GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

[doc. web n. 7400401]

Provvedimento su data breach - 21 dicembre 2017

Registro dei provvedimenti
n. 548 del 21 dicembre 2017

IL GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Nella riunione odierna, in presenza del dott. Antonello Soro, presidente, della dott.ssa Augusta Iannini, vice presidente, della dott.ssa Giovanna Bianchi Clerici e della prof.ssa Licia Califano, componenti, e del dott. Giuseppe Busia, segretario generale;

VISTO il d.lg. 30 giugno 2003, n. 196 ("Codice in materia di protezione dei dati personali", di seguito "Codice");

VISTI gli articoli di stampa che nei primi giorni del mese di agosto 2017 riportavano la notizia di una intrusione informatica ai danni della "Piattaforma Rousseau" e del blog www.beppegrillo.it, con conseguente violazione dei dati personali di numerosi cittadini;

VISTE le segnalazioni pervenute con le quali alcune persone hanno rappresentato le proprie preoccupazioni in ordine al "data breach" subìto dalla piattaforma Rousseau e, più in generale, in ordine alla sicurezza dei principali siti web riferibili al "Movimento 5 stelle";

VISTI gli approfondimenti effettuati dall'Autorità sulla vicenda, attraverso richieste di informazioni e un accertamento ispettivo in loco presso il soggetto risultato responsabile del trattamento;

ESAMINATA la documentazione in atti;

VISTE 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. La violazione dei sistemi informatici.

1.1 Nel primi giorni del mese di agosto 2017 si è avuta notizia di un attacco informatico ai danni della piattaforma tecnologica su cui si basa il c.d. "Sistema operativo 5 stelle", il cui esito è stato reso noto da un soggetto non identificato che ha annunciato tale violazione mediante una serie di messaggi diffusi sulla rete Twitter utilizzando lo pseudonimo "rogue0"; con tale identificativo dell'utenza sono apparsi sulla piattaforma social citata, a partire dal 3 agosto 2017, dati personali di iscritti o simpatizzanti del Movimento 5 Stelle, asseritamente estratti dal database anagrafico della "piattaforma Rousseau".

La notizia ha avuto un immediato risalto mediatico – alimentato anche dall'imminenza della votazione on-line per la scelta del "candidato premier del Movimento 5 Stelle" – e hanno fatto seguito ulteriori segnalazioni, con cui alcuni cittadini lamentavano le vulnerabilità della predetta piattaforma informatica.

Successivamente, proprio in concomitanza con le predette primarie, sono pervenute all'Ufficio ulteriori segnalazioni da parte di soggetti che erano già intervenuti in rete sull'argomento, con le quali veniva evidenziata la debolezza delle misure di sicurezza nel frattempo predisposte dai gestori dei sistemi interessati per sanare i problemi sino a quel momento evidenziati. Si fa riferimento, in particolare, allo stesso utente "rogue0" che, trascorsi diversi giorni dalla prima pubblicazione, sosteneva di aver inserito dei post sul sito www.movimento5stelle.it impersonando altri utenti iscritti che ne apparivano, quindi, autori, e di aver effettuato, parimenti, il login sul sito www.beppegrillo.it utilizzando le credenziali di altri utenti su di esso registrati (tra i quali, anche alcuni deceduti).

I siti web riconducibili al Movimento 5 Stelle che risultano interessati dalla violazione dagli attacchi informatici sono:

1. https://www.movimento5stelle.it

2. https://rousseau.movimento5stelle.it

3. www.beppegrillo.it

Il sito www.ilblogdellestelle, seppure riconducibile al Movimento, non risulta essere stato oggetto di intrusioni.

Da una prima verifica effettuata dall'Autorità in ordine alle procedure di autenticazione informatica on-line (login), è emerso che, nel caso dei siti di cui ai nn. 1 e 2, la procedura di registrazione e di creazione dell'utenza è comune (il sito 3 e il "blog delle stelle", invece, attualmente non risultano consentire alcuna registrazione). Infatti, la funzione "iscrizione" del sito rousseau.movimento5stelle.it rimanda al form di iscrizione del sito www.movimento5stelle.it. Su quest'ultimo sito la registrazione può essere di tipo "base" o "verificata". La registrazione base consente l'accesso al sito del Movimento, ma non permette di utilizzare le funzioni del "Sistema operativo 5 Stelle" per le quali è necessario che i dati di registrazione siano verificati. La registrazione "verificata" prevede la verifica dell'identità dell'utenza tramite l'inserimento di un numero di cellulare (utilizzato per l'invio di un SMS per la comunicazione di una One Time Password – OTP) e il caricamento di una copia elettronica di un documento di identità.

La verifica dell'utenza non è immediata ed è svolta tramite intervento di un operatore che provvede ad analizzare la documentazione prima di procedere alla certificazione dell'identità associata all'utenza.

