Sul voto via Internet nelle elezioni pubbliche

Dr. Denis Roio
Fondazione Dyne.org
jaromil@dyne.org

Il voto via Internet nelle elezioni pubbliche

Perché rimane insicuro, nonostante vent'anni di sperimentazioni (e l'ennesima "innovazione" annunciata)

Policy advisory - Febbraio 2026

Il dibattito pubblico sulla modernizzazione del voto parte spesso da una constatazione semplice: l'ambizione di digitalizzare i processi democratici è un segno dei tempi, ma richiede una tecnologia che renda il voto via Internet sicuro per elezioni su larga scala. Tuttavia, ad oggi, tale tecnologia non solo non esiste, ma non è nemmeno prevedibile nel prossimo futuro.

Questa non è una posizione ideologica né "conservatrice", ma il punto di approdo di un consenso scientifico consolidato. Recentemente, il 16 gennaio 2026, ben 21 esperti di sicurezza elettorale del Center for Information Technology Policy (CITP) di Princeton hanno ribadito questa impossibilità strutturale. Non si tratta infatti di una semplice opinione "da addetti ai lavori", ma di un rigore metodologico confermato dal report delle National Academies of Sciences, Engineering, and Medicine (NASEM) del 2018. Nel documento Securing the Vote, la raccomandazione 5.11 è esplicita:

> "At the present time, the Internet (or any network connected to the Internet) should not be used for the return of marked ballots."

Tale indicazione chiarisce che il rischio coinvolge ogni forma di trasmissione digitale, inclusi email, fax o linee telefoniche. Per chi prende decisioni il punto chiave è la natura del rischio: il voto via Internet lo sposta da un piano "locale e controllabile" (seggi, carta, catena di custodia) a un piano "remoto e scalabile". In questo scenario, i dispositivi compromessi o le infrastrutture attaccabili rendono le manipolazioni potenzialmente invisibili e impossibili da contestare senza violare la segretezza stessa del voto.

Il modello tecnico del voto remoto rompe garanzie fondamentali come la segretezza effettiva, l'assenza di coercizione e la verificabilità comprensibile: riconoscerlo non significa fermare il progresso, ma proteggerlo.

La mia raccomandazione, dunque, è quella di non adottare il voto via Internet (incluso smartphone e ogni forma di "ballot return" elettronico) nelle elezioni pubbliche. Al contrario, la scelta più avanzata è investire in soluzioni che aumentino l'accessibilità mantenendo un record cartaceo verificabile e procedure di controllo pubblico, come il Remote Accessible Vote-By-Mail (RAVBM) senza ritorno elettronico e gli audit risk-limiting. Solo così l'innovazione serve davvero la democrazia.

1. Il problema non è l'implementazione: è il modello

Nel dibattito pubblico si tende a parlare di "migliorare" il voto online: software più sicuro, crittografia più avanzata, verifiche più sofisticate. Questa impostazione è fuorviante.

Il voto via Internet introduce rischi sistemici non mitigabili perché:
- avviene su dispositivi dell'elettore non controllati dall'autorità elettorale;
- avviene in un ambiente non supervisionato (domestico, lavorativo, familiare);
- concentra l'attacco: un singolo attaccante può colpire moltissimi voti.

1.1 Dispositivi dell'elettore intrinsecamente non fidati

Il voto via Internet presuppone che l'atto di voto avvenga su dispositivi:
- non controllati dall'autorità elettorale;
- potenzialmente compromessi da malware e spyware;
- aggiornati e configurati in modo eterogeneo;
- esposti ad attacchi continui.

In termini tecnici: il client è intrinsecamente non fidato.
Un malware non deve "rompere" la crittografia: gli basta intervenire prima della cifratura (o prima dell'invio), alterando la scelta dell'elettore e mostrando comunque all'utente l'interfaccia attesa.

1.2 Ambiente di voto non supervisionato: segretezza e coercizione

Il seggio elettorale non è solo un luogo fisico: è un dispositivo sociale che garantisce:
- segretezza del voto;
- assenza di coercizione;
- impossibilità di dimostrare a terzi come si è votato.

Il voto remoto elimina queste garanzie. Nessun protocollo crittografico può impedire che un elettore voti sotto pressione (familiare, economica, politica) né può prevenire il voto di scambio a distanza.

Questo è un punto decisivo per i policy makers: anche un sistema "crittograficamente elegante" può fallire democraticamente.

1.3 Centralizzazione e scalabilità dell'attacco

Il voto cartaceo può essere attaccato, ma gli attacchi di massa richiedono logistica, rischio, più persone, e spesso lasciano tracce. Il voto via Internet, invece, consente attacchi scalabili e remoti.

