggiore specificazione delle funzionalità dei diversi siti e delle relative tipologie di trattamenti, sia ai fini della corretta identificazione dei soggetti cui i dati venivano comunicati (salvo provvedere alla designazione degli stessi quali responsabili del trattamento ai sensi dell'art. 29 del Codice).

In ordine a tali specifici profili l'Autorità, dopo aver preso atto che, entro il termine stabilito nel dispositivo del provvedimento n. 548 (trenta giorni), i titolari del trattamento interessati (all'epoca, Associazione Rousseau e Giuseppe Piero Grillo) avevano adempiuto alle predette prescrizioni, ha avviato anche un procedimento sanzionatorio, peraltro già estinto con il pagamento delle relative sanzioni.

1.2 L'adempimento del complesso di prescrizioni di cui al punto 1) del dispositivo del citato provvedimento n. 548, relativo all'adozione delle misure necessarie riguardanti i profili di sicurezza informatica (sintetizzate al par. 7, lett. da A a F del provvedimento medesimo), ha dato luogo ad una serie di comunicazioni da parte dei titolari del trattamento attestanti il progressivo, dichiarato completamento delle prescrizioni stesse. Al riguardo l'Autorità, sulla base dei riscontri pervenuti, ha effettuato i necessari approfondimenti tecnici - anche, laddove tecnicamente possibile, mediante test operati sui siti web del Movimento e della piattaforma Rousseau - rilevando e, quindi, segnalando le criticità e le debolezze strutturali che emergevano dalla predetta analisi.

Nelle more dei predetti adempimenti la titolarità del trattamento dei dati personali riferiti ai siti del Movimento 5 Stelle è peraltro transitata dal Sig. Giuseppe Piero Grillo ad un nuovo soggetto giuridico, Associazione Movimento 5 Stelle, che ha provveduto a designare l'Associazione Rousseau quale responsabile del trattamento ex art. 29 del Codice in allora vigente.

Al contempo, il sito www.beppegrillo.it è stato oggetto di una completa ristrutturazione e trasferito su una nuova infrastruttura informatica che non consente più la creazione di account personali ovvero, come dichiarato, "non vi è alcuna possibilità per i navigatori del blog di iscriversi e lasciare i propri dati personali" (cfr. nota del 28 febbraio 2018). La gestione di tale sito è ora affidata alla società Beppegrillo s.r.l. avente sede in Genova, soggetto del tutto diverso rispetto a quello precedentemente individuato; ne consegue che il predetto sito si è collocato fuori dal campo di attenzione del presente provvedimento (cfr. par. 7, lett. F del provvedimento del 21 dicembre 2017), centrato sulle criticità dei trattamenti dei dati della c.d. "piattaforma Rousseau" (par. 7 lett. da A a E).

A seguito di un complesso e attento esame delle informazioni e della documentazione tecnica medio tempore pervenuta, il Garante, anche sulla base dell'esigenza rappresentata dal titolare del trattamento di poter disporre di un termine ulteriore per l'effettivo e completo adempimento delle prescrizioni di cui al par. 7, lett. E, del

provvedimento in ragione della complessità delle implementazioni tecnologiche (che necessitavano anche dell'ausilio di società esterne, Wind Tre S.p.a e ITnet s.r.l. in particolare), con i provvedimenti del 16 maggio 2018 e, infine, 4 ottobre 2018 ha prorogato al 15 ottobre 2018 il termine ultimo per il completamento delle operazioni, chiedendo, al contempo, ulteriori dettagli e precisazioni relativamente ad alcuni profili, ancora non sufficientemente chiari, attinenti all'adempimento delle prescrizioni di cui ai punti A, B e D.

Alla scadenza del predetto termine, data la complessità e delicatezza delle banche dati interessate, l'Autorità ha avviato una complessiva verifica degli adempimenti richiesti.

Già il 16 ottobre 2018, prendendo atto di quanto dichiarato da Associazione Rousseau (responsabile del trattamento) in ordine all'avvenuto completamento di tutti gli adempimenti previsti dal provvedimento in questione (ivi compresa la dichiarazione di Wind Tre S.p.a., a sua volta designata quale responsabile del trattamento, di aver portato a compimento le implementazioni tecniche relative alla sicurezza perimetrale), l'Ufficio del Garante ha informato i predetti responsabili che nei giorni 12 e 13 novembre 2018 sarebbe stato effettuato un accertamento ispettivo di natura prettamente tecnica avente lo scopo di verificare in concreto attraverso una serie di accessi ai sistemi informatici svolti in presenza di tutte le professionalità necessarie – la robustezza dei sistemi di sicurezza adottati rispetto alle criticità rappresentate dall'Autorità, ancora nei due provvedimenti di proroga sopracitati.

