Document de politică
Votarea online: Provocări și Soluții

Introducere

Tehnologiile digitale oferă publicului posibilități multiple de acces și e-conectare instantanee. Deși acest lucru vine cu un preț. Conectarea la internet și la portalurile de e-participare face ca aceste tehnologii să devină vulnerabile în fața corupției interne și la hacking-urile externe. În același timp, mass-media online face opinia publică mai sensibilă spre manipulare. Aceste aspecte sunt relevante în special pentru votul electronic ca metodă principală de luare a deciziilor în cadrul politicii de internet, guvernanță electronică și democrație digitală. Totuși, datorită unui set de soluții constructive din domeniul legislativului, a procedurilor și conștientizării, riscurile votului electronic pot fi atenuate.

Așadar, obiectivul acestei lucrări este de a identifica, structura și aborda riscurile votului electronic, oferind soluții practice pentru combaterea acestora. În contextul unei reforme electorale mai largi, după efectuarea analizei cost-beneficiu și dacă a fost adoptată introducerea votului electronic, acest document de politică poate ajuta la prevenirea unor provocări presupuse și respingerea ulterioară a obiecțiilor neîntemeiate. Spre deosebire de majoritatea publicațiilor care se concentrează pe riscuri particulare sau descriu procedura de vot electronic, această lucrare inspectează mai multe provocări și le abordează. Lucrarea poate servi drept referință pentru politicieni, funcționari publici, activiști civici și cetățeni, în general, pentru prevenirea, identificarea și atenuarea abuzului în cazul votului electronic, protejând democrația electronice împotriva denaturărilor și consolidarea bunei guvernări.

În sensul acestei cercetări, vor fi considerate toate varietățile de vot electronic (e-voting), cum ar fi votarea prin intermediul unui aparat de vot electronic în interiorul secției de votare sau votarea electronică la distanță folosind o „cabină” în afara unei secții de votare, iar, în mod special, va fi considerat votul pe internet la distanță. În acest sens, votul pe internet (i-voting) este definit ca „votarea folosind internetul și tehnologiile computerizate cel puțin pentru votarea propriu-zisă și numărarea voturilor”. Așadar, votul electronic pe internet este sinonim cu votul online și votul mobil.

Fiind un instrument universal de e-participare, i-votingul este privit în raport cu un spectru de formate de democrație electronică, incluzând, dar fără a se limita la: sondaje de opinie online care nu sunt obligatorii, votul electronic obligatoriu pentru politici nationale, plebiscite și referendumuri online, și alegeri electronice pe internet (alegeri online). Prin urmare, votul electronic poate servi tuturor formelor de democrație reprezentativă, directe și de altă natură.

Acest studiu se bazează pe o analiză documentară a cercetărilor academice și de politici existente și pe analiza datelor secundare disponibile privind statisticile legate de e-voting. Concluziile sunt făcute în baza cazurilor naționale și locale și, prin urmare, pot fi aplicate pentru o varietate de modele de voturi electronice la distanță în contexte politice diverse.

Lucrarea prezintă secvența temporală a provocărilor majore ale votului electronic, oferă soluții recomandate, analizează detaliat fiecare problemă specifică pentru votarea electronică și încheie cu reflecții finale. De asemenea, include o imagine de ansamblu succintă a cazurilor de alegeri electronice practicate și abandonate, luate în considerare și abandonate, practicate in prezent și considerate pentru viitor.

Autor: Dmytro Khutkyy, Consilier privind politicile de democratie digitala, Alianța Europeană de Dezvoltare Digitală.

Recenzenți: Daniel Innerarity, Profesor, School of Transnational Governance, European University Institute, Italia; Robert Krimmer, Profesor de E-Guvernare, TalTech Tallinn University of Technology, Estonia.

Recunoaștere: Această lucrare a fost pregătită in cadrul bursei de studiu „Policy Leader Fellowship” din partea Școlii de School of Transnational Governance, European University Institute.

Disclaimer: *Poziția și opinia exprimate sunt cele ale autorului și nu reprezintă neapărat poziția și opinia Institutului Universitar European (EUI) sau a Școlii de Guvernare Transnațională (STG).*

Traducător: Stela Cudalb, Expert independent, EU Del Moldova.

Editor: European Digital Development Alliance, Bruxelles, Belgia, August 2020.

