DOPPIOZERO

Tre problemi per Rousseau

Giovanni Ziccardi
5 Settembre 2019

Il dibattito sui sistemi di consultazione o di sondaggio online – eviterei il termine “voto” che sarebbe, a mio parere, da riservare unicamente alle reali, e rarissime, tornate elettorali elettroniche durante elezioni o referendum – si accende, regolarmente, quando un dato campione di persone (la base/iscritti di un partito o gli appartenenti a un determinato gruppo o movimento) viene “interrogato” su un determinato punto programmatico o politico.

Si tratta di un dibattito vecchio di decenni che, però, il caso di Rousseau in Italia riporta regolarmente in auge. Ogni volta, al contempo, appaiono, evidenti, alcune criticità molto importanti che gli studiosi, da anni, affrontano e denunciano con riferimento a simili sistemi.

Sono, a nostro avviso, punti centrali e non di mero dettaglio, “difetti” che possono viziare senza pietà, parzialmente o totalmente, un sistema che può presentare, indubbiamente, anche dei vantaggi e dei lati positivi.

Muovendo proprio da ciò che è successo in questi giorni in Italia – ma mantenendo lo sguardo fisso anche su altri Paesi, quali l’Estonia, la Svizzera, la Germania, l’India e gli Stati Uniti d’America che, da tempo, sperimentano sistemi simili – si possono individuare tre punti di criticità che sono idonei a sollevare spunti di riflessione.

Si tratta di un argomento, quello della consultazione politica online, che è molto delicato e scivoloso: non vi sono, infatti, soltanto i problemi tecnologici che andremo a evidenziare, ma anche spinose questioni politiche, di democrazia, di rappresentanza che, spesso, si fondono insieme e rendono il quadro ancora più complesso per l’interprete. Si pensi, a puro titolo di esempio, alla “morte” dell’intermediazione e, quindi, alla necessità di quesiti semplici, spesso banali, più adatti a un click immediato e “distratto” che a una reale riflessione prima dell’espressione del consenso.

I tre punti tecnologici critici sono, a nostro avviso, i seguenti.

1. Il problema della trasparenza generale del sistema utilizzato

Qualsiasi sistema di consultazione, o “voto” elettronico, che abbia un’importanza centrale per un sistema politico o per uno Stato e che sia da considerare, quindi, come una vera e propria “infrastruttura critica”, deve essere obbligatoriamente trasparente.

“Trasparente” significa sia verificabile nella sua gestione e proprietà, sia nel codice sorgente utilizzato. Il codice sorgente, ossia il DNA del software o, comunque, delle tecnologie che sono utilizzate, deve essere

aperto, verificabile da tutti (sottoponibile a una sorta di “scrutinio pubblico”) e controllabile in ogni momento nel suo intero processo.

La trasparenza non ha, si badi bene, solo un fine di sicurezza (che vedremo meglio nel punto che segue), ma anche una funzione di garanzia di correttezza, di regolarità e di fiducia (“trust”).

Un sistema chiuso, oscuro, proprietario richiede in chi lo utilizza una enorme dose di fiducia acritica da parte di chi vota. Ci si deve fidare ciecamente della società che offre il prodotto, ma se il “motore” del sistema non è visibile, già di per sé si tratta di un sistema non idoneo a operazioni di questo tipo. In altre parole: un sistema oscuro è già, di per sé, un sistema insicuro e non idoneo.

Negli Stati Uniti d’America ci fu, su questo punto, una polemica molto violenta nei confronti di un produttore di macchine per il voto elettronico che non voleva rivelare il funzionamento delle sue tecnologie (per proteggere, ovviamente, il segreto industriale e il valore del prodotto) ad alcuni Stati che glielo avevano domandato. Un documentario di alcuni anni fa (era il 2006), intitolato *Hacking Democracy* e candidato a un Emmy Award per il giornalismo investigativo, ha ben descritto questo punto. Altri sviluppatori, nel mondo, hanno scelto, invece, di costruire simili piattaforme su codice aperto proprio per prevedere sin dall’inizio una trasparenza “congenita” del sistema.