L'elemento di maggiore criticità di tale procedura è risultata la potenziale debolezza della password scelta in fase di registrazione (è infatti risultato possibile scegliere password di lunghezza inferiore agli otto caratteri).

1.2 In risposta ad alcune richieste di informazioni formulate da questa Autorità - a partire dal 10 agosto 2017 - nei confronti della Casaleggio & Associati s.r.l. (soggetto cui inizialmente sembravano riferibili i trattamenti in questione), il dott. Davide Federico Casaleggio, legale rappresentante della predetta società e che tuttavia, nella vicenda in esame, ha precisato di rispondere in qualità di legale rappresentante dell'Associazione Rousseau, con le note del 28 agosto e 21 settembre 2017, nel confermare che il sistema Rousseau e il blog www.beppegrillo.it avevano subìto una intrusione nei rispettivi server (dai quali erano stati sottratti dati personali degli iscritti), ha comunicato di avere presentato un esposto presso gli Uffici della Polizia Postale e delle Comunicazioni di Milano (cui ha fatto seguito una denuncia querela presentata l'8 settembre 2017) e di avere intrapreso azioni volte a migliorare la sicurezza informatica dei sistemi, la cui capacità di "resistenza" ad attacchi malevoli è stata oggetto di analisi e verifica da parte di tre società specializzate impegnate in attività di vulnerability assessment.

2. Gli accertamenti ispettivi presso l'Associazione Rousseau.

Con la nota del 21 settembre 2017 l'Associazione Rousseau ha fornito chiarimenti, tra gli altri, relativamente ad aspetti di tipo tecnico la cui disamina, anche sulla base delle prime verifiche effettuate sulle procedure di autenticazione on-line ai siti in questione, ha determinato questa Autorità a disporre, in considerazione dei potenziali rischi per la protezione dei dati personali - anche di natura sensibile - degli interessati, l'effettuazione di un'attività ispettiva in loco ai sensi dell'art. 157 del Codice.

Nel corso di tale attività, condotta nei giorni 4 e 5 ottobre 2017, è stato possibile acquisire una serie di informazioni specifiche tramite raccolta di dichiarazioni a verbale (rese dal citato legale rappresentante dell'Associazione Rousseau), sia in ordine all'architettura complessiva del sistema informativo alla base delle applicazioni web interessate dagli attacchi informatici, sia in ordine alla corretta identificazione dei ruoli di titolare e di responsabile del trattamento dei dati personali in questione. Tali informazioni sono state integrate dalla documentazione richiesta dall'Ufficio in sede ispettiva e successivamente trasmessa all'Autorità.

Sulla base di quanto dichiarato dal dott. Davide Casaleggio, è emerso che:

1) con riferimento al blog www.beppegrillo.it, nonché al portale www.movimento5stelle.it e alla piattaforma informatica https://rousseau.movimento5stelle.it, il titolare del trattamento è Giuseppe Piero Grillo, detto Beppe Grillo, il quale ha provveduto a nominare l'Associazione Rousseau quale responsabile del trattamento, con atto di nomina del 25 aprile 2016 (cfr. all. 3 al verbale del 5 ottobre 2017);

2) con riferimento al sito www.blogdellestelle.it, il titolare del trattamento è l'Associazione Rousseau.

In ordine alle rispettive platee di riferimento è stato, peraltro, precisato che le banche dati degli iscritti al sito www.blogdellestelle.it e al portale www.movimento5stelle.it sono nell'esclusiva disponibilità dei rispettivi titolari del trattamento e che non è stato effettuato alcun "travaso automatico" di dati personali dal più risalente blog di Beppe Grillo (www.beppegrillo.it) alla piattaforma Rousseau che del predetto portale è una sorta di "estensione".

Al riguardo si osserva che l'Associazione Rousseau, costituita l'8 aprile 2016 con lo scopo di "promuovere lo sviluppo della democrazia digitale nonché di coadiuvare il Movimento 5 Stelle ed i suoi esponenti nell'organizzazione, promozione e coordinamento delle attività e dei servizi necessari ed utili per l'esercizio dell'azione politica e culturale ed il perseguimento dei suoi obiettivi", si propone di svolgere anche "ogni attività connessa ritenuta utile e opportuna" al raggiungimento del predetto scopo, tra cui la "gestione del sito internet del Movimento 5 Stelle", la "formazione e la gestione degli elenchi degli iscritti" nonché "l'organizzazione e gestione di sistemi e piattaforme di consultazione e votazione in rete" (cfr. Atto costitutivo e Statuto Associazione Rousseau – art. 4, documento inviato in allegato alla nota del 18 ottobre 2017).