Puncte pricipale

	Riscuri	Soluții
1.	**Încadrarea problemei:** Manipularea buletinului de vot în cadrul votului electronic într-un sondaj de opinie , plebiscit, referendum sau alegeri; de asemenea - sistematizarea unei probleme de vot în publicațiile mass-media	**Formulare echilibrată:** asigurată printr-o revizuire a unei comisii, publicare anticipată, discuții și corectarea buletinului de vot; acces gratuit la Internet
2.	**Polarizarea părtinitoare:** efectul de preselecție și prejudecăți confirmate duc spre divizarea grupului, creează bule de filtru și o realitate socială distorsionată	**Conexiune deliberativă:** Facilitarea unui aranjament care să susțină diversitatea punctelor de vedere, o percepție critică a informației și discuții inteligente
3.	**Manipularea opiniei publice:** folosirea volumelor mari de date („big data"), roboți și scriitori plătiți pentru micro-direcționarea opacă a alegătorilor în mod individual prin mesaje personalizate	**Reglementarea mass-mediei online:** Aplicarea legislativă sistematică, și acțiunea civică pentru a impune limite, a asigura transparențași implementarea masurilor
4.	**Funcționarea defectuoasă a sistemului tehnic:** Probleme tehnice ale echipamentelor sau programelor sistemului de vot, precum și erori umane în utilizarea acestora	**Funcționarea viabilă a sistemului:** efectuarea testelor de sistem, instruirea personalului care administrează sistemul de votl electronic, planificarea măsurilor de urgență tehnică și organizațională
5.	**Hacking-ul rău intenționat:** preocupările privind securitatea cibernetică legate de hacking-ul unui sistem de vot electronic de către agenți guverna-mentali sau neguvernamentali din țară sau din afară	**Securitate și integritate cibernetică:** evaluare și certificare a sistemului, strategie de securitate cibernetică, test de sistem, concurs de identificare a erorilor, instruire a personalului și campanie de educație
6.	**Excluderea:** îngrijorări cu privire la eligibilitatea legală a anumitor grupuri și problemele de accesibilitate impuse de decalajul digital	**Incluziune:** garantarea dreptului de vot pentru toți cetățenii eligibili, adăugarea votului electronic ca o opțiune suplimentară la votul offline tradițional
7.	**Incorectitudinea registrelor de alegători:** Registrele de alegători corupte pot fi utilizate greșit pentru a împiedica anumite persoane să voteze și pentru aexploata registrefalse pentru votul corupt/controlat	**Exactitatea registrelor de alegători:** Măsuri tehnice și organizatorice standard combinate cu tehnologii de evidență distribuite, cum ar fi de exemplu blockchain-ul
8.	**Identificare greșită:** riscul ca unii alegători eligibili să nu aibă voie să voteze în timp ce unii alegători falși vor vota fără să aibă dreptul de a face acest lucru	**Autenticitatea identificării:** Introduceți mai multe etape de identificare fiabilecare, combinate, vor minimiza riscurile de identificare greșită
9.	**Dezvăluirea, presiunea și cumpărarea votului:** provocările divulgării voluntare sau forțate a votului, presiunea grupului, constrângerea votului și cumpărarea voturilor	**Secretizarea votului, libertatea și integritatea:** mecanisme tehnice și organizatorice, schimbari ale votului, campanii de sensibilizare, raportare și aplicare a masurilor in vigoare
10.	**Votul de rutină și absentismul:** valoarea scăzută a actului de votare care duce la o campanie de vot mai puțin masivă, unificată	**Votarea deliberativă bazată pe valori:** Tehnologiile digitale facilitează acțiunea civică și obișnuințele noi; educarea civică și sensibilizarea motivează persoanele să voteze mai activ
11.	**Numărarea si stocarea coruptă a voturilor:** rezultatele votului electronic pot fi denaturate la etapele înregistrării, stocării și numărării voturilor	**Control și responsabilitate:** controlul minuțios, tehnologii de evidențădistribuite, sistem tip „*Prêt à Voter*", tragerea la răspundere juridică, audite și responsabilizare
12.	**Discreditarea campaniei de vot:** votul manipulat poate reduce încrederea față de instituțiile democratice și poate dăuna legitimității rezultatelor votului	**Legitimitate și încredere:** dezbateri și discuții pre-campanie electorală conduse de experți despre proiectarea votului electronic combinate cu comunicarea bazată pe transparență pentru public

1. Cadrul problemei *versus* formularea balansată

Deja în primele etape de pregătire a votului electronic, formularea subiectului în sine poate fi problematică. În principal, aceasta se referă la sondaje de opinie, sondaje neobligatorii și la plebiscite sau referendumuri obligatorii, dar se poate referi și la alegeri. Regulamentele Consiliului Europei cu privire la votul electronic afirmă clar: „Toate informațiile oficiale de vot sunt prezentate în mod egal, în cadrul și pe toate canalele posibile de vot ... Buletinul de vot electronic utilizat pentru votarea electronică nu trebuie să conțină informații despre opțiunile de vot, altele decât cele cerute de lege ... Dacă informația despre opțiunile de vot sunt accesibile de pe pagina votului electronic, acestea trebuie să fie prezentate în mod echitabil."[1]

În cel mai rău caz, un scrutin corupt pentru alegerile electronice ar (i) încalca ordinea (aleatorie) definită prin lege prin poziționarea candidatului preferat pentru o funcție publică sau un partid în topul listei sau (ii) poziționarea adversarilor în comparație cu candidatul preferat în partea de jos a listei, (iii) acoperirea adversarilor printre candidații „tehnici" asemănătorisau chiar (iv) ar include publicitate verbală sau vizuală în favoarea unui candidat preferat. Acest lucru poate fi prevenit prin previzualizarea buletinului de vot de către o comisie echilibrat formată din diverși reprezentanți - fie printr-o selecție aleatorie a cetățenilor (aplicarea proiectului de democrație aleatorie prin tragere la sorți) sau dintr-un grup divers de organizații ale societății civile și de partide politice. Un mecanism suplimentar de prevenire este publicarea în avans a buletinului de vot, care permite suficient timp pentru a corecta eventualele discrepanțe.

Un buletin de vot manipulat pentru votarea electronică într-un sondaj de opinie, plebiscit sau referendum ar putea (i) să conțină o întrebare ambivalentă sau cu dublu înțeles care să confunde sau să inducă în eroare un alegător sau (ii) să presupună o secvență de întrebări cu o opinie implicită sau o anumită emoție – direcționând astfel alegerea unui votant spre o opțiune dorită. Acest lucru poate fi atenuat printr-o publicare în avans, discuții/dezbateri și corectarea buletinului de vot. În concluzie, transparența publică și mecanismele de supraveghere civică pot preveni abuzul de vot electronic în primele etape ale aprobării buletinului de vot.

O manipulare mai subtilă poate fi realizată prin includerea unei probleme de vot în discursul mass-media. Acest lucru este deosebit de periculos atunci când majoritatea surselor mass-media populare din țară sau o comunitate sunt dominate de o singură persoană sau un grup de persoane influente. În acest caz, accesul gratuit la Internet este o soluție, deoarece internetul poate oferi acces la media online, având costuri mai reduse în crearea conținutului divers.

2. Polarizare părtinitoare *versus* conexiune deliberativă

Domeniul opiniei publice este populat de numeroase provocări: existența „bulelor de filtrare", efectul de preselecție, tendința de a interpreta noi dovezi ca o confirmare a convingerilor existente, polarizarea grupului, știri false și realitatea socială denaturată. Provocarea inițială este aceea că „lumea social media tinde să creeze mici grupuri puternic polarizate de indivizi care vor tinde să creadă tot ceea ce aud, indiferent cât de distanțat de realitate este subiectul".[2] Oamenii care trăiesc în interiorul unei bule de filtru nu primesc știri care contestă părerile rigide ale lor și ale grupurilor sociale din care fac parte. Mai mult, persoanele afectate de prejudecăți caută numai informațiile cu care sunt de acord,nu informatii verificate independent. Știrile false exploatează preselecția și prejudecata ca trăsături caracteristice ale bulelor de filtru care tind să polarizeze grupurile sociale.[3] Deoarece oamenii au prejudecăți cognitive inerente și tind să se unească în grupuri sociale cu credințe/obiceiuri comune, aceste fenomene fac parte din politica tradițională și, prin urmare, nu reprezintă o problemă în sine. Cu toate acestea, atunci când aceste procese sunt amplificate în spațiile online, acest lucru devine într-adevăr problematic.