Al riguardo occorre precisare che Wind Tre S.p.a., per l'esecuzione del contratto di servizi stipulato con l'Associazione Rousseau che include anche servizi di gestione sistemistica - si avvale della società ITtnet s.r.l..; per tale ragione la società ITnet ha partecipato agli accertamenti tecnico-informatici effettuati presso il data center di Wind in località Siziano (PV).

1.3 Oltre alla prescrizione di misure e accorgimenti necessari, il provvedimento n. 548 ha anche evidenziato una serie di misure e di accorgimenti opportuni volti a minimizzare, in particolare, i rischi per i diritti e le libertà degli utenti del sistema di e-voting (cfr. par. 8.2 del provvedimento e punto 2) del relativo dispositivo). In particolare era stata suggerita la cancellazione o la trasformazione in forma anonima dei dati personali trattati, una volta terminate le operazioni di voto, nonché il disaccoppiamento del numero telefonico del votante (dato personale particolarmente identificativo) dal voto espresso, allo scopo di rendere i dati relativi alle votazioni meno direttamente riconducibili ai votanti o, addirittura, del tutto anonimi. In

proposito, all'esito dell'iter istruttorio relativo alla verifica dell'adempimento, sono state evidenziate persistenti criticità di cui si darà conto nei paragrafi 2.2 e 3.4.

2. Le risultanze dell'accertamento ispettivo.

A seguito dell'accertamento ispettivo sopra indicato - tenutosi presso la sede dell'Associazione Rousseau e presso il data center di Siziano della società Wind Tre S.p.a. – cui è affidata la gestione del sistema informativo relativo ai siti web "rousseau.movimento5stelle.it" e www.movimento5stelle.it" – l'Autorità, sulla scorta della copiosa documentazione acquisita, ha analizzato lo stato di adempimento delle prescrizioni impartite, con specifico riferimento agli aspetti tecnologici e di sicurezza informatica (par. 7 del provvedimento), esaminando le diverse misure adottate in relazione a ciascuna prescrizione, tenuto conto degli elementi informativi forniti dal titolare e dai responsabili del trattamento e delle ulteriori informazioni acquisite sia nel corso che a seguito dell'attività ispettiva.

Si riporta di seguito, per comodità di lettura, una descrizione sintetica delle prescrizioni di misure necessarie di cui al par. 7, lett. da A a E del provvedimento e del relativo stato di attuazione:

A. conduzione di un'attività di vulnerability assessment con lo scopo di individuare e correggere eventuali vulnerabilità nei servizi prima di renderli fruibili al pubblico, da rinnovare periodicamente e in occasione di evoluzioni o modifiche, al fine di contribuire ad assicurare un livello costantemente adeguato di protezione dei dati personali. Al riguardo, il 12 novembre 2018, l'Associazione Rousseau ha dichiarato che "tutte le vulnerabilità classificate Critiche, Alte e Medie sono state risolte" e dalle verifiche effettuate è stato effettivamente constatato come le componenti software affette da tali vulnerabilità siano state rimosse dal sistema (cfr. verbale ispezione presso l'Associazione del 12 novembre 2018, p. 4); residuano alcune perplessità più generali, legate essenzialmente all'obsolescenza dei sistemi in uso, per le quali si rinvia al par. 3.1.

B. si tratta di una prescrizione volta a rimediare alle debolezze individuate nella procedura di creazione degli account individuali (da parte degli utenti) e nella successiva fase di autenticazione informatica, da un lato migliorando la qualità delle password, dall'altro suggerendo misure idonee a mitigare l'impatto di eventuali attacchi brute force (volti a individuare la componente riservata delle credenziali tramite la enumerazione di tutte le possibili stringhe alfanumeriche che possono costituire una password); sul punto, tenuto conto che i siti web in questione sono stati

dotati di un sistema di reCaptcha, di un indicatore di qualità della password in fase di scelta da parte degli utenti e di un controllo sulla lunghezza della password, l'adeguamento deve ritenersi compiuto;

C. si tratta di una prescrizione relativa all'adozione di protocolli di rete sicuri e di certificati digitali, con lo scopo, da una parte, di proteggere i dati nel loro transito in rete, dall'altra, di scongiurare il rischio di inganno degli utenti derivante dalla possibile contraffazione dei siti web del Movimento (ossia l'attrazione degli utenti visitatori, tramite artifizi e raggiri, verso siti contraffatti – fake sites - riproducenti le sembianze del sito originario); tali misure risultano essere state adottate già nei primi riscontri pervenuti all'Autorità (prima delle due proroghe poi concesse);

D. la quarta prescrizione intendeva porre rimedio alla debolezza del metodo di conservazione delle password di accesso ai servizi on-line del Movimento 5 Stelle, dovuta all'utilizzo di algoritmi crittografici deboli e all'obsolescenza tecnologica della piattaforma di Content Management System (Cms) su cui sono stati sviluppati i siti stessi; sul punto, a seguito degli accertamenti tecnico-informatici effettuati anche in modo incrociato presso la sede dell'Associazione Rousseau, tramite accesso al database mysql, e presso il data center di Wind, è stato constatato che, alla data del 12 novembre 2018, "per la maggior parte degli utenti, circa il 77%, le password risultano memorizzate attraverso l'utilizzo di algoritmi crittografici robusti" (cfr. verbale ispezione 12 novembre 2018 presso Wind, p. 4);