La predetta piattaforma web (il c.d. "sistema operativo del Movimento 5 Stelle"), che svolge un ruolo centrale e caratterizzante rispetto all'attività politica del Movimento e della collegata Associazione, presenta diverse funzionalità, tra le quali meritano di essere segnalate:

a) la possibilità di rendere disponibili documenti relativi all'attività amministrativa svolta negli enti locali dai consiglieri eletti nel movimento;

b) la possibilità di inserire proposte da parte degli eletti nel parlamento nazionale, in quello europeo e nei consigli regionali, allo scopo di promuovere il confronto su bozze di proposte legislative da sottoporre poi alle rispettive assemblee, previo confronto con gli iscritti alla piattaforma;

c) la possibilità di svolgere operazioni di c.d. "voto elettronico" per la scelta dei candidati da inserire nelle liste elettorali o per dirimere posizioni all'interno del Movimento (sul punto si rinvia al par. 8).

Nel corso dell'accertamento ispettivo l'Autorità ha chiesto informazioni in ordine ai soggetti addetti alle funzioni di "amministratore di sistema" relativamente ai sistemi software di base (sistemi operativi, sistemi di gestione di base dati e sistemi di gestione dei contenuti) a servizio della piattaforma Rousseau. Al riguardo, il dottor Casaleggio, nel fornire copia di un contratto per servizi di housing e sicurezza gestita stipulato dall'Associazione Rousseau con Wind Tre S.p.a., ha dichiarato che "le funzioni sistemistiche sono affidate da Wind Tre S.p.a. alla società ITNET s.r.l. che mette a disposizione dell'Associazione alcuni tecnici"; peraltro, con successiva nota trasmessa in data 18 ottobre 2017, il dottor Casaleggio ha fornito i nominativi di quattro soggetti ai quali sono stati conferiti ruoli (e relative funzioni) riconducibili alla figura del c.d. "amministratore di sistema".

3. I ruoli di titolare e di responsabile del trattamento.

In relazione agli indicati rapporti interni ed esterni alla "galassia" del Movimento 5 Stelle, si rileva che ai fini del rispetto della normativa in materia di protezione dei dati personali assume, anzitutto, rilievo identificare con precisione i soggetti che, a diverso titolo, possono trattare i dati personali e definire chiaramente le rispettive attribuzioni, in particolare quella di titolare e di responsabile del trattamento (artt. 4, comma 1, lett f) e g) , 28 e 29 del Codice).

In particolare, l'identificazione del titolare del trattamento deve avvenire tenendo conto della sussistenza in capo allo stesso di un effettivo potere decisionale in ordine alle finalità, alle modalità del trattamento e agli strumenti utilizzati, ivi compreso il profilo della sicurezza. Tale potere si estrinseca, tra l'altro, nella facoltà di designare uno o più soggetti - persone fisiche o giuridiche – quali responsabili del trattamento.

Questi ultimi che possono essere individuati dal titolare tra soggetti che per esperienza, capacità ed affidabilità forniscano idonee garanzie in ordine al rispetto delle disposizioni del Codice (cfr. art. 29 del Codice), ivi compreso il profilo relativo alla sicurezza, sono tenuti ad effettuare le operazioni di trattamento nel rispetto delle istruzioni impartite analiticamente e per iscritto dal relativo titolare.

Ciò posto, alla luce di quanto dichiarato dal dottor Casaleggio nel corso dell'accertamento ispettivo e della documentazione prodotta in atti, va esaminato con attenzione il ruolo dei due soggetti sopra indicati, ovvero Wind Tre S.p.A. e ITNET s.r.l..

In particolare, dall'analisi delle modalità con le quali vengono gestiti i database riferiti al Movimento, emerge che le predette società, presso le quali si collocano alcune delle funzioni che rientrano nel campo di applicazione del provvedimento generale dell'Autorità del 27 novembre 2008 su "Misure e accorgimenti prescritti ai titolari dei trattamenti effettuati con strumenti elettronici relativamente alle funzioni di amministratore di sistema" (doc. web 1577499), dovrebbero essere entrambe nominate quali responsabili del trattamento da parte del relativo titolare.

Al riguardo, si evidenzia che la mancata designazione delle società Wind Tre S.p.A. e ITNET s.r.l. quali responsabili del trattamento dei dati personali degli utenti dei diversi siti riferibili al Movimento 5 Stelle, configura l'illiceità del trattamento medesimo in ragione della comunicazione dei dati a soggetti terzi, in mancanza del consenso degli interessati; pertanto, questa Autorità, si riserva di verificare, con autonomo procedimento, la sussistenza dei presupposti per l'eventuale contestazione delle sanzioni amministrative di cui all'art. 162, comma 2bis del Codice.

