eVoting, opportunità o sfida impossibile?

Negli ultimi due anni il mondo, le nostre vite, il nostro modo di lavorare, di comunicare, di rapportarci con gli altri sono cambiati. La pandemia ha imposto una presa di coscienza sulle necessità e le potenzialità dei mezzi tecnologici per la comunicazione a distanza, recepite in modo tutto sommato positiva nel nostro paese, tradizionalmente restio all'innovazione, nonostante sacche di resistenza che di tanto in tanto riaffiorano.

Il cambiamento è ormai in atto e tutti i professionisti del settore informatico e tecnologico si augurano che il processo di digitalizzazione sia finalmente affrontato con l'entusiasmo e la consapevolezza che caratterizzano altri aspetti delle nostre vite personali e sociali.

L'impossibilità di utilizzare modalità presenziali ha, tra le tante, riacceso il dibattito sulla tematica del voto elettronico dati gli evidenti vantaggi logistici come la facilità di accesso al voto (voto da remoto, *anytime and anywhere*), potenziale riduzione dei costi (meno personale, meno burocrazia), ed immediatezza dei risultati (metriche istantanee e verificabili). Eppure la comunità scientifica è per lo meno scettica rispetto al voto elettronico, perché? É davvero, passateci il termine, tutto *rose e fiori*?

Le elezioni sono un processo democratico, unico nel loro genere, fondato sulla fiducia di tutti i partecipanti. Senza tale fiducia, il processo democratico perde di significato.

Questo articolo, a firma di un gruppo di ingegneri della Commissione ICT dell'Ordine di Verona, si pone come obiettivo il dare spunti di riflessione sui vantaggi e sulle sfide della transizione al voto digitale, sottolineandone aspetti positivi e problemi ad oggi irrisolvibili. L'occasione di un confronto nasce anche con il rinvio della sperimentazione del voto elettronico per le elezioni politiche al 2023 (Camera dei Deputati 2022), e la scelta data dal CNI ai singoli Ordini provinciali rispetto alla decisione di adozione della modalità telematica per il rinnovo dei Consigli (Zambrano 2022).

Premesse e requisiti di un sistema di voto

Il processo di voto non può prescindere da una serie di premesse e requisiti che devono essere rispettati, in mancanza di anche uno solo dei quali l'intero sistema perde di validità e di riconoscimento. La costituzione stessa (art.48) sancisce il diritto di voto a suffragio universale, definendolo, tra l'altro, personale, libero e segreto. Al fine di rispettare tali principi, si rendono necessari diversi accorgimenti nel meccanismo di raccolta, registrazione e conteggio dei voti, nonché per l'elettore durante l'esercizio dello stesso.

Come si legge nell'articolo di Monica Rosini (Rosini 2020) per la rivista dell'Associazione Italiana Costituzionalisti, che si interroga sulle problematiche connesse all'implementazione del voto elettronico nel contesto costituzionale italiano:

> *"Le maggiori difficoltà riscontrate attengono alla affidabilità e sicurezza del voto, ovvero alla capacità di garantire la corrispondenza tra l'autentica volontà dei cittadini, individualmente e nel loro complesso, e i risultati ufficiali della loro consultazione. Solo sistemi di voto elettronico sicuri, affidabili, efficienti, tecnicamente solidi, aperti a verifiche indipendenti e facilmente accessibili agli*

> *elettori, sono in grado di rafforzare la fiducia del pubblico, che costituisce un prerequisito irrinunciabile per lo svolgimento di elezioni elettroniche"*

Lo stato di necessità o la maggiore diffusione o la presunta praticità del voto elettronico, del resto, non può far venir meno tali requisiti:

> *"Questi "standards di democraticità nella formazione e nell'espressione del suffragio", individuati nei principi di personalità, uguaglianza, libertà e segretezza, "vanno osservati in ogni caso in cui il relativo diritto debba essere esercitato […] anche in caso di elezioni di secondo grado". Se, pertanto, è da escludere che l'adozione di modalità di voto caratterizzate dall'uso di tecnologie informatiche faccia venir meno il carattere universale di tale principio, resta da riflettere sulla possibile configurabilità in tali casi di una loro diversa interpretazione e/o di un diverso bilanciamento tra i medesimi. Non può, infatti, aprioristicamente escludersi che in riferimento all'e-voting i principi di universalità, personalità, uguaglianza, libertà e segretezza del voto possano essere declinati in maniera non coincidente con quella consolidata per il voto cartaceo"*

Assodato ciò, è dunque importante che nell'adozione di un sistema di voto elettronico o ibrido (ossia che preveda la doppia possibilità) si dia modo all'elettorato, in modo trasparente, di comprendere e valutare tale sistema nel suo complesso. Infatti, prima che un processo tecnologico, il sistema di voto è un processo sociale, che richiede la massima fiducia nei meccanismi che lo regolano; si vuole dire che la sua fiducia deve essere tale da convincere il perdente di aver correttamente perso.