E. la prescrizione concerneva le misure di auditing, che obbligano alla tenuta delle registrazioni degli accessi e delle operazioni compiute (log) sul database del sistema Rousseau, anche come misura di attuazione del provvedimento generale del Garante del 27 novembre 2008 in tema di amministratori di sistema. Ciò come necessario presupposto a garanzia dell'integrità dei dati e con lo scopo di permettere almeno il controllo ex post delle attività svolte dagli incaricati.

2.1 Più specificamente, in relazione a tale ultima prescrizione (par. 7, lett. E) che, per la sua complessità, ha richiesto - come già evidenziato - la proroga del termine di adempimento del provvedimento fino al 15 ottobre 2018, sono state effettuate in loco una serie di verifiche tecniche al fine di accertare l'avvenuta adozione di misure che consentano un completo auditing informatico mediante la tenuta delle registrazioni degli accessi e delle operazioni compiute (log). In particolare:

a) Log applicativi

In relazione alla tenuta di log di tipo applicativo, nel corso degli accessi alla piattaforma del Movimento 5 Stelle, di cui sono stati salvati alcuni file e realizzati alcuni screenshot, si rappresenta che è stato tentato "un accesso applicativo di tipo amministrativo all'applicazione dell'Associazione Rousseau inserendo, al fine di generare un'apposita riga di log, credenziali non corrette e successivamente utilizzando con successo" credenziali valide (v. verbale ispezione presso l'Associazione del 12 novembre 2018, p. 4). L'Associazione ha in seguito fornito copia dei log di tracciamento relativi agli accessi e alle operazioni compiute durante l'attività ispettiva.

b) Log del database

Nel corso dell'attività ispettiva presso Wind, ITnet s.r.l. ha "rappresentato che l'accesso al database può avvenire attraverso due modalità". La prima, sostanzialmente riservata agli amministratori di sistema di ITnet, avviene attraverso l'utilizzo della piattaforma XX, che permette l'accesso previo inserimento di credenziali di autenticazione nominali, assegnate agli amministratori di sistema medesimi. Tali accessi e le relative operazioni compiute, sia a livello di sistema operativo che di database, sono oggetto di registrazione da parte della citata piattaforma. La seconda modalità, che consiste invece nell'accesso all'interfaccia web di gestione del DBMS (c.d. interfaccia XX) e che è utilizzata esclusivamente dal personale tecnico dell'Associazione Rousseau, "non prevede alcuna registrazione degli accessi e delle operazioni compiute e avviene attraverso l'utilizzo di credenziali di autenticazione non nominative (utenze applicative). In particolare, dalle registrazioni risulta esclusivamente che l'utente ha visualizzato la pagina di login all'interfaccia XX". La società ITnet ha peraltro precisato che "il sistema attuale non permette la registrazione degli accessi e delle operazioni compiute sul database a causa delle limitazioni presenti nella edizione (community edition) del pacchetto mysql installato" (cfr. verbale ispezione presso Wind del 12 novembre 2018, pp. 3-4).

L'Associazione ha inoltre rappresentato che i log di cui dispone includono "tutti i log di accesso (ovvero di azione di visita delle pagine) alle piattaforme web (XX), tra cui quelle di XX. È quindi tracciato ogni accesso alle pagine web erogate e visitate e anche alle pagine web di questo tool attraverso cui è poi possibile raggiungere il database", precisando di "aver pianificato la rimozione del tool XX in favore di strumenti che sfruttino la connettività SSH per un migliore tracciamento delle operazioni sul database" (v. nota dell'Associazione del 19 novembre 2018, p. 4).

c) Piattaforma di raccolta e correlazione dei log

L'Associazione ha dichiarato che "il contratto con Wind Tre S.p.A. prevede la fornitura di alcuni servizi di sicurezza perimetrale (…) per la raccolta e la correlazione dei log generati dai dispositivi di sicurezza (…) e che è presente un secondo sistema (…) gestito da ITnet S.r.l., che fa da collector e correlatore dei log per i sistemi relativi al perimetro interno (…). [OMISSIS]. L'Associazione ha fornito copia di due report generati dalla piattaforma (…) e relativi rispettivamente alle minacce e alle connessioni VPN instaurate.

d) Protezione e conservazione dei log

L'Associazione ha dichiarato che "la protezione dei log da accessi non autorizzati, da alterazione e da distruzione accidentale o deliberata è stata demandata a Wind Tre S.p.A. che a sua volta si avvale di ITnet s.r.l. per questo aspetto specifico". Wind ha peraltro rappresentato che "i file di log vengono conservati per un periodo minimo di sei mesi fino ad un massimo di un anno" (v. verbale ispezione presso Wind del 12 novembre 2018, pp. 3-4).

e) Amministratori di sistema

A seguito dell'attività ispettiva, con nota del 23 novembre 2018, l'Associazione ha fornito un "elenco degli amministratori delle piattaforme applicative in uso presso l'Associazione, con l'elenco delle funzioni ad essi attribuite". Tale elenco ha messo in evidenza l'esistenza di credenziali di autenticazione, con privilegi amministrativi, condivise da più soggetti con la qualifica di amministratore di sistema.