4. La sicurezza informatica della piattaforma Rousseau.

L'esame delle informazioni acquisite presso l'Associazione Rousseau e delle risultanze dei vulnerability assessment da questa commissionati a società esterne e successivamente parzialmente trasmesse all'Autorità e l'analisi tecnica conseguentemente condotta dall'Autorità medesima su tutto il materiale di cui è potuta venire a conoscenza hanno consentito di comprendere le criticità dei sistemi informatici e, quindi, le vulnerabilità software probabilmente sfruttate dall'attaccante (o dagli attaccanti) per compiere le intrusioni informatiche e la conseguente diffusione di dati personali.

In particolare è emerso che:

a) il portale web del Movimento 5 Stelle e parte della piattaforma Rousseau sono stati realizzati avvalendosi di un prodotto software, il CMS Movable Type che, nella versione Enterprise 4.31-en, è risultata affetta da indiscutibile obsolescenza tecnica (il produttore individuava nel 31 dicembre 2013 la data di "fine vita" delle versioni 4.3x). Il blog www.beppegrillo.it utilizza invece una versione del CMS Movable Type ancora più risalente (versione 3.35), con la quale la registrazione delle password avveniva in chiaro. Le obsolescenze dei CMS (sistemi di gestione dei contenuti), oltre a esporre i dati personali trattati a rischi di accesso abusivo (rischi derivanti dalle vulnerabilità informatiche già note e segnalate dallo stesso produttore), ha condizionato l'efficacia di alcuni accorgimenti tecnici adottati successivamente dall'Associazione a seguito delle intrusioni informatiche; ad esempio il portale non realizzava policy efficaci sulla qualità delle password, ammettendo l'uso di password banali, facilmente esposte alla decifrazione e ad attacchi di tipo brute force anche in modalità interattiva online;

b) i vulnerability assessment commissionati dall'Associazione Rousseau hanno evidenziato una serie di criticità cui sarebbe stato possibile porre rimedio avvalendosi di una metodologia di sviluppo del software maggiormente strutturata, che avesse contemperato la tempestività realizzativa delle nuove funzionalità con una attenta valutazione e prevenzione dei rischi informatici. In proposito si osserva che il nuovo Regolamento generale riconosce come la protezione dei dati personali debba essere perseguita individuando misure a protezione dei dati sin dalla fase di progettazione dei sistemi informativi con cui si realizzano i trattamenti (c.d. approccio basato sulla "Data protection by design" - cfr. art. 25 Regolamento UE 2016/679 "Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita");

c) con riferimento al database Rousseau, il documento trasmesso all'Autorità recante "Estratto delle tabelle principali di Rousseau", ha permesso di valutare alcuni aspetti relativi alla riservatezza delle operazioni di voto elettronico svolte tramite la piattaforma; in particolare, l'esame delle predette tabelle ha mostrato come l'espressione del voto da parte degli iscritti, in occasione della scelta di candidati da includere nelle liste elettorali del Movimento o per orientare altre scelte di rilevanza politica, venga registrata in forma elettronica mantenendo uno stretto legame, per ciascun voto espresso, con i dati identificativi riferiti ai votanti; nello schema del database risulta infatti che ciascun voto espresso sia effettivamente associato a un numero telefonico corrispondente (come del resto confermato dal dottor Casaleggio in sede ispettiva, cfr. verbale 5 ottobre 2017) al rispettivo iscritto-votante. Tale riferimento sarebbe mantenuto nel database per asserite esigenze di sicurezza, comportando, tuttavia, la concreta possibilità di associare, in ogni momento successivo alla votazione, oltre che durante le operazioni di voto, i voti espressi ai rispettivi votanti. La possibilità di tracciare a ritroso il voto espresso dagli interessati non risulta neppure bilanciata, per esempio, da un robusto sistema di log degli accessi e delle operazioni svolte da persone dotate dei privilegi di amministratore della piattaforma che consenta, almeno, di condurre a posteriori azioni di auditing sulla liceità dei trattamenti attuati dal detentore dell'archivio elettronico.

5. Profili di carattere generale: l'informativa.

Nel corso dell'accertamento ispettivo, anche tenendo conto di alcune richieste ed osservazioni contenute nelle segnalazioni pervenute all'Autorità, si è proceduto a richiedere alcuni chiarimenti preliminari, con specifico riferimento alle informative rilasciate ai sensi dell'art. 13 del Codice agli utenti dei diversi siti web sopra indicati collegati all'attività del Movimento 5 Stelle.

Al riguardo, alla luce delle sintetiche informazioni pervenute nonché sulla base dell'esame delle informative pubblicate nei rispettivi siti web (quali risultano alla data del 18 dicembre 2017 e allegate al presente provvedimento), si formulano le osservazioni di seguito riportate.

5.1 Il sito www.movimento5stelle.it, che indica quale titolare del trattamento il Sig. Giuseppe Grillo, riporta una informativa formulata in modo estremamente sintetico, che contiene sostanzialmente la maggior parte degli elementi previsti dall'art. 13 del Codice e indicati anche dall'Autorità nel provvedimento del 6 marzo 2014 "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" (doc. web 3013267).