[1] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[2] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.
[3] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

În astfel de circumstanțe, soluția principală este intenția de a facilita un mediu caresă susțină diversitatea de opinii, abordarea critică a informațiilor prezentate și discuții inteligente. În primul rând, este relevant să alimentăm proactivitatea individuală în căutarea informațiilor alternative, evaluarea critică a sursei și conținutului informațiilor, crearea obiceiului de a forma o opinie personală independentă bazată pe surse multiple și reflecție critică. În al doilea rând, este rezonabil să încurajăm și să susținem cultura de a avea opinii contracdictorii. Savanții sugerează o serie de corecții posibile pentru forumuri și chat-uri online, pagini web și bloguri: moderare, decizii editoriale, control public, semnarea unui acord de utilizator care recunoaște normele de discuție și ghiduri pentru depolizare cu sancțiunea de a fi eliminat în cazul încălcării normelor,[4] a discursului cooperant și nepolarizat. Pentru identificarea abaterilor potențiale, ei propun să aplice un program/sistem de cartografierecognitivă, care analizează automat textul pentru a arăta direcția dezbaterii.

Astfel de intervenții se bazează pe presupunerea că normele și practicile orientate spre dezbateri sunt capabile să inverseze tendințele de polarizare și să promoveze formarea opiniei informate, o dezbatere profundă și mai multe rețelede consens. În acest scop, posibilele măsuri de depolarizare includ: (1) crearea unui spațiu sigur pentru diluarea identității și formarea identității superordonate; (2) promovarea interacțiunilor și structurilor sociale offline cu reguli de de-polarizare care scad polarizarea online; (3) introducerea unui cadru de cooperare și negociere pentru a reduce limbajul negativ și a crește limbajul conciliator; (4) crearea de legături și conectarea persoanele care împărtășesc aceleași griji i, dar care caută pace și nu violență, creând și menținând norme de depolarizare[5]. Prin urmare, structura normativă a unui spațiu de discuții online va orienta spre exprimarea unor opinii diferite, implicareaîn dispute inteligente și stabilirea de conexiuni multiple cu interlocutorul, constituind astfel un lanț mai complex și mai interconectat de indivizi cu puncte de vedere similare.

3. Manipularea opiniei publice *versus* reglementările media online

Dincolo de dezechilibrele emergente la etapa formării, opinia publică poate fi distorsionată în mod deliberat de mass-media online. Informațiile numeroase privind profilurile utilizatorilor oferă suficiente date pentru vizarea precisă a alegătorilor individuali cu mesaje personalizate și astfel influențând comportamentul lor într-un mod în care nu este posibil de către mass-media convenționale. De exemplu, o analiză automată a aprecierilor pe Facebook ale oamenilor a fost în măsură să identifice informațiile lor demografice și convingerile politice de bază și a fost folosită pentru a viza votanțispecifici în Statele Unite.[6]

În timp ce publicitatea tradițională a mass-media este o practică standard a campaniilor politice, micro-targetarea este echivocă din punctul de vedere al integrității. Cantitatea de informații utilizate pentru a viza o persoană depășește ceea ce este utilizat în mass-media tradițională, iar cititorii sau telespectatorii nu sunt întotdeauna conștienți de ceea ce se dezvăluie despre ei înșiși. De asemenea, mesajele despre un anumit politician adaptat alegătorilor individuali pot fi inconsistente sau chiar contradictorii între ele, punând astfel în discuție o platformă politică unificată. În timp ce mesajele tradiționale de masă pot fi văzute, verificate și puse la îndoială de către alți spectatori, anunțurile micro-targetate sunt dificil de monitorizat și de contrastat. Mai mult, opacitatea algoritmică a casetei negre a newsfeed-ului, a algoritmului de căutare și a segmentării anunțurilor împiedică supraveghetorii sau autoritățile de reglementare să înțeleagă care publicități sunt afișate cui și când, cine a plătit pentru ele, cât și când[7]. În plus, un mesaj poate fi consolidat în rețelele de socializare, fie prin numeroase postări ale unor roboți (semi) automatdin conturi false sau prin postări extrem de vizibile plătite în secret. Deși unii autori ar putea susține sincer un candidat, problema apare atunci când o astfel de activitate este coordonată sau finanțatăpe ascuns. Acest lucru

[4] van Dijk, J.A.G.M., Hacker, K.L, & Mollov, B. 2018. Digital Media and Networking: Opportunities and Constraints for Depolarizing Political Discourse. In: van Dijk, J.A.G.M., Hacker, K.L. *Internet and Democracy in the Network Society*. Pp. 108-130. New York: Routledge.

[5] van Dijk, J.A.G.M., Hacker, K.L, & Mollov, B. 2018. Digital Media and Networking: Opportunities and Constraints for Depolarizing Political Discourse. In: van Dijk, J.A.G.M., Hacker, K.L. *Internet and Democracy in the Network Society*. Pp. 108-130. New York: Routledge.

[6] Hull, G. 2019. Social Media Is Not Good for Democracy. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 100-104. New York: Greenhaven Publishing.

[7] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.

creează o iluzie de sprijinire autentică independentă al unui politician sau al unui partid, în timp ce, de fapt, nu este așa.