In particolare, nel documento del 23 novembre 2018, a scioglimento delle riserve formulate nel corso dell'attività ispettiva del 12 e 13 novembre, si è rilevato che per il sito www.movimento5stelle.it sono previste due distinte utenze con privilegi di amministrazione, ciascuna condivisa tra più persone (tre nel primo caso e due nel secondo caso), mentre per il sito "rousseau.movimento5stelle.it" è prevista una singola utenza amministrativa (incidentalmente coincidente con una delle due utenze citate in relazione al sito www.movimento5stelle.it) che risulta condivisa tra cinque persone (alcune delle quali operano anche sul sito www.movimento5stelle.it).

Le funzionalità accessibili tramite tali accessi appaiono ampie, in particolare per il sito rousseau.movimento5stelle.it rispetto a cui l'utenza segnalata risulta "utilizzata per gestire tutte le funzioni della piattaforma Rousseau", mentre per il sito www.movimento5stelle.it le funzionalità accessibili appaiono limitate a quanto necessario a "gestire gli iscritti e dare seguito alle loro richieste".

2.2 Con riferimento alla misura opportuna di cui al par. 8.2 del provvedimento (v. sopra par. 1.3), nel corso dell'attività ispettiva sono state effettuate alcune verifiche tecniche per accertare le modalità di cancellazione o di trasformazione in forma anonima dei dati personali trattati, una volta terminate le operazioni di voto. In particolare, presso la sede Wind di Siziano è stato constatato che la tabella di database contenente le informazioni relative alle operazioni di e-voting effettuate nelle settimane e mesi precedenti l'accertamento ispettivo (ultimi dati relativi alla votazione online del 12 settembre 2018) "non contiene [più] il numero di cellulare del soggetto votante" e che la medesima tabella "contiene un ID utente [che] permette indirettamente di risalire [al] soggetto votante" (v. verbale ispezione presso Wind del 12 novembre 2018, p. 4).

Inoltre, l'Associazione ha dichiarato che "è stato previsto un processo che cancella dal database i dati relativi all'espressione della volontà del votante, immediatamente dopo la certificazione dell'esito della votazione da parte di un notaio". Al riguardo è stato constatato che "la colonna relativa all'espressione del voto è valorizzata a "NULL", da cui si evince che, effettivamente, sono stati cancellati tutti i dati relativi all'espressione del voto" (v. verbale ispezione presso l'Associazione del 12 novembre 2018, pp. 3-4).

Tuttavia, nel corso dell'attività ispettiva presso Wind è stata rilevata l'esistenza di un'ulteriore tabella di database contenente informazioni relative a operazioni di voto (ultimi dati relativi alla votazione online del 22 settembre 2017) ed è stato constatato che "la stessa contiene il numero di cellulare e l'ID utente del soggetto votante" oltre che i dati relativi all'espressione di voto (v. verbale ispezione presso Wind del 12 novembre 2018, p. 4). Al riguardo, l'Associazione ha dato successivamente prova di "aver immediatamente avviato e ultimato le operazioni per procedere alla cancellazione dei dati presenti nella tabella" (v. verbaleispezione presso l'Associazione del 13 novembre 2018, p. 3).

3. Le considerazioni dell'Autorità

Sulla base dell'esame delle informazioni acquisite in sede ispettiva e dell'analisi tecnica condotta anche sulla documentazione integrativa successivamente pervenuta (23 novembre 2018 e 10 dicembre 2018), l'Autorità, pur ritenendo che nel complesso sia stato realizzato un sostanziale innalzamento dei livelli di sicurezza dei trattamenti effettuati nell'ambito dei siti web oggetto del provvedimento del 21 dicembre 2017, deve tuttavia formulare le seguenti considerazioni relativamente alle prescrizioni di cui al par. 7, lett. A, D, E e par. 8.2 del provvedimento medesimo.

3.1 Attività di vulnerability assessment (par. 7, punto A del provvedimento)

Alla luce di quanto descritto nel paragrafo 2, si deve ritenere che il titolare del trattamento abbia dato attuazione alle prescrizioni del provvedimento, svolgendo dei vulnerability assessment relativi alle funzioni di nuovo sviluppo e risolvendo alcune criticità della piattaforma software.