Il "Comitato per i Requisiti del Voto in Democrazia", costituitosi nel 2018 con lo scopo di tutelare e innovare i requisiti di voto, compreso anche quello per via elettronica, ha stilato una interessante lista che comprende 70 punti critici da valutare nell'implementazione di un sistema di e-voting (Comitato dei requisiti per il voto in democrazia 2021). Già in premessa a tale lista troviamo una interessante considerazione:

> *"Quando si sta valutando una proposta di sistema elettorale online o basato su blockchain è necessario dare agli elettori gli strumenti per comprendere meglio le sue implicazioni sulla sicurezza. L'espressione semplicistica che un sistema sia sicuro, o che sia stato valutato, eventualmente in segreto e senza alcuna esposizione pubblica di una analisi che risponde alle seguenti domande, dovrebbe essere guardata con sospetto. Ogni sistema, anche il meno open e più proprietario dovrebbe fornire adeguate risposte ad ognuna di queste domande e coloro che dovranno votare in un sistema del genere hanno ogni diritto di ottenere le seguenti informazioni."*

Tale check list è articolata in diverse macro sezioni che affrontano il problema da diversi punti di vista. Tra i vari punti, oltre alla sicurezza stessa del sistema di voto, che deve garantire che il conteggio dei voti rispecchi la reale intenzione degli elettori, merita menzione l'aspetto - rilevato dal Comitato, come sopra esposto - delle "verifiche elettorali", ossia la possibilità di convincere il candidato perdente dell'effettivo risultato anche con un riconteggio o una verifica, nonché gli aspetti della logistica e della distorsione del pubblico.

Si tratta di un aspetto sottile e raramente preso in considerazione. Idealmente la scelta di un **meccanismo di voto non dovrebbe alterare la partecipazione del pubblico alla votazione. Tuttavia, è innegabile che alcune scelte nel meccanismo potrebbero dissuadere o rendere complicata la partecipazione di alcune categorie di elettori. Tali ostacoli non devono necessariamente essere reali, potrebbero essere semplicemente "percepiti", in particolare qualora il sistema stesso sia poco trasparente se non addirittura opaco, oppure troppo complesso per essere compreso dal pubblico. E' il**

caso di un accesso al voto che preveda l'autenticazione degli utenti con meccanismi troppo complicati per certe categorie di elettori.

Si legge perciò al punto 70:

> *70. Al di là dalla loro effettiva esistenza possono essere percepite dal pubblico aree di opacità nel meccanismo elettorale che potrebbero portare ad una disaffezione indotta di intere classi di potenziali elettori?*[1]

Viceversa è chiaro che in molti contesti, in particolare in condizioni emergenziali, l'utilizzo del voto elettronico, magari come alternativa opzionale al voto "di persona", potrebbe genuinamente incentivare l'adesione al voto.

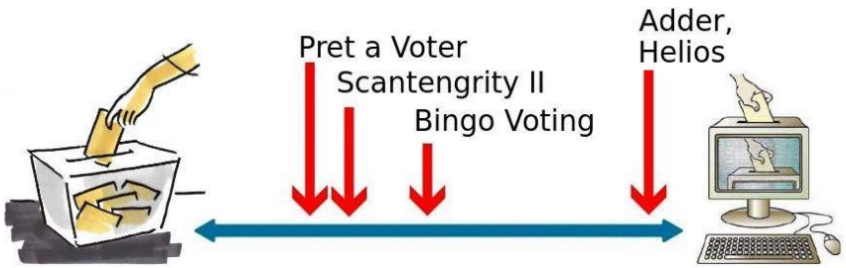
Gli aspetti tecnico-informatici

Come detto il processo di votazione si fonda sulla fiducia. Indipendentemente dalle competenze tecniche dell'elettore i votanti devono potersi fidare che le schede sono conservate in un luogo protetto, non manomissibile e che verranno scrutinate correttamente ed in modo trasparente. In altre parole, il processo di voto deve essere palese.