La letteratura (e le raccomandazioni istituzionali) insiste su questo elemento: la possibilita' di sferrare un attacco di ampia scala cambia la natura del rischio e i costi dell'avversario.

2. Evidenze empiriche: cosa è successo quando si è provato

Finiamola qui con gli scenari teorici e diamo uno sguardo aggiornato a cosa accade quando sistemi reali vengono esposti a revisione e attacco.

2.1 Washington D.C. (2010): compromissione rapida

Nel 2010 un sistema di voto online per elettori all'estero nel District of Columbia fu compromesso durante un test pubblico; ricercatori ottennero controllo e dimostrarono la possibilità di alterare voti e risultati. L'episodio è documentato anche in letteratura scientifica.

2.2 Estonia (dal 2005): modello "funziona" non significa "è sicuro"

L'Estonia viene spesso usata come argomento conclusivo ("se lo fanno loro, allora si può"). Ma la ricerca accademica ha evidenziato limiti architetturali e gap procedurali; inoltre, l'assenza di prove pubbliche di attacco non equivale a sicurezza. In sistemi progettati per poter fallire "in silenzio", l'assenza di evidenza non è evidenza di assenza.

Un dettaglio che raramente entra nelle slide di presentazione: il report NASEM 2018 ricorda che nel 2017 l'Estonia ha sospeso l'uso delle proprie smartcard di identità a seguito della scoperta di una vulnerabilità ampia; più di 750.000 ID card risultarono coinvolte. Se l'infrastruttura di identità è anche infrastruttura di voto, una falla di identità diventa immediatamente una falla democratica.

2.3 New South Wales iVote (2015): vulnerabilità e fallimenti operativi

Un sistema di voto online può essere vulnerabile non solo sul piano crittografico ma anche su disponibilità e affidabilità: in NSW iVote sono state documentate vulnerabilità gravi e, in alcune consultazioni, migliaia di elettori non sono riusciti a votare. Questo è un promemoria per chi legifera: l'accessibilita' è parte della sicurezza elettorale.

NASEM 2018 include esplicitamente, tra gli "ostacoli" al voto via Internet, attacchi man-in-the-middle dimostrati contro New South Wales (2015): non solo teoria, ma incidenti con capacità di violare integrità, segretezza e verifica.

2.4 Svizzera SwissPost (2019–): valutazione seria, costosa, e stop

La Svizzera è interessante non perché "ha risolto", ma perché ha mostrato il metodo: analisi indipendenti approfondite, trasparenza del codice, e quando sono emersi difetti rilevanti il

sistema è stato sospeso e sottoposto a ulteriori studi. Le valutazioni serie costano (ordine di grandezza: fino a un milione di franchi per round di esami indipendenti) e comunque non garantiscono un esito positivo.

2.5 Voatz (West Virginia, 2020) e altri casi recenti

Casi di voto via Internet in contesti reali (anche solo per elettori UOCAVA) hanno mostrato criticità sostanziali in analisi indipendenti. Il pattern è ricorrente: sistema annunciato come "sicuro", revisione indipendente, scoperta di vulnerabilità gravi, ridimensionamento o abbandono.

3. End-to-End Verifiable Internet Voting (E2E-VIV): perché "verificabile" non basta

Quando i vendor rispondono alle critiche dicendo "ma è verificabile end-to-end", stanno spostando il discorso. In teoria, l'E2E-VIV può rendere alcune frodi rilevabili. In pratica, restano problemi strutturali che la ricerca discute da decenni:

3.1 Verifica mediata da software

Gli elettori devono usare applicazioni per verificare. Se l'app (o il dispositivo) è compromesso, può mentire. È un paradosso: chiedere al canale insicuro di certificare se stesso.

3.2 Receipt-freeness: senza, la compravendita del voto diventa un servizio

Un requisito classico del voto segreto è che l'elettore non possa dimostrare a terzi come ha votato (receipt-freeness). Se invece può produrre una "prova" convincente, si scala la coercizione e il voto di scambio.

3.3 Human factors: la maggioranza non verificherà

La sicurezza che richiede comportamenti responsabili agli elettori fallisce, statisticamente, su larga scala. Lo stesso Appel ricorda che perfino controlli semplici (come leggere una stampa) vengono trascurati dalla maggioranza. Se la verifica richiede più dispositivi o passaggi non intuitivi, l'adozione reale cala ulteriormente.