L’idea di una piattaforma per la consultazione, o voto, che non sia trasparente nel suo progetto e funzionamento, vanifica sin dagli esordi l’affidabilità di un sistema pensato per simili finalità.

2. Il problema della vulnerabilità del sistema

Un sistema di voto che abbia effetti sugli equilibri democratici deve essere, poi, sicuro.

La sicurezza non si raggiunge soltanto attraverso la trasparenza del codice, come indicato nel punto precedente, ma anche pensando sin dall’inizio il sistema come un ambiente che può essere soggetto ad attacchi operati da individui o da organizzazioni con grandi mezzi e capacità tecniche.

Il rischio è di avviare un progetto con una piattaforma/architettura intrinsecamente debole e, poi, cercare di "aggiustare le cose" in corsa, procedura che non dà mai, di solito, buoni frutti.

Il problema è che la predisposizione di un quadro informatico sicuro è la parte più costosa dell'intero progetto/processo. Richiede competenze e tecnologie ad hoc, penetration test (attacchi esterni concordati contrattualmente) operati da società esterne indipendenti, certificazioni dei processi.

Ma non solo: la sicurezza deve essere anche prevista con riferimento a competenze e azioni malevole interne, ossia la possibilità che, ad esempio, gli amministratori di sistema o i gestori della piattaforma possano modificare a loro piacimento l'esito, spostare i voti, sopprimere preferenze. Anche i votanti, ossia le utenze che possono, con un click, dare una preferenza, dovrebbero essere controllati con cura, per evitare che un singolo cittadino abbia, ad esempio, quattro o cinque utenze attive e possa, così, esprimere più voti.

Nel febbraio del 2019 ENISA, l'agenzia dell'Unione Europea che si occupa di cybersecurity, ha pubblicato uno studio ("Election cybersecurity: challenges and opportunities") dove evidenzia una tendenza, in molti Stati Europei, di abbandonare i sistemi di voto elettronico, e di tornare al voto "cartaceo", proprio per timori correlati alla sicurezza informatica degli stessi. Il report cita i casi dell'Irlanda, dell'Olanda, della Francia, della Finlandia e della Germania e, al contrario, gli esempi di Estonia e Belgio quali Paesi più fiduciosi nelle possibilità del voto elettronico.

3. Il punto spinoso della "certificazione" dei risultati

Qui il punto cruciale, finale, è la differenza tra una certificazione dei risultati della consultazione e una certificazione della correttezza dei processi alla base.

Per "certificazione dei risultati" s'intende, ad esempio, l'azione di un notaio (o di altro organo terzo) che certifichi l'esito della consultazione/sondaggio.

Si tratta però, in molti casi, di una certificazione di un "qualcosa", uno stato di fatto, che viene comunicato al notaio ma che può essere benissimo esito di una alterazione precedente.

Differente, ma molto più complesso nella pratica, è invece il permettere a un notaio di seguire in tempo reale l'intero processo e certificare la correttezza dei voti dopo aver potuto verificare anche, preliminarmente, la correttezza del procedimento.

Si immagini, però, la difficoltà, ad esempio in una votazione che coinvolga 70.000 persone, di una simile operazione: il notaio dovrebbe controllare uno a uno i votanti, verificare la loro identità, verificare i voti espressi e certificare la regolarità del tutto.

Nel caso di Rousseau, tutti e tre i punti che abbiamo esposto sono stati, negli anni e anche nelle ultime ore, messi in discussione.

Il Garante per la Protezione dei dati si è concentrato, nei mesi scorsi, sull'analisi degli aspetti di responsabilità degli amministratori del sistema (e tenuta dei file di log) per il timore di manipolazione, di protezione della privacy degli utenti/votanti, di individuazione di sistemi di autenticazione (anche tramite cellulare) e di separazione tra identità degli utenti e loro dati di voto. Questo si è trattato di un processo di "adeguamento" obbligatorio, per i gestori di Rousseau, perché legato a possibili sanzioni future.

La parte, invece, della trasparenza si presenta più come una scelta per così dire “etica” che, però, è inscindibilmente legata all’essenza stessa e, soprattutto, alla credibilità del sistema.


LaPresse
LaPresse