Tuttavia, seppur in un contesto di incremento dei livelli di sicurezza, persistono criticità derivanti dall'obsolescenza di alcune componenti software dei siti web del Movimento; si fa riferimento, in particolare, alla piattaforma Cms che è ancora Movable Type 4 mentre la versione corrente è Movable Type 7 (release 7.1.1. del 29 gennaio 2019). Ciò rende particolarmente gravoso il compito di mantenere aggiornato e sicuro il Cms a supporto dei siti web del Movimento, poiché lo stesso produttore ha cessato la distribuzione di aggiornamenti e di patch di sicurezza al raggiungimento della End of Life del prodotto, verificatasi il 31 dicembre 2013.

Tale circostanza rende estremamente difficoltoso il patching dei sistemi online realizzati sulla piattaforma Cms, l'adozione di accorgimenti ad hoc e l'intervento, realisticamente non tempestivo, di sviluppatori in grado di apportare le correzioni necessarie a fronte di future vulnerabilità la cui scoperta non può essere esclusa, come per ogni sistema software complesso, ma che in questo caso potrebbe avere un impatto particolarmente gravoso stante l'assenza di supporto ufficiale da parte del produttore.

3.2 Database delle utenze della piattaforma Rousseau (par. 7, punto D)

Alla luce di quanto descritto nel paragrafo 2, benché l'Autorità non disponga di elementi per verificare che la conservazione delle password degli utenti della piattaforma Rousseau sia stata resa effettivamente più robusta in termini crittografici, alcuni accorgimenti tecnici adottati dal titolare del trattamento e documentati (quali l'introduzione di salt individuali che consentono di rendere più complesso l'hash generato rispetto a quanto fosse in precedenza) fanno ritenere che la prescrizione possa ritenersi sostanzialmente adempiuta.

3.3 Misure di auditing informatico (par. 7, punto E)

Da quanto sopra descritto (par. 2.1), risulta che gli accessi da terminale remoto sono oggetto di registrazione che permette a posteriori la verifica puntuale delle attività compiute (login, logout, comandi impartiti), mentre per quanto riguarda l'interfaccia

XX, questa non consente di tracciare adeguatamente gli accessi al database né, tantomeno, di tracciare le operazioni compiute sul database in lettura o in modifica.

Per questo motivo, mentre la misura prescritta con il punto E del provvedimento può considerarsi soddisfatta nei casi di accesso tramite emulatore di terminale con protocollo ssh, la stessa risulta disattesa laddove gli accessi siano effettuati avvalendosi dell'interfaccia XX, riservata al solo personale dell'Associazione Rousseau con qualifica di amministratore di sistema (un numero estremamente esiguo di persone) previo utilizzo di una connessione Vpn (Virtual Private Network).

Risulta quindi che un ristretto novero di addetti con particolari capacità d'azione tecnica, nell'ambito dei sistemi informativi del Movimento 5 Stelle e dell'Associazione Rousseau, abbia la possibilità di accedere a delicate funzionalità delle piattaforme software con cui vengono erogati i servizi senza che il loro operato possa essere soggetto a verifiche, a iniziare da quelle che lo stesso titolare del trattamento sarebbe tenuto a compiere nei confronti delle figure più critiche rispetto alla sicurezza informatica dei trattamenti. L'assenza di capacità di auditing o, meglio, la presenza di modalità di accesso e interazione con i sistemi che, non comportando la generazione di auditable events funzionali all'auditing informatico, eludono le verifiche successive, costituisce una grave carenza che espone un sistema così delicato a potenziali rischi di violazione dei dati personali (cfr. par. 2.1, lett. b)).

3.4 Riservatezza delle operazioni di voto elettronico (par. 8.2 del provvedimento)

Sulla base delle evidenze descritte al par. 2.2, non può ritenersi che la mera rimozione del numero telefonico, a fronte della presenza di un altro identificativo univoco dell'iscritto, possa essere considerata quale misura coerente con gli obiettivi di protezione dei dati personali che si intendevano promuovere.

Tale circostanza, unitamente a quanto rilevato in materia di auditing informatico (cfr. par. 2.1 e 3.3) evidenzia che le misure adottate, consistenti in procedure organizzative o comunque non basate su automatismi informatici, lasciando esposti i risultati delle votazioni (per un'ampia finestra temporale che si estende dall'istante di apertura delle urne fino alla successiva c.d. "certificazione" dei risultati, che può avvenire a distanza di diversi giorni dalla chiusura delle operazioni di voto) ad accessi ed elaborazioni di vario tipo (che vanno dalla mera consultazione a possibili alterazioni o soppressioni, all'estrazione di copie anche offline), non garantiscano l'adeguata protezione dei dati personali relativi alle votazioni online.