Ai principi generali del voto, ossia che il voto sia unico, segreto e che vi possa accedere senza discriminazioni solo gli aventi diritto, che la sua espressione sia libera, ossia esente da coercizione o da compravendita, e che l'intero processo sia integro, esente da vizi e manomissioni, si aggiungono le problematiche tecnologiche utili al rispetto di tali principi nonché la necessità, come visto, di consentire una fiducia incondizionata in coloro che progettano, implementano e gestiscono il processo di voto.

Gli attacchi alla fiducia in un sistema elettorale sono ben noti e presenti da sempre. Si consideri solamente il dibattito insensato sull'utilizzo o meno di matite copiative che ha caratterizzato gli ultimi anni: gli elettori vedono un oggetto a loro familiare (una matita) con proprietà tecnologiche avanzate (non cancellabilità) e sulla base delle loro competenze ed esperienze mettono in dubbio l'effettiva funzionalità dello strumento. In un processo di voto telematico, ogni passaggio, anche se trasparente, richiede una comprensione tecnica avanzata di temi architetturali, ingegneristici e matematici (si pensi solamente alle garanzie di integrità basate sulla firma digitale).

In letteratura, e più ingenuamente nei media mainstream, si sono proposti diversi sistemi di votazione, ciascuno dei quali si prefigge di correggere i difetti degli altri. Per citare alcuni nomi per il lettore che volesse approfondire il tema, possiamo citare Prèt-à-voter, Adder, Helios, Scantegrity-II, Bingo Voting. Queste soluzioni adottano approcci diversi in base alla loro vicinanza alla modalità di voto presenziale o a quella completamente telematica.



[1] Ibidem

In generale, comunque ogni sistema di voto elettronico offre dei miglioramenti rispetto al volto tradizionale che dipendono dalla specifica implementazione del sistema di voto stesso. Tra queste, abbiamo soluzioni che offrono garanzie crittografiche su integrità, verificabilità e supervisione del processo. D'altro canto però ogni elemento aggiunto al processo è una potenziale vulnerabilità che potrebbe compromettere l'intero processo.

Dal punto di vista prettamente tecnologico, il processo di votazione può essere attaccato lato elettore (cabina di voto, portale web), lato entità organizzatrice (processo di scrutinio, conservazione, verifica) e sul canale di comunicazione utilizzato per trasferire il voto dall'elettore all'organizzatore (media fisico come usb, cd, o digitale come email o trasmissioni web).

Problematiche lato elettore

Ad oggi, il voto fisico fornisce un'esperienza d'uso per il cittadino che instilla fiducia nel processo elettorale: i seggi elettorali sono protetti e controllati da volontari e forze dell'ordine, le urne sigillate, i controlli su identità ed autorizzazione puntuali. D'altra parte, le elezioni in presenza sono scomode e presentano una sfida logistica per entrambe le parti. Il voto elettronico, in teoria, permetterebbe un turnaround maggiore offrendo la flessibilità e l'efficienza necessarie per snellire il processo di voto.

La conversione dell'azione dell'elettore nella cabina in un dato digitale è un fenomeno la cui verifica assoluta non è affatto banale. Anche ipotizzando di avere accesso al codice sorgente del software asseritamente eseguito sul dispositivo, e di averne fatto un auditing completo ed esaustivo, non c'è modo di garantire che il software in esecuzione e l'hardware su cui viene eseguito siano integri e non compromessi. Senza scomodare vulnerabilità note e sconosciute (zero day) ed attacchi sofisticati di tipo elettronico (fault injection, side-channel) è comunque possibile minare la fiducia dei votanti nel processo elettorale semplicemente instillando il dubbio che questo sia stato compromesso.

L'utilizzo di dispositivi personali come smartphone e tablet, come taluni ingenuamente suggeriscono, non risolverebbe affatto il problema, anzi, imporrebbe all'utente la verifica della sicurezza del proprio dispositivo e di tutte le app in esso installato, compito che quasi certamente l'elettore non sarebbe preparato a svolgere. In aggiunta, il voto da remoto risulterebbe fin troppo facile da ottenere in modo criminale: anche garantendo l'identità dell'elettore attraverso meccanismi di autenticazione forte, infatti, non vengono date garanzie circa l'assenza di altri soggetti con l'elettore, abilitando scenari di coercizione e compravendita di voti. Verrebbe a mancare nuovamente la fiducia da parte del soggetto organizzatore e degli aventi diritto al voto rispetto al processo elettorale.