3.4 Dispute resolution: la falla politica più che tecnica

Se un elettore "scopre" un problema, come lo prova senza violare la segretezza del voto? Cosa deve fare l'amministrazione? Annullare l'elezione? Fare un rerun? E come distinguere errori reali da campagne coordinate di disinformazione?

Questa è la parte spesso taciuta nelle brochure: senza un protocollo credibile di contestazione e rimedio, la “verifica” rischia di essere solo un’interfaccia rassicurante.

L’importanza della dispute resolution è discussa anche nella letteratura sui sistemi crittografici accessibili: ad esempio Audiotegrity analizza perché i sistemi senza un record cartaceo leggibile dal votante rendono la contestazione praticamente ingestibile.

3.5 Disponibilità e DoS: il voto come servizio essenziale (ma fragile)

Un’elezione non è un e-commerce: se “cade” il giorno del voto, non si recupera con un rimborso. NASEM sottolinea che gli attacchi denial-of-service (DoS) sono una costante dell’Internet moderno e che le mitigazioni offerte sul mercato “usually require full decryption of all transmitted data” e spesso si appoggiano a sistemi condivisi con terze parti. Tradotto: per “proteggere la disponibilità” si rischia di compromettere privacy e confidenzialità lungo la filiera.

3.6 Email e fax: quando il rischio è normalizzato per abitudine

NASEM è insolitamente diretto su pratiche ancora diffuse in alcuni contesti (spesso per UOCAVA): “standard email is an inappropriate medium for distributing strong credentials or transmitting marked ballots.” E ricorda che “Most fax transmissions travel, at least in part, over the Internet”, quindi vanno considerati, di fatto, forme di voto via Internet “con tutti i rischi aggiuntivi”.

3.7 Blockchain: non è una scorciatoia

Il report NASEM dedica spazio anche alle proposte “blockchain voting”: l’immutabilità non aiuta se il voto può essere alterato sul dispositivo prima di essere registrato; inoltre le blockchain non risolvono autorizzazione e segretezza, e possono introdurre nuovi punti d’attacco (attori che possono censurare, ritardare o creare incertezza sullo stato del registro). In sintesi: nel caso specifico del voto via Internet, “blockchain methods do not redress the security issues”.

4. Il caso VoteSecure: “scienza da comunicato stampa”

A fine 2025 la Mobile Voting Foundation e Free & Fair hanno promosso VoteSecure come SDK open source per voto mobile “sicuro e verificabile”. Nel comunicato si è parlato di traguardo tecnologico e implementazioni attese nel 2026.

Il CITP (16 dicembre 2025 e 16 gennaio 2026) risponde con un punto che dovrebbe interessare direttamente chi governa: non basta annunciare un “core crittografico”. Un’elezione pubblica è un sistema socio-tecnico completo: identità, procedure, distribuzione del software, governance, logistica, audit, gestione incidenti, dispute resolution, trasparenza pubblica.

In particolare, l'analisi CITP sostiene che:

- i problemi strutturali del voto via Internet restano (malware sui dispositivi degli elettori, compromissioni server, attacchi scalabili);
- nel paradigma E2E-VIV restano irrisolti receipt-freeness e dispute resolution;
- sono stati evidenziati ulteriori problemi di verificabilità, inclusi "clash attacks" (Teague e Pereira, 13 gennaio 2026) che consentirebbero a un attaccante di far "verificare" voti uguali a più elettori e rubare voti senza essere rilevato.

Per un dirigente pubblico, il messaggio è semplice: quando un venditore dice "è verificabile", la domanda da porre non è "è facile da usare?", ma "è governabile?". E la governabilità richiede che i fallimenti siano rilevabili e rimediabili senza distruggere segretezza, fiducia e legittimità.

5. Perché non si parla di compromessi accettabili

Le elezioni non sono un problema di ottimizzazione tecnologica. Sono un processo di legittimazione democratica.

Per questo:
- la fiducia pubblica è più fragile (e più importante) dell'efficienza;
- l'auditabilità deve essere comprensibile anche a cittadini e osservatori non tecnici;
- un fallimento "silenzioso" è peggiore di un fallimento "visibile", perché può alterare l'esito senza attivare rimedi.

Un'analogia utile è quella bancaria: sulle frodi esistono dispute resolution robuste, tracciabilità e rimedi legali operativi. Nel voto segreto questi strumenti non possono essere trasferiti "per legge" senza rompere la segretezza del voto.

6. Cosa fare: accessibilità e modernizzazione senza voto online

Dire "no" al voto via Internet non significa ignorare accessibilità, diaspora, mobilità, disabilità. Significa scegliere strumenti che mantengano audit e controllo pubblico.