A ciò si aggiunge che la rilevata assenza di adeguate procedure di auditing informatico, escludendo la possibilità di verifica ex post delle attività compiute, non consente di garantire l'integrità, l'autenticità e la segretezza delle espressioni di voto, caratteristiche fondamentali di una piattaforma di e-voting (almeno sulla base degli standard internazionali comunemente accettati). Infatti, gli addetti tecnici alla gestione della piattaforma e, in particolare, coloro che svolgono la funzione di Dba (Data Base Administrator), pur individuati tra persone di elevata affidabilità, sono comunque tecnicamente in grado di accedere alle delicate funzionalità del Dbms in cui vengono registrati i dati relativi alle espressioni di voto mantenendo una capacità d'azione totale sui dati e sfuggendo alle procedure di auditing.
La regolarità delle operazioni di voto è quindi affidata alla correttezza personale e deontologica degli incaricati di queste delicate funzioni tecniche, cui viene concessa una elevata fiducia in assenza di misure di contenimento delle azioni eseguibili e di suddivisione degli ambiti di operatività, cui si aggiunge la pratica certezza che le attività compiute, al di fuori del ristretto perimetro soggetto a tracciamento, non potranno essere oggetto di successiva verifica da parte di terzi (cfr. par. 2.1 lett. b) e 3.3.).

In questo senso, la piattaforma Rousseau non gode delle proprietà richieste a un sistema di evoting, come descritte, per esempio, nel documento "E-voting handbook - Key steps in the implementation of e-enabled elections" pubblicato dal Consiglio d'Europa a novembre 2010 e nel documento "Recommendation CM/Rec(2017)5 of the Committee of Ministers to member States on standards for e-voting" adottato dal Comitato dei Ministri del Consiglio d'Europa il 14 luglio 2017, che prevedono la protezione delle schede elettroniche e l'anonimato dei votanti in tutte le fasi del procedimento elettorale elettronico.

La stessa, infatti, non appare in grado, tra l'altro, né di prevenire gli eventuali abusi commessi da addetti interni, non essendo stati in essa previsti accorgimenti per partizionare il loro dominio d'azione (in particolare, degli amministratori di sistema e dei DBA – data base administrators), né di consentire l'accertamento a posteriori dei comportamenti da questi tenuti, stante la limitata efficacia degli strumenti di tracciamento delle attività.

In questo senso sussistono forti perplessità sul significato da attribuire al termine "certificazione" (cfr. par. 2.2) riferito dal titolare del trattamento all'intervento di un notaio o di altro soggetto terzo di fiducia in una fase successiva alle operazioni di voto, con lo scopo di asseverarne gli esiti. Non c'è dubbio, infatti, che qualunque intervento ex post di soggetti di pur comprovata fiducia (notai, certificatori accreditati) poco possa

aggiungere, dal punto di vista della genuinità dei risultati, in un contesto in cui le caratteristiche dello strumento informatico utilizzato, non consentendo di garantire tecnicamente la correttezza delle procedure di voto, non possono che produrre una rappresentazione degli esiti non suscettibile di analisi, nell'impossibilità di svolgere alcuna significativa verifica su dati che sono, per loro natura e modalità di trattamento, tecnicamente alterabili in pressoché ogni fase del procedimento di votazione e scrutinio antecedente la c.d. "certificazione".

3.5 Ulteriori considerazioni: la condivisione delle credenziali di autenticazione

Come anzi descritto (v. par. 2.1 lett. e)), nella documentazione pervenuta a seguito dell'attività ispettiva è stata rilevata la condivisione di credenziali di autenticazione assegnate a incaricati dotati di elevati privilegi per la gestione delle piattaforme applicative a supporto dei siti "www.movimento5stelle.it" e "rousseau.movimento5stelle.it".

Le modalità di assegnazione delle credenziali e dei privilegi relativi alle varie funzionalità dei siti dell'Associazione, tenendo conto del contesto e delle specificità del trattamento che tramite essi viene svolto - caratterizzato dalla raccolta ed elaborazione di particolari categorie di dati su larga scala - risultano inadeguate sotto il profilo della sicurezza poiché la condivisione delle credenziali impedisce di attribuire le azioni compiute in un sistema informatico a un determinato incaricato, con pregiudizio anche per il titolare, privato della possibilità di controllare l'operato di figure tecniche così rilevanti.

In più, si osserva che, allorquando le medesime credenziali permettano l'accesso a più sistemi informatici e vengano condivise tra più incaricati, possono determinarsi situazioni in cui non c'è coerenza tra i profili di autorizzazione attribuiti e le effettive esigenze di operatività per la gestione dei sistemi, rendendo possibile a un soggetto autorizzato soltanto all'uso di una determinata piattaforma di operare, grazie alla condivisione delle credenziali e in assenza di una specifica volontà del titolare o del responsabile, anche su altre piattaforme che sfruttino il medesimo sistema di autenticazione.