Problematiche lato entità organizzatrice

Il processo di voto come lo conosciamo oggi è frutto di secoli di perfezionamento, durante i quali praticamente ogni truffa o vulnerabilità concepibile è stata provata (a volte con successo) avendo in comune un aspetto: la compromissione di un gruppo più o meno ristretto di persone con accesso diretto al processo di voto. Se da un lato il processo elettorale in presenza risulta essere lento e macchinoso, dall'altro garantisce che non ci sia mai un solo soggetto con funzioni di protezione e controllo delle votazioni. Questa proprietà è evidente in un seggio elettorale, dove tra volontari e rappresentanti di lista non c'è mai una sola persona a garanzia dell'integrità del processo. Il voto elettronico invece non permette tale protezione, infatti, per natura dei sistemi tecnologici e informatizzati esisterà sempre una figura come quella dell'amministratore di sistema con poteri assoluti e capacità d'operato completa.

Il problema dell'identità dell'elettore e l'associazione tra questa ed il voto risulta essere tecnologicamente impossibile da risolvere, pertanto aprendo la possibilità a ricorsi successivi. Si tratta, infatti, di proprietà diametralmente opposte, non compatibili tra di loro. Se da un lato si preservasse l'anonimato dell'elettore, non sarebbe possibile verificare l'autenticità della scheda votata e che il voto espresso provenga da un soggetto avente diritto. Dall'altro lato, garantendo la provenienza e l'autenticità della scheda, sarebbe possibile risalire all'elettore, per cui violando il principio di segretezza. Tecnologie come i ledger distribuiti (le cosiddette blockchain) vanno ad intaccare solo una minima parte di questo problema, ovvero l'immutabilità dei dati una volta ricevuti e memorizzati. Tuttavia, l'utilizzo di tali tecnologie introduce ulteriori limitazioni circa il livello tecnico necessario per gestire il sistema senza per altro risolvere i problemi legati alla fiducia dell'elettorato nel sistema di voto.

Problematiche canale di comunicazione

L'atto di trasferire il voto dalla cabina elettorale (leggasi dispositivo personale di voto) all'urna (o server di conservazione) è un passaggio chiaro e trasparente nel caso di una votazione in presenza. L'elettore ed il personale del seggio garantiscono che la scheda venga registrata, autenticata e poi successivamente conteggiata. Non vi sono possibilità di intercettare o **manomettere la scheda dal momento della firma al momento dell'inserimento nell'urna. Viceversa, in un processo digitale di trasferimento del voto (sia esso fisico attraverso una periferica o virtuale via rete) il canale è opaco e non di immediata verifica da parte degli interessati**. Se nel voto tradizionale questo meccanismo è pubblico e il suo controllo sono demandati alle forze dell'ordine e agli scrutatori provenienti dalla popolazione civile, nel voto elettronico la verifica è ipso facto riservata ad un ristretto gruppo di super esperti che abbiano accesso a conoscenze e strumenti che al pubblico sono precluse. È un trasferimento di fiducia immenso, che per forza di cose deve essere ponderato attentamente.

Considerazioni conclusive

Alcune di queste problematiche sono presenti anche nel voto tradizionale, ma la fiducia in esso, oltre che dalla trasparenza, è garantita dalla difficoltà di corrompere il sistema in un numero elevato di punti fisicamente vulnerabili, cosa che richiede un'organizzazione enorme: sostituire le urne è sicuramente una possibilità, ma non passa facilmente inosservata. Il dato digitale invece, si può alterare con sforzo minimo e in modo anonimo e discreto. La differenza fondamentale è quindi nella scalabilità della compromissione del processo elettorale: un gruppo molto ristretto di esperti è in grado di violare un sistema digitale e di modificarne i risultati su una scala ad oggi impensabile.

Ad oggi, dunque, il voto fisico fornisce un'esperienza d'uso per il cittadino che instilla fiducia nel processo elettorale: i seggi elettorali sono protetti e controllati da volontari e forze dell'ordine, le urne sigillate, i controlli su identità ed autorizzazione puntuali.

Il voto elettronico viceversa, e a maggior ragione da remoto, è un tema non ancora completamente esaminato e vagliato, sia dal punto di vista tecnico che da quello giuridico, nonostante esso sia in sperimentazione nel nostro paese dal 2006 e il primo esperimento risalga addirittura al 2001 con l'elezione del Rettore dell'Università di Pisa (Tedesco 2001).

Alcuni paesi esteri hanno già sperimentato il voto elettronico. Esso è usato estensivamente soltanto in Estonia e Svizzera, e comunque con contestazioni e iniziative atte a proibire l'uso di mezzi elettronici già in costituzione (Comité d'initiative «pour une démocratie sûre et fiable»

2020). Invece Stati Uniti, Brasile e India ne fanno uso nella modalità offline all'interno di luoghi pubblici e sorvegliati (Rosini 2020).