Aceste provocări necesită drept răspuns o acțiune legislativă sistematică, de aplicare și de acțiune civică. Guvernul poate impune limite, asigura dezvăluirea și poate efectua aplicarea respectării problemei: cumpărătorii, cum ar fi partidele politice și furnizorii precum Facebook, ar trebui să fie obligați să dezvăluie în mod proactiv informații complete despre un anunț politic într-un format online, care să poată fi citit online de public și autoritățile de reglementare electorală[8]. Sprijinul politic sponsorizat ar trebui să fie declarat în mod explicit de către scriitori, monitorizat de către furnizorii de platforme de socializare și pedepsit în cazurile în care sunt depistate mesaje politice ascunse. De exemplu, Facebook identifică și șterge deja conturile care afișează semne de comportament neautentic coordonat. Mai mult decât atât, activitatea guvernamentală ar trebui să fie însoțită de activismul acționarilor, acoperirea mass-media, documente de politici pe această temă și presiune publică.[9]

4. Funcționarea defectuoasă a sistemului tehnic *versus* funcționarea fiabilă a sistemului

Preocuparea uzuală legată de votarea prin mijloace digitale se referă la posibile probleme tehnice de funcționare a sistemului de vot, indiferent de caracterul tehnic sau de sistem. Este posibil să fie un cod incorect care să conducă la erori la votarea sau la numărarea voturilor, la o suprasarcină a sistemului sau la o blocare a echipamentelor. În cel mai rău caz, „mici greșeli în implementarea și configurarea aplicațiilor web pot duce la un compromis total”[10]. Într-adevăr, un astfel de risc există deoarece sistemele de vot digital sunt centralizate. Cu toate acestea, poate fi atenuat prin efectuarea de teste cu sarcină maximă de muncă și împotriva riscurilor multiple.

O altă problemă conexă poate fi atribuită factorului uman. Întrucât „Administratorii slab instruiți pot crea din greșeală erori care erodează rapid încrederea publicului.”[11] Trebuie menționat că această provocare nu este atribuită în mod special votului electronic, ci poate apărea în timpul oricărei campanii de vot. Pentru a preveni erorile în interacțiunea om-computer în timpul votării electronice, autoritatea electorală trebuie să aibă încredere și să înțeleagă tehnologia votării, care este asigurată prin procese riguroase de evaluare și strategii de instruire eficiente.[12]. Autorii recomandă, de asemenea, ca furnizorii de servicii externi, atât cei privați, cât și cei publici, să respecte legile și cerințele, aceasta fiind asigurată de evaluarea riscurilor asociațiilor și dependențelor potențiale ale furnizorilor de servicii externe.

Mai mult, regulamentele Consiliului Europei cu privire la votarea electronică sunt extrem de relevante în acest sens. În special, acestea subliniază măsuri tehnice și organizatorice pentru păstrarea datelor chiar și în cazul unei defalcări, verificări periodice a funcționării sistemului și a disponibilității pentru utilizatori, stocarea echipamentelor de votare electronică într-o zonă sigură, dispunerea de aranjamente de rezervă, un plan de recuperare a dezastrelor și o procedură de urgență, procedura de instalare a actualizărilor și corecțiilor în sistem și de manipulare a materialului criptografic în siguranță. [13]

5. Hacking-ul rău intenționat *versus* securitatea și integritatea cibernetică

Probabil cel mai adesea, preocupările legate de votul electronic sunt asociate cu riscuri de securitate cibernetică. Amenințările de hacking pot apărea în societatea în care se desfășoară votarea electronică, în cadrul autorităților care

[8] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.
[9] Howard, A., & Wonderlich, J. 2019. Social Media Sites Should Have to Disclose Political Advertising Files. In: Heitkamp, K.L. (ed.). *Interference in Elections*. Pp. 105-112. New York: Greenhaven Publishing.
[10] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.
[11] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[12] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[13] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

administrează votul electronic și provin din partea criminalilor cibernetici din altă țară sau dintr-un guvern străin ostil. În ceea ce privește atacurile din interiorul societății, trebuie remarcat faptul că votul offline la distanță are riscuri similare - de exemplu, votarea prin poștă, numărarea de voturi etc. Datorită utilizării serverelor accesibile pe internet care permit votarea online, votul electronic pe internet este într-adevăr mai expus la atacuri străine, fie ele private sau orchestrate de stat. Astfel, „guvernele care doresc să investească un nivel ridicat de resurse în atacarea oricărei platforme Internet ar putea direcționaaceste resurse către votarea pe Internet, cu scopul de a schimba efectiv rezultatul unei alegeri sau de a submina încrederea publicului în rezultatul alegerilor."[14] Similar cu combaterea coruperii votului offline la distanță, soluția de atenuare a riscurilor de securitate cibernetică a votului online este dezvoltarea unor mecanisme de securitate mai bune. Înainte de lansarea votului electronic, sistemul tehnic ar trebui să fie supus evaluării și certificării. Consiliul Europei recomandă „un organism independent și competent să evalueze conformitatea sistemului de votare electronică și a oricărei componente privind tehnologia informației și comunicațiilor (TIC) cu cerințele tehnice", sub formă de certificare oficială sau un alt control adecvat .[15]

Există mai multe moduri în care un sistem de vot electronic poate fi corupt. De exemplu, „oricine poate încerca să modifice (cod rău intenționat) sau funcționarii pot permite, din neatenție, altora să modifice procesul de votare (atacuri de viruși) ."[16] Într-un studiu de caz, „cercetătorii au arătat că un atacator intermediar ar putea exploata vulnerabilitățile din sistemul votului electronic australian pentru a injecta un cod de furt de vot ... inclusiv compromiterea punctelor de acces Wi-Fi nesigure, otrăvirea cache-urilor DNS ISP, atacarea routerelor vulnerabile și deturnarea prefixelor BGP. " [17] De asemenea, au raportat că comisia electorală a modificat a doua zi configurația serverului de vot electronic . Într-un alt exemplu „în timpul proceselor electorale la Washington DC, echipa de testare a efectuat o serie de atacuri și a demonstrat că infractorii ar putea fura secrete, schimba voturile din trecut, schimbă voturile viitoare, compromite scrutinul secret, introduce un efect de furt amânat." [18] Se pare că aceste vulnerabilități sunt ușor de remediat, privind în retrospectivă. Prin urmare, unele probleme de sistem sunt tehnice și pot fi reparate. În acest scop, hackerii etici de „bună credință" (care identifică punctele slabe de securitate și urmăresc să le remedieze și să prevină să fie abuzate de răufăcători) pot fi angajați (într-o operațiune de recompensare de tip „bug bounty") pentru a provoca sistemul, a identifica vulnerabilitățile sale și a ajuta la îmbunătățirea securitatea sa cibernetică.

