PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 21 - numero 4445 di Mercoledì 10 aprile 2019

Il provvedimento dell'autorità Garante sulla piattaforma Rousseau

I giornali stanno dando ampio spazio alla reazione del titolare del trattamento della piattaforma Rousseau per l'applicazione di una significativa sanzione da parte del Garante. Perché i lettori possano farsi un'opinione, è bene che conoscano i fatti.

In allegato a questa notizia ho riportato il provvedimento, in base al quale l'autorità Garante ha ritenuto che le indicazioni in merito al livello di sicurezza della piattaforma Rousseau, emanate in occasione di una precedente ispezione con emissione di sanzione, non siano state pienamente rispettate.

È stata così applicata una nuova sanzione, secondo le modalità indicate nel decreto legislativo 101/2018. Il titolare del trattamento ha fatto presente che probabilmente la sanzione era dovuta all'appartenenza politica del presidente dell'autorità Garante.

Al proposito, i fatti dicono che l'autorità Garante è un organismo collegiale, composto da quattro componenti, designati dai due rami del parlamento. Tutti e quattro i componenti si sono dichiarati d'accordo nell'emissione della sanzione, dopo aver letto i risultati della ispezione effettuata dai tecnici dell'autorità Garante.

Per quanto riguarda i motivi tecnici, alla base dell'applicazione delle sanzioni, riporto di seguito alcuni passi del provvedimento, che è disponibile comunque nella sua completezza in allegato a questa nota. In corsivo riporto di seguito alcuni passi di questo provvedimento.

Tanto per cominciare, gli esperti dall'autorità Garante hanno messo in evidenza come la piattaforma su cui gira questo applicativo di voto elettronico è oltremodo obsoleta, tant'è vero che il produttore ha smesso di sostenerla, con l'emissione di aggiornamenti, al 31 dicembre 2013.

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 log 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.

Durante l'ispezione, è stato accertato che gli accessi ai dati contenuti in questa piattaforma possono essere effettuati sia da un terminale remoto, con modalità sufficientemente garantistiche in termini di procedura di accesso e log delle attività svolte, mentre gli accessi non sono controllati, utilizzando un altro percorso, accessibile solo agli amministratori di sistema. Per questi accessi non è nemmeno documentabile il log delle attività svolte, lasciando quindi ampio spazio a possibili manipolazioni non documentabili o tracciabili.

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,

Gli esperti hanno anche messo in evidenza come le procedure di "certificazione" dei risultati, che possono essere eseguite da notai o altri soggetti pubblici affidabili, possono essere attuate a distanza di numerosi giorni dalla chiusura delle votazioni elettroniche, lasciando ampio spazio per una manipolazione dell'esito delle votazioni, senza che di tale eventuale manipolazione risulti alcuna traccia.

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.

Questa fondamentale lacuna, che non protegge quindi da possibili manipolazioni i voti, espressi dai votanti, è aggravata dalla assenza di adeguate procedure di auditing. In altre parole alcuni soggetti fisici, ben identificati, possono fare tutto ciò che desiderano, senza lasciare alcuna traccia del loro operato.

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.

Il provvedimento prosegue ribadendo tutte le perplessità degli ispettori sulle modalità di validazione dei voti.

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".

Gli ispettori metto in evidenza un'altra grave lacuna, che non viene mai tollerata, legato al fatto che il codice identificativo personale e le parole chiave che vengono attribuite ai soggetti fisici, autorizzati al trattamento, sono condivise fra più persone fisiche diverse. La condivisione di credenziali è uno dei peccati più gravi che può compiere un titolare, in quanto impedisce una oggettiva attribuzione di responsabilità a una persona fisica, in caso di trattamenti non appropriati.

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

Infine, gli ispettori hanno rilevato un'altra grave lacuna, in quanto il titolare del trattamento non ha effettuato la valutazione di impatto, in conformità all'articolo 35 del regolamento generale europeo 679 / 2018, che ovviamente è obbligatoria per trattamenti di tali criticità.

Infine, il provvedimento si chiude elencando le ragioni, in base ai quali è stata determinata la sanzione di 50.000 ?. Sono stati analizzati tutti i vari fattori, che contribuiscono a che la sanzione sia "effettiva, proporzionata e dissuasiva", come esplicitamente il regolamento prevede.

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).

A questo punto, conosciuti fatti, ogni lettore è libero di sviluppare la propria opinione.

Il provvedimento (pdf)

Adalberto Biasiotti

www.puntosicuro.it