

A seguito dell'audizione in commissione parlamentare di oggi 17/05/2022 di Roberto Baldoni, direttore generale dell'Agenzia per la cybersicurezza nazionale, e delle dichiarazioni in merito dell'on. Brescia, la comunità informatica italiana, rappresentata dalle due associazioni accademiche GRIN e GII e dal Laboratorio Nazionale di Cybersecurity del CINI ribadisce la propria mozione approvata nell'autunno del 2021 che sottolinea i rischi che accompagnano l'uso del voto elettronico per le elezioni politiche e concorda al riguardo con la posizione assunta dal direttore Baldoni.

http://www.grin-informatica.it:8080/opencms/opencms/grin/news/news_0024.html

È importante proseguire la ricerca di soluzioni innovative, ma tutte quelle finora proposte per il voto elettronico non offrono garanzie sul rispetto della volontà dell'elettore, con voto personale ed eguale, libero e segreto, come previsto dalla Costituzione. Non si può correre il rischio di minare la fiducia nel processo elettorale, che è uno dei pilastri fondanti della democrazia: il cittadino deve essere in grado di convincersi della veridicità del risultato delle elezioni e la conoscenza necessaria per i controlli non può essere patrimonio solo di un ristretto gruppo di persone.

Le possibilità di successo di un eventuale attacco informatico dipendono da quanto un attaccante è disponibile a investire e, quindi, da quanto si possa potenzialmente guadagnare dall'attacco. Nel caso di elezioni politiche possono esistere soggetti interessati a investire molto per controllare o destabilizzare una nazione, anche solo interrompendo l'elezione e creando scompiglio. E un attacco che abbia successo può comportare l'elezione di persone sbagliate, o falsare risultati di referendum. Riteniamo quindi che introdurre l'uso di sistemi di voto elettronico nelle elezioni politiche rischi di mettere a repentaglio le basi fondanti della nostra democrazia.

Fabio Gadducci, Università di Pisa, Presidente GRIN, 338 506 6591

Stefano Paraboschi, Università di Bergamo, Presidente GII, 347 431 8855

Paolo Prinetto, Politecnico di Torino, Direttore Laboratorio Nazionale di Cybersecurity del CINI, 335 227529

Allegata la mozione GII GRIN



Gruppo di
Ingegneria Informatica



Gruppo di Informatca

Mozione sul Voto Elettronico

(approvata dalle Assemblee GII del 16 novembre e GRIN del 29 ottobre 2021)

Il 9 luglio 2021 il Ministro dell'Interno, di concerto con il Ministro per l'Innovazione Tecnologia e la Transizione Digitale, ha approvato un decreto per la sperimentazione del voto elettronico in Italia¹, con le relative linee-guida², che punta a valutare modalità di espressione del voto in via digitale per le elezioni politiche ed europee e per i referendum previsti dagli articoli 75 e 138 della Costituzione. Successivamente, l'ambito della sperimentazione è stato esteso alle elezioni regionali e amministrative, con l'obiettivo di consentire la prima sperimentazione già nel 2022. Il decreto prevede che il voto venga espresso mediante una *web application* a cui l'elettore può accedere con qualsiasi dispositivo digitale collegato alla rete internet. Lo scopo dichiarato è quello di agevolare la possibilità di voto degli italiani all'estero e degli elettori fuori sede per motivi di lavoro, studio o cure mediche.

La comunità informatica italiana considera suo dovere sottolineare i rischi che accompagnano l'uso del voto elettronico nelle elezioni politiche. Pur ribadendo la necessità della ricerca su sistemi elettorali sicuri, riteniamo doveroso – sulla base degli innumerevoli risultati scientifici raccolti in questi anni³ – sottolineare i rischi di voto di scambio, di attacco e manipolazione (a fronte di un incerto aumento della partecipazione elettorale, allo stato attuale delle ricerche ancora non dimostrato), ma anche i rischi connessi a un modello elettorale in cui il cittadino non è grado di convincersi della veridicità del risultato delle elezioni e la conoscenza necessaria per i controlli è patrimonio solo di un ristretto gruppo di persone.

Il voto è soprattutto un esercizio sociale, prima che un fatto tecnico e tecnologico, al termine del quale è assolutamente fondamentale, per la tenuta della democrazia, che tutti gli interessati, soprattutto quelli sconfitti, accettino razionalmente il risultato finale come affidabile e veritiero. Un'elezione con un meccanismo tecnologico di voto che milioni di cittadini non sono in grado di comprendere e ritenere regolare, aprirebbe sicuramente la strada a contestazioni e minerebbe irrimediabilmente quella fiducia nel processo elettorale che è uno dei pilastri fondanti della democrazia. Queste considerazioni sono proprio quelle alla base della decisione della Corte Costituzionale tedesca di sancire la non costituzionalità in Germania del voto elettronico⁴.

Per quanto riguarda gli aspetti tecnologici la nostra valutazione, coerentemente con quanto già espresso dalla comunità internazionale, può essere sintetizzata come segue⁵:

- tutti i sistemi e le tecnologie per la votazione su Internet sono al momento attuale inerentemente insicuri;
- non esiste alcuna evidenza tecnica che una qualunque tecnologia di votazione su Internet sia

¹ https://www.interno.gov.it/sites/default/files/2021-07/decreto_ministro_su_sperimentazione_voto_elettronico_9.7.2021.pdf

² https://www.interno.gov.it/sites/default/files/2021-07/linee_guida_voto_elettronico_decreto_9.7.2021.pdf

³ Un compendio dei problemi relativi all'uso delle tecnologie digitali in ambito elettorale si trova qua:
<http://www.csl.sri.com/neumann/risks-voting.pdf>

⁴ <https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2009/bvg09-019.html>

⁵ <https://www.aaas.org/programs/epi-center/internet-voting-letter>



Gruppo di
Ingegneria Informatica



Gruppo di Informatica

sicura o possa essere resa tale in un prevedibile futuro, mentre al contrario tutta la ricerca attualmente esistente dimostra il contrario;

- l'eventuale ricorso a tecnologie basate su certificazione distribuita (ad esempio *blockchain*) non riduce gli elevati rischi di compromissione della votazione su Internet;
- nessuna *app* per la votazione con dispositivo mobile è sufficientemente sicura da permetterne l'uso;
- a prescindere dal tipo di tecnologia utilizzata, il voto da remoto non può soddisfare contemporaneamente il requisito di essere personale e di essere libero e segreto, rendendo impossibile soddisfare i vincoli costituzionalmente previsti a tutela del voto democratico.

A oggi non esistono sistemi informatici completamente sicuri e le possibilità di successo di un attacco dipendono da quanto un attaccante è disponibile a investire e, quindi, da quanto si possa potenzialmente guadagnare dall'attacco. Ebbene, nel caso di elezioni politiche possono essere molti i soggetti interessati a investire molto per governare, controllare o destabilizzare una nazione. Un singolo individuo o un'agenzia di *intelligence* possono attaccare a distanza un'elezione online, modificando o filtrando le schede elettorali in modi non rilevabili e non correggibili o anche solo interrompendo l'elezione e creando scompiglio. E un attacco che abbia successo può comportare l'elezione di persone sbagliate, o falsare risultati di referendum. **Riteniamo quindi che introdurre l'uso di sistemi di voto elettronico nelle elezioni politiche rischi di mettere a repentaglio le basi fondanti della nostra democrazia.**