La nivelul construcției de sistem, pot fi introduse mai multe soluții. În acest sens, Institutul Național de Standarde și Tehnologie (NIST) Cadrul de securitate cibernetică oferă mai multe recomandări pentru atenuarea riscurilor de hacking: realizarea modelării minuțioase a amenințărilor, elaborarea unui plan de gestionare a riscurilor și a unei strategii de securitate cibernetică, utilizarea protecțiilor criptografice (pentru transfer de date și date în repaus) , avansarea tehnicilor de vot criptografic, utilizarea hardware-lui dedicat și de încredere (cum ar fi o carte de identitate electronică), folosirea scanării de securitate a punctului final (pentru a verifica dacă o piesă de software de votare electronică nu a fost modificată), mediul de bootare pre-configurat sau tehnologie de virtualizare (pentru a contracara software-ul rău intenționat) și canale de comunicare secundare (cum ar fi codul QR estonian care permite alegătorilor să își verifice votul cu un dispozitiv alternativ) [19]. Un bun model de securitate cibernetică este sistemul de vot electronic eston care folosește o carte de identitate protejată și posibilitatea de a verifica propriul vot. Potrivit informațiilor, „nu există dovezi că votul pe internet din Estonia a fost compromis." [20] De asemenea, un sistem de vot

[14] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[15] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[16] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[17] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.
[18] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.
[19] The National Institute of Standards and Technology. 2011. *The Security Considerations for Remote Electronic UOCAVA Voting*.
[20] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

electronic coordonat, dar descentralizat, este o soluție bună pentru controlul daunelor în caz de defecțiune parțială sau atac. [21]

În mod alternativ, un atacator poate decoda și publica informații sensibile, cum ar fi datele alegătorilor, punând comisia electorală în dilema anulării unei alegeri sau anunțarea ei valabilă, dar confruntându-se cu dezvăluirea online a datelor sensibile. Cu toate acestea, chiar și acest risc poate fi atenuat. În special: (1) rezultatul poate fi raportat pentru subgrupurile de alegători, astfel încât numărul de voturi pentru fiecare candidat să fie suficient de mare pentru a ascunde informațiile codate în zgomotul statistic furnizat de voturile alegătorilor cinstiți; (2) statisticile privind voturile nevalide ar trebui să fie reduse la minimum și raportate sub formă agregată și nu pentru fiecare district de vot sau alte regiuni mici; (3) statisticile și informațiile detaliate ar trebui considerate secrete. [22]

Pe lângă vulnerabilitățile tehnice, există erori umane care pot compromite sistemul de votare electronică pe internet. În primul rând, administratorii de sistem care au acces la servere și la software-ul de vot pot contribui intenționat sau accidental la un atac prin utilizarea unităților flash USB infectate sau prin reducerea protecției sistemelor. [23] Pentru a preveni astfel de incidente, se recomandă o pregătire riguroasă a personalului electoral.

Chiar dacă securitatea cibernetică maximă este asigurată la nivelul sistemului central de vot electronic, rămâne provocarea securității cibernetice a dispozitivelor personale utilizate pentru votarea electronică. Se estimează că „multe computere personale sau dispozitive mobile folosite pentru a vota online sunt slab securizate.” [24] Tehnic vorbind, atacatorii ar putea lansa atacuri de blocare a serviciului menite să perturbe alegerile, să încerce să redirecționeze alegătorii către pagini false de vot și să efectueze atacuri pe scară largă asupra aparatelor alegătorilor, probabil folosind infecții *botnet* preexistente. [25] Iar aceste amenințări sunt considerate una dintre cele mai dificile și cel mai puțin rezolvate probleme în securitatea Internetului. Cu toate acestea, o testare completă a sistemului cu sarcină maximă și atacuri cibernetice diverse poate atenua aceste riscuri.

Alternativ, un atacator poate aplica virusul Bayesian invers pentru a denatura software-ul alegătorilor. Acest lucru poate fi efectuat printr-un atac de blocare a serviciului asupra filtrelor de spam al unui alegător - antrenând în mod secret filtrul de spam al alegătorului, trimițând mesaje de spam create pentru a include cuvinte cheie de la e-mailuri autentice din sistemul de vot și, în acest fel, suprimândastfel în mod discret mailurile din sistemul de votare.[26] Cu toate acestea, autorii sugerează că utilizatorii pot atenua efectele inversate ale virusului Bayesien, punând pe o listă „albă” adresa de e-mail pentru alegeri și astfel împiedicând suprimarea e-mailurilor, în timp ce oficialii electorali pot atenua acest atac folosind canale alternative (de ex. Mesaje SMS) pentru a notifica utilizatorii cărora le-au fost trimise mailurile cu informațiile de autentificare.

Alegătorii individuali ar putea fi supuși altor atacuri ale hackerilor. Prin intermediul introducerii unui virus informatic, furtul acreditărilor, atacurilor de tip phishing sau de inginerie socială ar putea împiedica un alegător săvoteze, să modifice alegerile unui alegător, să monitorizeze modul în care un votant votează, să folosească parolele alegătorului pentru a obtine accesul și să extindă acest acces pentru deteriorarea sistemului de votare, schimbarea rezultatelor alegerilor sau daunarea credibilității rezultatelor alegerilor. [27] Probabil, astfel de manipulări nu ar afecta un număr

[21] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[22] Wikström, D., Barrat, J., Heiberg, S., & Krimmer, R. 2017. How Could Snowden Attack an Election? In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 280-291. Cham, Switzerland: Springer.
[23] Applegate, M., Chanussot, T., & Basysty, V. 2020*. Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[24] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[25] Halderman, J.A. 2017. Practical Attacks on Real-World E-Voting. In: Hao, F., & Ryan, P.Y.A. (eds.) *Real-world Electronic Voting: Design Analysis and Deployment*. Pp. 143-170. London: CRC Press.
[26] Jonker, H., Mauw, S., & Schmitz, T. 2017. Reverse Bayesian Poisoning: How to Use Spam Filters to Manipulate Online Elections. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 183-197. Cham, Switzerland: Springer.
[27] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

mare de alegători. În orice caz, aceste riscuri ar trebui să fie luate în considerare. Unul dintre motivele pentru care alegătorii sunt extrem de vulnerabili este că „deși pot observa dacă ceva nu merge bine cu serviciile bancare online, din cauza banilor pierduți, anonimatul procesului de vot înseamnă că este aproape imposibil să observe dacă votul lor ar fi fost schimbat. "[28] Totuși, această ingrijorare priveste doar arhitecturile procesului de vot electronic în care alegătorii nu-si pot verifica voturile în niciun moment. Unele soluții IT au o astfel de posibilitate. În general, având în vedere spectrul larg de manipulări orientate către alegători, este rezonabil să se lanseze campanii de educație civică atrăgând atenția asupra riscurilor de votare electronică explicând modul de a vota în siguranță, sugerând utilizarea unui software antivirus avansat, ignorarea solicitărilor de tip phishing, verificarea voturilor acestora etc.