La stessa - che è stata oggetto di recenti aggiornamenti - risulta, tuttavia, carente con riferimento al punto d) dell'art. 13, comma 1, del Codice relativo all'indicazione "dei soggetti o categorie di soggetti ai quali i dati possono essere comunicati". Nel testo dell'informativa, infatti, mentre da un lato si indica l'Associazione Rousseau quale responsabile del trattamento ai sensi dell'art. 29 del Codice (designata con atto datato 25 aprile 2016 e allegato al verbale dell'accertamento ispettivo del 5 ottobre 2017), dall'altro, non è fatta menzione delle società Wind Tre S.p.A. e ITNET s.r.l. cui i dati personali degli utenti vengono comunicati, ed è anzi riportato che "i dati non verranno diffusi né comunicati a terzi" (cfr. par. 3).

Pertanto, risultando la predetta informativa parzialmente inidonea rispetto al dettato normativo di cui all'art. 13, comma 1, lett. d) del Codice, l'Autorità si riserva di verificare, con autonomo procedimento, la sussistenza dei presupposti per l'eventuale contestazione della sanzione amministrativa di cui all'art. 161 del Codice.

5.2 La piattaforma Rousseau (https://rousseau.movimento5stelle.it), in quanto sistema operativo del Movimento, si avvale della medesima informativa di cui al punto 5.1; sul punto si rileva che la piattaforma - all'interno della quale l'utente può navigare come "ospite" o invece accedere (tramite login e password, cui segue verifica dell'identità) al fine di "parteciparlo attivamente" – offre funzionalità di particolare delicatezza sotto il profilo della riservatezza dei dati personali degli interessati che utilizzano il sistema operativo quale strumento di interazione e di partecipazione politica (cfr. le osservazioni sulla votazione elettronica al par. 4, lett. c)).

In ragione della delicatezza di tali profili, questa Autorità ritiene di dover prescrivere, nei confronti del titolare del trattamento, ai sensi dell'art. 154, comma 1, lett. c) del Codice, considerata anche la rilevata sinteticità dell'informativa generale sul trattamento dei dati, la previsione di un'informativa ad hoc, che illustri in modo puntuale le finalità e le modalità del trattamento dei dati personali connessi all'utilizzo della piattaforma in questione.

5.3 Il sito www.beppegrillo.it, che indica quale titolare del trattamento il Sig. Beppe Grillo e la società Casaleggio Associati s.r.l. quale responsabile del trattamento, pur contenendo un'informativa sostanzialmente comprensiva di tutti gli elementi previsti dall'art. 13 del Codice, presenta la descrizione di alcune modalità di trattamento dei dati sulle quali occorrerebbe uno sforzo volto a meglio chiarire alcuni passaggi che risultano troppo sintetici e non agevolmente comprensibili da un utente che consulti tale informativa per la prima volta.

Si evidenzia infatti che, mentre nell'informativa in esame è riportato che "i dati acquisiti verranno condivisi con il "Blog delle Stelle" e dunque comunicati alla Associazione Rousseau che ne è il titolare", nel corso dell'accertamento ispettivo il dottor Davide Casaleggio ha dichiarato (cfr. verbale del 5 ottobre 2017) che "non è stato effettuato alcun travaso automatico di dati personali dal più risalente blog di Beppe Grillo (www.beppegrillo.it) alla piattaforma Rousseau". Per quanto, infatti, i soggetti in gioco non siano perfettamente sovrapponibili (la "condivisione" citata riguarderebbe infatti la banca dati riferita al blog www.beppegrillo.it e il "blog delle stelle" e non la piattaforma Rousseau), appare chiaro che l'intreccio dei siti web in questione e l'assunzione, da parte dell'Associazione Rousseau, del ruolo di titolare del trattamento in alcuni casi e di responsabile in altri, non favorisce, nelle informative in esame, il raggiungimento di quegli obiettivi di trasparenza, correttezza ed affidabilità nei confronti degli interessati cui tale istituto è volto.

Si rileva peraltro che anche con riferimento all'informativa contenuta nel blog in esame, devono essere formulate le medesime considerazioni già espresse al punto 5.1 relativamente alla mancata indicazione dei soggetti ai quali i dati vengono comunicati (Wind Tre S.p.A. e ITNET s.r.l.); pertanto l'informativa in questione dovrà essere riformulata conformemente a quanto indicato al predetto 5.1

Con riferimento alle finalità promozionali e pubblicitarie, di cui pure vi è cenno nel blog in questione, si rinvia al successivo paragrafo 6.