Per concludere, l'adozione di un sistema di voto sperimentale non può prescindere dalla valutazione dei rischi connessi: la scelta verso l'applicazione di tale tecnologia porterà evidentemente all'assunzione di tali rischi e delle conseguenti contestazioni, che potranno essere sollevate qualora non si sia in grado di garantire il rispetto dei principi fondamentali regolanti la materia.

Bibliografia

Camera dei Deputati. 2022. "Digitalizzazione del procedimento elettorale e sperimentazione del voto elettronico." Documentazione parlamentare. https://temi.camera.it/leg18/temi/voto-elettronico-e-digitalizzazione-del-procedimento-elettorale.html.
Comitato dei requisiti per il voto in democrazia. 2021. "Valutazione dei requisiti del voto elettronico (e del voto con blockchain) in democrazia – CRVD – Centro di documentazione." CRVD. https://blog.crvd.org/valutazione-dei-requisiti-del-voto-elettronico-e-del-voto-con-blockchain-in-democrazia/.
Comité d'initiative « pour une démocratie sûre et fiable ». 2020. "Moratoria sul voto elettronico." Moratoire sur le vote électronique | initiative populaire | Pour une démocratie sûre et digne de confiance. https://moratoire-e-vote.ch/interruption-de-la-recolte-de-signatures-pour-un-moratoire-sur-le-vote-electronique/.
Rosini, Monica. 2020. "Il voto elettronico tra standard europei e principi costituzionali. Prime riflessioni sulle difficoltà di implementazione dell'e-voting nell'ordinamento costituzionale italiano." *Rivista AIC*, 12 22, 2020. https://www.rivistaaic.it/it/rivista/ultimi-contributi-pubblicati/monica-rosini/il-voto-elettronico-tra-standard-europei-e-principi-costituzionali-prime-riflessioni-sulle-difficolta-di-implementazione-dell-e-voting-nell-ordinamento-costituzionale-italiano.
Tedesco, Vincenzo. 2001. "Diritto & Diritti - rivista giuridica on line." *Diritto & Diritti - rivista giuridica on line* (Pisa), 03, 2001. https://www.diritto.it/articoli/dir_tecnologie/tedesco.html.
Zambrano, Armando. 2022. *Elezioni per il rinnovo dei Consigli degli Ordini territoriali degli Ingegneri*. N.p.: Consiglio Nazionale degli Ingegneri. Presentation. https://www.cni.it/images/Presentazione_Zambrano_ADP1.pdf.

Autori

- Ing. Mattia Zago, PhD work@zagomattia.it
- Ing. Stefano Maistri stefanomaistri1990@gmail.com
- Ing. Federico Fuga fuga@studiofuga.com
- Prof. Ing. Claudio Tomazzoli claudio.tomazzoli@uniroma1.it

Biografie

Ing. Mattia Zago ha ottenuto il dottorato in sicurezza informatica nel 2021 presso l'Università di Murcia, in Spagna. Ha studiato applicazioni di intelligenza artificiale per l'identificazione e l'analisi di minacce informatiche in rete. Ad oggi si occupa di soluzioni per l'identità digitale e la protezione dei dati enterprise.

Ing. Stefano Maistri ha ottenuto la laurea magistrale in Ingegneria e Scienze Informatiche presso l'Università degli Studi di Verona con specializzazione in sicurezza informatica. Nella sua tesi di laurea triennale ha analizzato i sistemi di voto elettronici sopracitati e ha proposto e implementato un nuovo sistema di voto elettronico ad uso interno per l'università di Verona. Ad oggi si occupa di vulnerability assessment e penetration testing.

Ing. Federico Fuga ha ottenuto la laurea Magistrale in Ingegneria Elettronica a Padova nel 2000 e si occupa come freelance di progettazione Hardware e Software di sistemi embedded; per passione e per lavoro si occupa di sicurezza informatica e digital forensics; nel tempo libero scrive di informatica per alcune riviste online. E' Coordinatore della commissione ICT dell'Ordine degli Ingegneri di Verona.

Ing. Claudio Tomazzoli ha ottenuto la laurea Magistrale in Ingegneria Elettronica a Padova nel 1997 ed il dottorato in informatica nel 2014 presso l'Università degli Studi di Verona sui temi dell'intelligenza Artificiale. Già ricercatore professore a contratto dal 2015 presso l'Ateneo Scaligero, dal 2020 è ricercatore professore a contratto presso Sapienza Università di Roma. I suoi interessi di ricerca sono l'Intelligenza Artificiale e l'ingegneria del software.