6. Excludere *versus* includere

O îngrijorare cu privire la votul electronic se referă la problema incluziunii. Ținând cont de complexitatea politicilor și diversitatea societăților, este esențial să se garanteze eficacitatea, pluralismul și corectitudinea prin mecanisme de democrație indirectă sau reprezentativă. [29] Se ia in considerare faptul căvotul electronic prezintă provocări referitoare la cerințele de eligibilitate pentru votarea la alegerile generale și evocă dezbateri cu privire la cine ar trebui să aibă dreptul de a vota, deoarece multe țări restricționează votarea la alegerile generale cetățenilor care sunt rezidenți în țară (fie pentru considerente de principii sau pentru chestiuni practice de administrare a voturilor cetățenilor cu domiciliul în afara țării). [30] Totuși, în astfel de cazuri, votul electronic are potențial de emancipare și de împuternicire. În primul rând, principiul votului universal garantează dreptul de vot tuturor cetățenilor eligibili. În al doilea rând, votarea la distanță, pe internet, ca o opțiune suplimentară la votul tradițional la secțiile de votare, este capabilă să extindă baza alegătorilor. Prin urmare, introducerea votului electronic poate genera dezbaterea cu privire la alegătorii eligibili, presupune schimbări legislative și poate asigura accesul la votul general pentru unele grupuri sociale excluse, cum ar fi expatriații, ceea ce ar putea face sondaje, consultări, referendumuri și alegeri mai inclusive.

Un punct de vedere contestat este dreptul la vot bazat pe merite. Există o opinie conform căreia, pentru decizii democratice eficiente și corecte, nu este neapărat nevoie de creșterea participării a alegătorilor la alegeri, dacă acest lucru stopează distincția dintre alegători cu preferințe intense (mai stabile și bazate pe cooperare) și alți votanți (de exemplu, votarea de acasă fără efort prin vot electronic pe internet s-ar putea să nu fie în cele din urmă de dorit). [31] Dar astfel de atitudine contravine principiului egalității drepturilor și voturilor egale și tinde să discrimineze persoanele care doresc să voteze online - prin urmare, ar trebui respinsă din motive normative. Argumentul citat este, de asemenea, defectuos, deoarece deliberarea și colaborarea online nu sunt „fără efort", dar uneori consumă multa energi sau chiar mai mult timp ca cele offline. În plus, o schimbare instantanee de opinie poate fi rezonabilă dacă se bazează pe unele informații noi despre o politică potențială, un candidat pentru o funcție publică sau un partid. Chiar dacă o schimbare de opinie nu este rațională, ci emoțională, este dreptul unui alegător să o facă. Este responsabilitatea factorilor de decizie și a politicienilor să comunice reprezentanților lor informații relevante despre ei înșiși, exacte și convingătoare.

O altă preocupare conexă se referă la problema divizării digitale. Îngrijorarea este că „votul pe internet poate să-i privilegieze pe „cei care au" și să le înlesnească votarea, dar nu îi poate ajuta pe„cei care nu au".[32] Însă combinația de opțiuni online și offline, ca alternativă, combate efectiv acest decalaj, deoarece un alegător poate alege în mod liber cel mai convenabil format de vot. În plus, există o listă de măsuri care pot facilita utilizarea votului electronic. În special, Consiliul Europei recomandă ca: (1) interfața alegătorilor unui sistem de votare electronică să fie ușor de înțeles și de utilizat de toți alegătorii; (2) opțiunile de vot de pe orice dispozitiv folosit sunt optimizate pentru alegătorul mediu, fără a avea cunoștințe informatice specializate; (3) alegătorii sunt implicați în proiectarea

[28] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[29] Innerarity, D. 2019. *Politics in the Times of Indignation: The Crisis of Representative Democracy*. London: Bloomsbury Academic.
[30] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[31] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[32] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.

sistemelor de votare electronică; (4) produsele IT noi sunt compatibile cu cele anterioare; (5) sistemul de votare electronică este accesibil persoanelor cu dizabilități și nevoi speciale; (6) la cerere, alegătorilor li se oferă interfețe speciale sau alte resurse echivalente; (7) Interfețele de vot electronic respectă, pe cât posibil, liniile directoare stabilite deInițiativa de Accesibilitate a Internetului (Web Accessibility Initiative).[33] De asemenea, de exemplu în țările europene, decalajul digital se diminuează datorita tendinței promițătoare a unei alfabetizări digitale în creștere și în difuzarea utilizării tehnologiilor bazate pe internet.[34]

7. Registre inexacte *versus* registre corecte de alegători

Registrele de alegători ar putea fi supuse manipulării. Ingrijorarea este că funcționarii electorali care au permisiuni la nivel superior pentru a adăuga alegători eligibili în baza de date de înregistrare a alegătorilor, pentru a elimina alegătorii neeligibili, pentru a configura buletinele de scrutin, pentru a defini ora și data de votare, a stabili regulile de concordanță pentru concursurile electorale și generarea de rapoarte electorale pot compromite în mod malițios și intenționat sistemul sau pot participa involuntar la un atac prin intermediul unei mașini infectate.[35] Apoi, registrele de alegători corupte pot fi utilizate greșit pentru a împiedica anumite persoane să voteze (de exemplu, identificarea preferințelor lor politice în funcție de declarațiile personale din social media) și pentru a exploata date ale persoanelor false sau moarte (să voteze ilegal pentru o politică preferată, un politician sau un partid).