In proposito, si evidenzia come l'utilizzo di "credenziali di autenticazione in uso esclusivo dei soggetti che operano sotto la sua autorità o quella del responsabile del trattamento" e la "definizione e configurazione di differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari per effettuare le diverse operazioni di trattamento" nel regime normativo previgente fossero addirittura previste quali misure

minime di sicurezza alla cui adozione erano tenuti tutti i titolari di trattamento (ai sensi del disciplinare tecnico di cui all'allegato B al Codice).

4. Valutazioni conclusive dell'Autorità.

Le considerazioni svolte nei paragrafi precedenti consentono di formulare le seguenti osservazioni conclusive in ordine allo stato di adempimento complessivo del provvedimento del 21 dicembre 2017.

In particolare, pur avendo constatato come le attività poste in essere abbiano migliorato in modo significativo gli aspetti di sicurezza della piattaforma Rousseau, residuano tuttavia alcune importanti vulnerabilità rispetto alle quali l'Autorità (valutata anche l'urgenza di intervenire su una struttura, come la piattaforma Rousseau, di particolare rilevanza e delicatezza anche sotto il profilo della partecipazione democratica dei cittadini alle scelte politiche) è tenuta ad intervenire attraverso i poteri che le sono attribuiti dal nuovo Regolamento (UE) 2016/679, pienamente applicabile dal 25 maggio 2018.

4.1 Al riguardo, ai sensi dell'art. 58, comma 2, lett. d) del Regolamento, il Garante ingiunge all'Associazione Movimento 5 Stelle e all'Associazione Rousseau quale responsabile del trattamento, di provvedere :

1. a completare l'adozione delle misure necessarie di auditing informatico previste al par. 7, lett. E, del provvedimento n. 548, prevedendo che anche gli accessi al database effettuati tramite interfaccia XX siano oggetto di completa registrazione in modo da consentire la verifica a posteriori delle attività compiute (cfr. punti 2.1 e 3.3), entro il termine di 60 giorni dalla ricezione del presente provvedimento; l'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento;

2. a rimuovere la criticità emersa a seguito dell'accertamento ispettivo del novembre 2018, come evidenziata ai punti 2.1 lett. e) e 3.5 - ovvero provvedere ad assegnare credenziali di autenticazione ad uso esclusivo di ciascun utente con privilegi amministrativi definendo per ciascuno i differenti profili di autorizzazione, entro il termine di 10 giorni dalla ricezione del presente provvedimento; l'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento;

3. entro il termine di 120 giorni dalla ricezione del presente provvedimento, ai fini del rispetto del principio di responsabilizzazione di cui all'articolo 24 del Regolamento, ad una rivisitazione complessiva delle iniziative di sicurezza adottate (cfr. par. 3.1 sulle "Attività di vulnerability assessment"), alcune delle quali, per quanto conformi, in termini di stretto adempimento, alle prescrizioni di cui al par. 7, lett. A del provvedimento n. 548 del 2017, risultano comunque inficiate nella loro efficacia dalle gravi limitazioni tecniche intrinseche al sistema utilizzato (CMS - Movable Type 4). L'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento;

4. all'effettuazione, entro il termine di 60 giorni dalla ricezione del presente provvedimento, di una valutazione d'impatto sulla protezione dei dati, specificamente riferita alle funzionalità di e-voting attribuite alla piattaforma. Solo in base ad una rigorosa progettazione e a una attenta valutazione dei rischi è, infatti, possibile realizzare un sistema di e-voting in grado di fornire garanzie di resilienza nonché di assicurare l' autenticità e la riservatezza delle espressioni di voto. Le conclusioni della valutazione d'impatto dovranno pervenire a questa Autorità entro 70 giorni dalla ricezione del presente provvedimento.
L'eventuale inosservanza del presente ordine è soggetta alla sanzione amministrativa prevista dall'art. 83, par. 5, lett. e) del Regolamento.

Tali termini sono commisurati tenendo conto dell'urgenza di assicurare l'integrità, resilienza e sicurezza di una piattaforma, quale quella in esame, utilizzata per l'esercizio dei diritti politici dei cittadini.

4.2 Ciò posto, si evidenzia che le predette criticità, come constatate e accertate dall'ufficio del Garante, costituiscono una violazione dell'art. 32 del Regolamento (UE) 2016/679 che individua alcuni parametri di sicurezza che il titolare e il responsabile del trattamento sono tenuti ad adottare al fine di garantire un livello di sicurezza adeguato in rapporto al rischio per i diritti e le libertà delle persone.