5.4 Il sito www.ilblogdellestelle.it, che indica quale titolare del trattamento l'Associazione Rousseau, presenta un'informativa formulata

anch'essa in modo estremamente sintetico e comunque priva di ogni indicazione relativa ai soggetti cui i dati vengono comunicati (Wind Tre S.p.A. e ITNET s.r.l.); ne consegue che la stessa dovrà essere riformulata conformemente a quanto indicato al predetto 5.1

Con riferimento alle finalità promozionali e pubblicitarie si rinvia al successivo paragrafo 6.

6. La raccolta del consenso degli interessati.

I siti web esaminati (con la sola eccezione di www.ilblogdellestelle.it in quanto non sembrerebbe attiva la funzione di autenticazione) contengono dei form per la registrazione/autenticazione degli utenti in cui, in calce agli spazi dedicati al conferimento dei dati personali necessari alla registrazione medesima, è presente un campo che l'utente è tenuto a "flaggare", esprimendo in questo modo il consenso al trattamento dei propri dati, anche sensibili, per le finalità illustrate nelle relative informative di cui contestualmente dichiara di aver preso visione.

In proposito, occorre in primo luogo ricordare che i partiti, i movimenti e le altre formazioni a carattere politico possono lecitamente utilizzare, senza uno specifico consenso degli interessati, i dati sensibili riferiti agli aderenti o ad altri soggetti che con gli stessi intrattengono contatti regolari per il perseguimento di scopi determinati e legittimi individuati, anzitutto, dall'atto costitutivo o dallo statuto, a condizione che non siano comunicati all'esterno o diffusi, siano determinate idonee garanzie e venga resa agli interessati medesimi un'idonea e preventiva informativa ai sensi dell'art. 13 del Codice (art. 26, comma 4, lett. a) del Codice; autorizzazione n. 3/2016 al trattamento dei dati sensibili da parte degli organismi di tipo associativo e delle fondazioni; punti 1 e 2 del "Provvedimento in materia di trattamento di dati presso i partiti politici e di esonero dall'informativa per fini di propaganda elettorale" - 6 marzo 2014 (doc. web 3013267).

Si segnala tuttavia che laddove, invece, si intendano utilizzare i dati degli aderenti per finalità ulteriori e diverse rispetto a quelle costitutive o statutarie quale la "promozione di iniziative commerciali e pubblicitarie" (come riportato nell'informativa rinvenuta sul sito www.beppegrillo.it e www.ilblogdellestelle.it), poiché tali finalità non sono sovrapponibili alle altre, alle stesse va data separata evidenza e, al riguardo, l'interessato deve poter esprimere un consenso specifico (ovvero negare lo stesso), ferma restando la possibilità di fruire dei contenuti e delle altre funzionalità dei siti web. Ciò, rimanendo comunque impregiudicata la possibilità di esercitare il diritto di opposizione al trattamento dei dati - e di eventuale loro cancellazione - ai sensi dell'art. 7 del Codice, anche successivamente.

Si prescrive, pertanto, nei confronti dei titolari del trattamento dei siti www.beppegrillo.it e www.ilblogdellestelle.it, quale misura necessaria ai sensi dell'art. 154, comma 1, lett. c) del Codice, l'adozione (qualora sia ravvisata la necessità di tali trattamenti) di una specifica modalità di acquisizione del consenso al trattamento dei dati personali per finalità di promozione commerciale e pubblicitaria, che consenta all'interessato di prestare - ovvero negare - il consenso al trattamento dei propri dati personali per tali finalità, ferma restando la possibilità di fruire dei contenuti e delle altre funzionalità dei relativi siti web nonché il diritto di esercitare i diritti di cui all'art. 7 del Codice (in particolare, di opposizione e di cancellazione).

7. Le valutazioni dell'Autorità in ordine ai profili di sicurezza informatica: misure e accorgimenti necessari.

Sulla base delle criticità tecniche accertate, si ritiene necessario prescrivere, nei confronti dei titolari del trattamento dei diversi siti web riferibili al Movimento 5 Stelle, le seguenti misure necessarie, come di seguito descritte.

A. I futuri sviluppi della piattaforma Rousseau e degli altri strumenti on-line del Movimento dovranno sempre essere validati sul piano della sicurezza informatica da adeguate azioni di **vulnerability assessment** attuate precedentemente alla messa in esercizio, allo scopo di individuare e correggere eventuali vulnerabilità nei servizi prima di renderli fruibili al pubblico. Le verifiche sulla tenuta delle misure di sicurezza dovranno essere periodicamente rinnovate, al fine di garantire un livello costante nel tempo di protezione dei dati personali.

B. Con riferimento al **sistema di autenticazione informatica** degli utenti, lo stesso dovrà essere modificato in modo che le password relative alle utenze degli iscritti ai siti on-line del Movimento siano di lunghezza non inferiore a otto caratteri e siano sottoposte a un controllo automatico di qualità che impedisca l'uso di password "deboli" costituite, ad esempio, da parole reperibili in dizionari o comunque facilmente individuabili. Contestualmente devono essere introdotte strette limitazioni al numero di tentativi di accesso online con password erronea, per impedire attacchi brute force interattivi.