Aceste riscuri ar trebui luate în considerare și prevenite. Conform regulamentelor Consiliului Europei, „Se va păstra autenticitatea, disponibilitatea și integritatea registrelor și listelor de alegători. Sursa datelor se autentifică. Dispozițiile privind protecția datelor trebuie respectate."[36] Există soluții tehnice și organizaționale standard pentru acest lucru. În special, „automatizarea și computerizarea sarcinilor funcționarilor electorali trebuie să fie însoțite de un set de protocoale care ar împiedica atacurile ascunse împotriva sistemului, niveluri adecvate de profiluri de conectare, parole și audituri, precum și programe de instruire și conștientizare cu privire la riscurile de securitate cibernetică. “[37]

La nivelul construcției de sistem, este posibil să se utilizeze tehnologii de evidență distribuite (de exemplu, blockchain). Datorită design-ului lor particular, ei stabilesc o rețea ‘peer-to-peer’ și un set de algoritmi de consens pentru un set consistent de date digitale replicate, partajate și sincronizate. Un registru de alegători care utilizează o astfel de tehnologie va fi mult mai dificil de modificat, deși acest lucru va necesita descentralizarea accesului la registru între mai multe entități (agenții publice) și familiarizarea administrațiilor sistemului cu această tehnologie elaborată. În plus, un astfel de sistem poate fi supraîncărcat de un număr mare de înregistrări și solicitări, de accceanecesită testări riguroase cu sarcină maximă.

8. Identificarea greșită *versus* identificarea corectă

Într-un mediu necontrolat în cazul votului la distanță pe internet, există riscul ca unor alegători eligibili să nu li se permită să voteze, în timp ce unii votanți falși (roboți semi sau complet automatizați sau persoane reale care utilizează documente furate sau false) vor vota, deși nu au dreptul să facă acest lucru. Îngrijorarea este că în cadrul votului pe internet „ar fi dificil, dacă nu imposibil, să constatăm că un anumit vot a fost emis de persoana îndreptățită să facă acest lucru și nu de un interlop.”[38] În cel mai rău caz, un număr critic de alegători identificați eronat astfel, pot

[33] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[34] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[35] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[36] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[37] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[38] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

„spori” în mod artificial o anume opțiune politică la un sondaj de consultare electronică, un referendum electronic obligatoriu sau pot alege la o funcție publică un anumit candidat în cadrul unei alegeri electronice.

Acest lucru poate fi evitat prin introducerea mai multor etape de identificare viabile care combinate vor minimiza riscurile de identificare greșită. De exemplu, rezidenții estonieni au identități digitale și „combinația unui token „puternic ”(cartea de identitate) și un token „slab”(numărul PIN) oferă securitate care verifică faptul că persoana care se conectează în sistem este, de fapt, persoana corectă. "[39] Ipotetic, o persoană poate renunța la identitatea sa digitală pentru bani. Dar acest lucru ar fi similar cu acordarea pașaportului care poate fi folosit pentru a lua un împrumut bancar sau pentru a înregistra o afacere. Astfel de riscuri sunt prea mari pentru ca o persoană să se angajeze intr-un astfel de demers. Cu toate acestea, există măsuri preventive chiar și pentru astfel de cazuride abuz de identitate digitală. Un alegător va trebui să facă o fotografie digitală în fața camerei de fotografiat imediat înainte de a emite un buletin de vot - fotografia va fi comparată cu fotografia alegătorului făcută pentru documentele de identitate emise de guvern. Aceste argumente în favoarea unei identificări mai stricte „sunt adesea încadrate ca o compensare între accesibilitatea procesului de vot pentru alegători și necesitatea unei mai mari securități împotriva fraudei în procesul de votare.” [40]

9. Dezvăluirea votului, presiune și cumpărare *versus* votul secret, libertate și integritate

Votarea prin internet la distanță pune problema asigurarii secretului unui vot. Se presupune, „votul electronic poate compromite secretul de scrutin.” [41] Cu toate acestea, multiple mecanisme tehnologice și organizaționale sunt concepute pentru a asigura secretul unui vot electronic. Conform regulamentelor Consiliului Europei, votarea electronică (1) asigură respectarea secretului votului în toate etapele procedurii de vot; (2) datele registrului alegătorilor trebuie să fie clar separate de componentele de vot; (3) un sistem de votare electronică și orice entitate autorizată protejează datele de autentificare, astfel încât părțile neautorizate să nu poată folosi în mod abuziv, să intercepteze, să modifice sau să obțină informații cu privire la aceste date; (4) un sistem de votare electronică nu furnizează alegătorului dovada conținutului votului emis pentru terți; (5) alegătorul ar trebui să fie informat cu privire la posibilele riscuri ale secretului votului electronic și la mijloacele recomandate pentru a le reduce înainte de vot; (6) alegătorul ar trebui să fie informat cu privire la modul de ștergere, acolo unde este posibil, a urmelor de vot din dispozitivul folosit la votarea de la distanță; (7) procesul de votare electronică se organizează astfel încât să nu fie posibilă reconstruirea unei legături între votul nesigilat și alegător; (8) informațiile despre alegători ar trebui separate de decizia alegătorului într-o etapă predefinită a procesului de numărare; (9) orice decodificare necesară pentru numărarea voturilor ar trebui să fie efectuată cât mai curând posibil după închiderea perioadei de votare. [42] În ciuda acestor măsuri, alegătorii pot încălca intenționat secretul votului și pot face fotografii cu buletinele de vot. Dar acest lucru poate apărea atât la voturile offline cât și la cele online. După cum s-a menționat, „țările ar trebui să fie, de asemenea, precaute să nu permită alegătorilor să trimită selfie-uri din cabinetul de votare.” [43] Astfel, restricțiile legale aplicate în practică și demonstrate prin vitrine ar trebui să oprească această practică.

Complexitatea soluțiilor tehnice se confruntă cu anumite critici. De exemplu, se consideră că dacă se permite alegătorului să definească un cod cunoscut doar lui, care va semnaliza semnificația votului (de exemplu, atunci când votează A, înseamnă că B) va eșua în sistemele de vot complexe și, la cel mai simplist nivel, un alegător poate să nu-și amintească codul atunci când votează. [44] Cu toate acestea, un alegător poate să uite de asemenea un număr de listă

[39] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[40] Hall, T. 2015. Internet voting: the state of the debate. In: Coleman, S., & Freelon, D. *Handbook of Digital Politics*. Pp. 103-117. Cheltenhaum, UK: Edward Elgar.
[41] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.
[42] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[43] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[44] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

sau să confunde numele unui candidat sau a unei politici dacă există liste de 'deghizare' similare. Riscurile par similare între votul online și offline și ar trebui tratate și atenuate în orice caz. Astfel, alegerile offline pot avea, de asemenea, eșecuri tehnice, dar totuși se desfășoară în ciuda acestor preocupări din motive normative de menținere a democrației.