In particolare:

1) il mancato, completo tracciamento degli accessi al database del sistema Rousseau e delle operazioni sullo stesso compiute (di cui alla specifica misura necessaria, tecnica e organizzativa, prescritta dall'Autorità con il provvedimento del 21 dicembre 2017 e oggetto di due proroghe) configura la violazione di quel generale dovere di controllo sulla liceità dei trattamenti che grava sul titolare del trattamento e, in particolare, dell'obbligo di assicurare più adeguate garanzie di riservatezza agli iscritti alla

piattaforma medesima; ciò sia in ragione delle dimensioni delle banche dati in questione, sia della tipologia di dati raccolti nonché delle funzionalità che le caratterizzano (tra cui, in particolare, il sistema di e-voting che deve essere necessariamente assistito da idonei accorgimenti a tutela dei dati personali dei votanti). Ciò a maggior ragione tenendo conto che tali banche dati sono particolarmente esposte al rischio di attività di hakeraggio o comunque ad attacchi informatici, quali quelli verificatisi più volte, anche successivamente al data breach di agosto 2017;

2) l'accertata condivisione delle credenziali di autenticazione da parte di più incaricati dotati di elevati privilegi per la gestione della piattaforma Rousseau e la mancata definizione e configurazione dei differenti profili di autorizzazione in modo da limitare l'accesso ai soli dati necessari nei diversi ambiti di operatività, nel previgente ordinamento erano addirittura qualificate come misure minime di sicurezza (cfr. regole nn. 2, 3 e 13 del disciplinare tecnico di cui all'allegato B del Codice) che i titolari del trattamento erano tenuti ad adottare al fine di assicurare un livello minimo di protezione dei dati personali. E' pertanto evidente come la mancata adozione di tali misure e, per converso, l'avvenuta condivisione delle credenziali di autenticazione tra più soggetti legittimati alla gestione della piattaforma rappresentino una violazione dell'obbligo di predisposizione, da parte del responsabile del trattamento, di misure tecniche e organizzative adeguate.

4.3 La violazione dell'art. 32 del Regolamento (UE) 2016/679, richiamata al paragrafo 4.2 è sanzionata ai sensi dell'art. 83, par. 4, lett. a) del Regolamento.

Pertanto, accertata la responsabilità, per la predetta violazione, dell'Associazione Rousseau quale responsabile del trattamento, in considerazione di quanto disposto dall'articolo 166, comma 5, del Codice, si ingiunge alla suddetta associazione, quale trasgressore, ai sensi dell'art. 58, paragrafo 2, lettera i) del Regolamento, il pagamento di euro 50.000, quale sanzione ritenuta adeguata ai sensi dell'art. 83, paragrafo 1, lettere a), c), d), f) e g) del medesimo Regolamento.

Deve, infatti, rilevarsi come, per un verso, il trattamento in questione concerna anche dati particolari di cui all'art. 9 del Regolamento (parametro rilevante ai sensi dell'art. 83, paragrafo 1, lettera g), la violazione si sia protratta per un tempo significativo, interessando un rilevante numero di soggetti, evidenziando altresì il ricorso a misure tecniche e organizzative carenti, nonché a dispositivi e sistemi obsoleti (criteri valevole ai fini dell'art. 83, paragrafo 2, lettera a) e, rispettivamente, lettera d del Regolamento).

Per altro verso, tuttavia, deve prendersi atto del percorso di progressivo adeguamento e miglioramento delle misure di sicurezza adottate al fine di rafforzare la resilienza della piattaforma: elemento rilevante ai fini di cui al citato art. 83, paragrafo 2, lettere c) ed f) .

Va infine considerata la natura, di associazione finalizzata all'esercizio di diritti politici dei cittadini, del trasgressore nonché il disposto di cui all'art. 22, comma 13, del decreto legislativo 10 agosto 2018, n. 101, in ordine all'irrogazione delle misure sanzionatorie nei primi otto mesi dell'applicazione della nuova disciplina.

TUTTO CIO' PREMESSO IL GARANTE:

accertato il non ancora completo adempimento del provvedimento del 21 dicembre 2017 e verificate le carenze relative ai profili di sicurezza di cui in motivazione:

1. ingiunge, ai sensi dell'art. 58, comma 2, lett. d) del Regolamento, all'Associazione Movimento 5 Stelle e all'Associazione Rousseau quale responsabile del trattamento, di provvedere nei modi e nei termini di cui al par. 4.1, punti 1, 2, 3 e 4 ;

2. ai sensi dell'art. 58, paragrafo 2, lettera i) del Regolamento, ingiunge all'Associazione Rousseau, quale responsabile del trattamento e in tale qualità trasgressore, il pagamento, entro 180 giorni dalla data di ricezione del presente provvedimento, di euro 50.000 a titolo di sanzione per la violazione di cui al combinato disposto degli artt. 32 e 83, paragrafo 4, lettera a) del Regolamento.

Ai sensi dell'art. 78 del Regolamento(UE) 2016/679, nonché dell'art. 152, comma 1-bis del Codice, fermo quanto disposto dall'art. 166, comma 8, del medesimo Codice, 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, 4 aprile 2019

IL PRESIDENTE
Soro

IL RELATORE
Bianchi Clerici

IL SEGRETARIO GENERALE
Busia