6.1 Usare Internet dove ha senso (e dove il rischio è mitigabile)

La letteratura e le linee guida istituzionali distinguono chiaramente:

- sì a registrazione elettorale, e-pollbooks, richiesta di voto per corrispondenza, tracking;
- no al ritorno elettronico della scheda votata (internet ballot return).

6.2 Remote Accessible Vote-By-Mail (RAVBM) senza ritorno elettronico

RAVBM è un compromesso pragmatico: rendere accessibile la compilazione (anche con assistive tech), ma mantenere un canale di ritorno auditabile (posta/in-person) con record cartaceo.

6.3 Carta e audit risk-limiting (RLA)

Se l'obiettivo è ridurre il rischio di errori o manipolazioni, la combinazione più robusta oggi è:
- schede cartacee (preferibilmente marcate a mano o con record verificabile dal votante);
- conteggio assistito dal computer;
- sistemi di mitigazione del rischio che controllino campioni di schede reali.

Qui NASEM è altrettanto netto: gli audit sugli esiti "dovrebbero includere l'esame manuale di campioni statisticamente appropriati di schede cartacee" e gli Stati dovrebbero operare delle analisi che mitighino i rischi prima della certificazione di un risultato elettorale.

7. Domande a cui chi vende non ama rispondere

1) Qual è il threat model reale (malware su device, server compromise, insider, coercizione, DoS)?
2) Cosa succede se la verifica segnala problemi? Qual è il protocollo di dispute resolution praticabile, con tempi e rimedi?
3) Il sistema è receipt-free? In che modo impedisce compravendita e coercizione a distanza?
4) Che percentuale di elettori deve verificare perché la frode diventi rilevabile? È realistico?
5) Qual è il piano per disponibilità: cosa succede se il sistema va giù il giorno del voto?
6) Come si fa audit indipendente? Qual è il record verificabile (non solo "crittografico", ma governabile)?
7) Quali sono i costi reali di valutazione indipendente, prima e dopo il deployment?

Conclusione

Dopo più di vent'anni di sperimentazioni, la domanda non è più "come rendere sicuro il voto via Internet", ma perché continuare a proporlo nonostante le evidenze contrarie.

La raccomandazione resta netta: non adottare il voto via Internet nelle elezioni pubbliche.
Investire invece in accessibilità, processi verificabili, record cartacei auditabili e audit risk-limiting. La sicurezza elettorale non è un "prodotto": è un equilibrio istituzionale e sociale costruito per resistere anche quando la tecnologia fallisce.

Riferimenti essenziali

- Andrew Appel, “Internet voting is insecure and should not be used in public elections”, CITP Blog (16 gennaio 2026).
- Andrew W. Appel, “Is Internet Voting Trustworthy? The Science and the Policy Battles”, University of New Hampshire Law Review 21(2):523 (2023).
- National Academies of Sciences, Engineering, and Medicine (NASEM), “Securing the Vote: Protecting American Democracy” (2018), DOI 10.17226/25120 (raccomandazioni 5.8 e 5.11).
- Cybersecurity and Infrastructure Security Agency (CISA), “Electronic ballot return is high risk” (2020).
- Jefferson et al., “A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)” (FVAP/DOD, 2004) (minority report del panel di esperti).

Riferimenti tecnici e casi studio (selezione)

- Scott Wolchok et al., “Attacking the Washington, D.C. Internet Voting System”, Financial Cryptography and Data Security (2012).
- Drew Springall et al., “Security Analysis of the Estonian Internet Voting System”, ACM CCS (2014).
- J. Alex Halderman & Vanessa Teague, “The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election”, E-Voting and Identity (2015).
- Michael A. Specter et al., “The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in US Federal Elections”, USENIX Security (2020).
- Thomas Haines et al., “How not to prove your election outcome”, IEEE Symposium on Security and Privacy (2020).
- Andrew W. Appel, Richard DeMillo, Philip B. Stark, “Ballot-Marking Devices Cannot Assure the Will of the Voters” (2019).
- Tyler Kaczmarek et al., “Dispute Resolution in Accessible Voting Systems: The Design and Use of Audiotegrity”, VoteID / LNCS 7985 (2013).
- David Basin et al., “Dispute Resolution in Voting”, arXiv:2005.03749 (2020).
- Josh Benaloh & Dwight Tuinstra, “Receipt-Free Secret-Ballot Elections” (extended abstract, 1994; versioni successive citate in letteratura).
- Vanessa Teague & Olivier Pereira, “Clash attacks on the VoteSecure voting and verification process”, GitHub issue #6 nel repo FreeAndFair/VoteSecure (13 gennaio 2026).