C. Con riferimento ai **protocolli di rete**, si ritiene necessario prescrivere l'adozione del protocollo https (secure hyper text transport protocol) per l'accesso a tutti i contenuti del sito www.movimento5stelle.it, basato su un certificato digitale emesso da una Certification Authority riconosciuta, dal momento che alla data odierna emerge solo una parziale adozione di questa misura di sicurezza. Infatti, sebbene l'accesso alla home page del sito avvenga tramite il protocollo https, alcuni contenuti sono ancora erogati su protocollo insicuro. Inoltre, nonostante il form di iscrizione sia accessibile tramite https, lo stesso risulta tuttora raggiungibile anche nella modalità insicura.

D. Con riferimento al **database delle utenze** del sito del Movimento della piattaforma Rousseau, tenuto conto delle segnalazioni ricevute - che hanno trovato conferma anche nell'analisi del CMS Movable Type v4.31 il cui codice sorgente è risultato liberamente disponibile -, si ritiene necessario prescrivere che le modalità di conservazione delle password degli utenti siano rafforzate adoperando algoritmi crittografici robusti in luogo delle semplici routine di cifratura accessibili tramite le funzioni native del CMS medesimo.

E. Con riferimento alle **misure di auditing** per la verifica della liceità dei trattamenti compiuti dagli incaricati dotati di profili di autorizzazione ampi e speciali, allo scopo di fornire maggiori garanzie a tutela degli iscritti votanti, in accordo al principio di trasparenza che dovrebbe caratterizzare un sistema di e-voting, si ritiene necessario prescrivere l'adozione di misure che consentano l'auditing informatico mediante la tenuta delle registrazioni degli accessi e delle operazioni compiute (log) sul database del sistema Rousseau, attuando gli accorgimenti di cui al provvedimento generale del Garante del 27 novembre 2008 in tema di amministratori di sistema (doc. web 1577499).

F. Con specifico riferimento al sito www.beppegrillo.it - che risulta essere stato realizzato impiegando il CMS Movable Type nella versione 3, ormai assolutamente obsoleta e affetta da un'ampia serie di vulnerabilità cui sono state esposte nel tempo le applicazioni web con essa sviluppate - allo scopo di incrementare con urgenza il livello di protezione dei dati contenuti nel database di tale sito, si prescrive:

1. l'adozione del protocollo sicuro https;

2. l'adozione di tecniche crittografiche efficaci per la conservazione delle password;

3. l'avvio di un'opera di correzione delle vulnerabilità segnalate nei report dei vulnerability assessment;

4. l'avvio di un'operazione di validazione delle utenze volta a eliminare quelle non più utilizzate da lungo tempo e, pertanto, ragionevolmente, abbandonate.

8. Il profilo della riservatezza delle operazioni di voto elettronico.

8.1 Ferma restando la libertà di ogni associazione privata – quale appunto un movimento o partito politico - di strutturarsi con proprie regole (e a condizione che delle stesse sia fornita adeguata informazione a tutti gli associati), si evidenzia come, alla luce delle risultanze istruttorie, le misure di sicurezza connesse al controllo delle operazioni di voto destino alcune perplessità.

In particolare, mentre la scelta di associare a ogni voto espresso il numero telefonico dell'iscritto "verificato", può avere, in astratto, motivazioni di carattere tecnico o di sicurezza relativamente all'esigenza di assicurare la "certezza" del voto, la stessa presenta delle forti criticità rispetto all'esigenza (se tale è, alla luce di quanto dichiarato a verbale) di garantire la riservatezza delle votazioni. I voti espressi tramite le funzionalità di e-voting offerte dalla piattaforma, infatti, vengono archiviati, storicizzati e restano imputabili a uno specifico elettore anche successivamente alla chiusura delle operazioni di voto, consentendo elaborazioni a ritroso con - in astratto - la possibilità di profilare costantemente gli iscritti sulla base di ogni scelta o preferenza espressa tramite il "sistema operativo" (siano esse relative alla scelta di un candidato ovvero all'approvazione di un'iniziativa politica o legislativa); ciò senza che sia previsto un meccanismo di anonimizzazione o pseudonimizzazione ex post (se non immediatamente dopo l'espressione del voto almeno alla conclusione delle votazioni e delle relative verifiche), e senza che sia previsto un termine, decorso il quale, le informazioni riferibili ad interessati vengano rimosse o trasformate in forma anonima.

8.2 In proposito, per sopperire a questa condizione di possibile violazione della riservatezza, acuita dalle vulnerabilità note e da quelle comunque residuali, perché non note e potenzialmente sfruttabili da un attaccante esterno sufficientemente esperto, sarebbe necessario che il sistema di e-voting venisse riconfigurato in modo da minimizzare i rischi per i diritti e per le libertà delle persone fisiche, in accordo al principio di "data protection by default" e alle previsioni di cui all'articolo 32, par. 1, lett. a) del nuovo Regolamento 679/2016, prevedendo la cancellazione o la trasformazione in forma anonima dei dati personali trattati (laddove per specifiche esigenze fossero presenti), una volta terminate le operazioni di voto. A tale scopo andrà modificato lo schema del database laddove prevede l'utilizzo del numero telefonico dell'iscritto in connessione ai voti elettronici espressi.

Nell'effettuare queste modifiche si potrà anche eventualmente trarre ispirazione dalle indicazioni in tema di anonimizzazione fornite dal Working Party WP29 con la Opinion 5/2014 on anonymization techniques.

TUTTO CIÒ PREMESSO, IL GARANTE,

- ai sensi dell'art. 154, comma 1, lett. a), b) e c) del Codice:

1) prescrive nei confronti dei titolari del trattamento dei siti web riferibili al Movimento 5 Stelle le misure necessarie relative ai profili concernenti la sicurezza informatica di cui al paragrafo 7 della premessa;

2) prescrive nei confronti del titolare del trattamento del sito web www.movimento5stelle.it e della piattaforma Rousseau:

a) quale misura necessaria, l'indicazione, nell'informativa resa ai sensi dell'art. 13 del Codice, dei soggetti (o categorie di soggetti) ai quali i dati sono comunicati, nei termini di cui al par. 5.1, salvo che il titolare del trattamento provveda alla loro designazione quali responsabili del trattamento ai sensi dell'art. 29 del Codice;

b) quale misura necessaria, la previsione di una informativa specifica relativa alle funzionalità della piattaforma Rousseau nei termini di cui al paragrafo 5.2.;

c) quale misura opportuna, l'adozione degli accorgimenti di cui al paragrafo 8.2.

3) prescrive nei confronti del titolare del trattamento del sito www.beppegrillo.it:

a) quale misura necessaria, l'adozione di una specifica modalità di acquisizione del consenso al trattamento dei dati per finalità di promozione commerciale e pubblicitaria nei termini di cui al paragrafo 6;

b) quale misura necessaria, l'indicazione, nell'informativa resa ai sensi dell'art. 13 del Codice, dei soggetti (o

categorie di soggetti) ai quali i dati sono comunicati, nei termini di cui al par. 5.1, salvo che il titolare del trattamento provveda alla loro designazione quali responsabili del trattamento ai sensi dell'art. 29 del Codice;

c) quale misura opportuna, una più chiara enunciazione dei flussi di dati nei confronti delle altre entità del Movimento, come rilevato nel paragrafo 5.3;

4) prescrive nei confronti del titolare del trattamento del sito www.blogdellestelle.it:

a) quale misura necessaria, l'adozione di una specifica modalità di acquisizione del consenso al trattamento dei dati per finalità di promozione commerciale e pubblicitaria nei termini di cui al paragrafo 6;

b) quale misura necessaria, l'indicazione, nell'informativa resa ai sensi dell'art. 13 del Codice, dei soggetti (o categorie di soggetti) ai quali i dati sono comunicati, nei termini di cui al paragrafo 5.1, salvo che il titolare del trattamento provveda alla loro designazione quali responsabili del trattamento ai sensi dell'art. 29 del Codice;

5) dichiara, nei confronti dei titolari del trattamento di tutti i siti riconducibili al Movimento 5 Stelle, l'illiceità del trattamento dei dati personali degli utenti in ragione della comunicazione a soggetti terzi (Wind Tre S.p.A. e ITNET s.r.l.) dei dati medesimi in mancanza di idoneo presupposto;

6) dichiara, nei confronti dei medesimi titolari del trattamento, la parziale inidoneità dell'informativa resa ai sensi dell'art. 13 del Codice, nei termini di cui al paragrafo 5;

7) si riserva di verificare, con riferimento ai precedenti punti 5) e 6), la sussistenza dei presupposti per l'eventuale contestazione delle sanzioni amministrative di cui agli artt. 161 e 162, comma 2bis del Codice;

• ai sensi dell'art. 157 del Codice, invita, altresì, i titolari del trattamento a comunicare quali iniziative siano state intraprese al fine di dare attuazione a quanto prescritto al punto 1) del presente dispositivo entro 60 giorni dalla data di ricezione del presente provvedimento e che le misure necessarie di cui ai punti 2), 3) e 4) siano adottate dai rispettivi titolari del trattamento entro 30 giorni dal ricevimento del presente provvedimento.

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, 21 dicembre 2017

IL PRESIDENTE
Soro

IL RELATORE
Bianchi Clerici

IL SEGRETARIO GENERALE
Busia