Marea provocare a secretului votului electronic este că prezintă riscuri suplimentare. Faptul că este imposibil să se garanteze că nimeni nu urmărește alegătorii carevotează , deschide ușa posibilității constrângerii alegătorilor. [45] Cu toate acestea, problema dată are o soluție. Pentru a face față provocării prin care un un om poate exercita măsuri de constrângere asupra unui alegător în timpul votului, Statele Unite permit alegătorului să voteze de mai multe ori, doar ultimul vot fiind luat in considerare. [46] Într-adevăr, dreptul la schimbări nelimitate a votului până la sfârșitul perioadei electorale protejează împotriva unei amenințări imediate pentru un alegător, deoarece este posibil să voteze conform instrucțiunilor și să schimbe votul ulterior. Obiecția este că „acest lucru nu rezolvă problema, deoarece presiunea de a schimba un vot poate influența alegătorul în ultima clipă înainte de închiderea votului." [47] Cu toate acestea, intenția de a abuza masiv de votul electronic ar solicita prea mulți „controlori" să fie prezenți lângă alegători până la sfârșitul unei perioade de votare electronică, ceea ce ar face această tehnică de presiune să nu fie posibilă la scară largă.

Mai mult, organele electorale pot păstra opțiunea de rezervă a unui vot offline la o secție de votare. Astfel, o persoană va putea vota offline chiar și după perioada de votare online. Un contraargument al acestei măsuri este acela de a permite alegătorului să schimbe votul într-un mediu controlat, cum ar fi secția de votare, nu este o soluție pentru această vulnerabilitate în integritatea procesului, deoarece „persoana constrânsă poate fi prea înspăimântată să meargă la secția de votare." [48] Cu toate că, o persoană poate fi înspăimântată și să facă o fotografie cu votul chiar și la alegerile offline. „Studiile istorice cu privire la incidentele în care s-au făcut voturi în aer liber în Statele Unite dezvăluie că alegătorii au fost deseori supuși hărțuirii și chiar răpirii sau uciderii dacă nu și-au exprimat voturile conform dorințelor coercitorilor. Chiar și în absența coerciției explicite, alegătorii ar fi putut să se abțină de la vot pentru a evita hărțuirea pentru exprimarea opiniilor lor." [49] Pentru a proteja alegătorii de acest aspect, ar trebui să existe o linie telefonică specială pentru raportarea unor astfel de cazuri și un sistem profesional de aplicare a legii, capabil să gestioneze astfel de cazuri. Din punct de vedere strategic, o simulare a demonstrat că este în interesul societății să nu se adapteze la strategia așteptată a celui care exercită măsuri de coerciție, ci să promoveze deschis politica anti-coerciție, deoarece o persoană rațională va fi obligată să se abțină de la constrângere. [50]

Chiar dacă o persoană care emite un buletin de vot este cea care are dreptul să voteze și nu există nicio amenințare imediată, este posibil ca persoana să nu aibă o intenție autentică de a face acest lucru. Alegătorii pot simți presiunea de a se conforma așteptărilor semenilor, pot fi dispuși să facă acest lucru deoarece un singur vot nu determină de obicei rezultatele alegerilor, pot fi supuși presiunilor familiale și tribale - această presiune nu ar fi eficientă în stabilirea unui vot secret la secția de votare. [51] Dar presiunile de la egal la egal, de familie și ale triburilor pot exista și în alegerile offline, atât timp cât oamenii discută preferințele lor înainte de perioada de votare. Aceste riscuri există indiferent de tehnologia de vot aplicată și pot fi atenuate prin încurajarea unei discuții publice deschise și inteligente.

---

[45] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[46] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[47] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[48] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[49] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

[50] Jamroga, W., & Tabatabaei, M. 2016. Preventing Coercion in E-Voting: Be Open and Commit. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 1-17. Cham, Switzerland: Springer.

[51] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

De fapt, cu o tehnologie mobilă de votare electronică ar fi dificil să se exercite o presiune constantă, deoarece o persoană este capabilă să găsească timp și loc când și unde nimeni nu este în jur și votează în confidențialitate.

Chiar dacă nu există presiune externă, cumpărarea voturilor se poate întâmpla. Se pare că „pierderea secretului votului poate duce la luare de mită și la o piață a voturilor. Avem dovezi atât din Statele Unite, cât și din Marea Britanie că cumpărarea voturilor a devenit neatractivă doar atunci când nu exista un mecanism extern care să garanteze că un vot a fost într-adevăr dat așa cum a declarat alegătorul. ” [52] Aceasta se referă la soluțiile menționate anterior, de modificare a voturilor și votării offline, după votarea online. Cea mai critică perspectivă presupune că în prezent nicio tehnologie nu poate atenua eficient cumpărarea voturilor.[53] Într-adevăr, este o problemă socio-politică complexă, care poate apărea deopotrivă la alegeri offline și online, și ar trebui abordată prin campanii de conștientizare, combinată cu măsuri de aplicare a legii.

10. Votul de rutină și absentismul *versus* votul deliberat și bazat pe valori

O critică suplimentară a votului electronic este cea care contestă valoarea acțiunii civice. Probabil, votul electronic poate „afecta modul în care un buletin de vot se face mai degrabă asemănător cu un„ Like”decât cu un act deliberativ de implicare publică”, poate „crește importanța pe care alegătorii o dau intereselor private, distinctă de obiectivele comune”, eliminând valoarea și motivația de a fi „văzuți” de vecini, prieteni, colegi și familie ca cetățeni activi și angajați ”și chiar„ duc la scăderea ratei votului, în ciuda avantajelor ușurinței și costurilor reduse. ” [54] Cu toate acestea, înainte de a vota online, oamenii ar putea investi timp, atenție și energie în studierea politicilor în cauză sau a candidaților politici. Apoi, actul de votare pe internet va avea foarte multă valoare. Mai mult, oamenii pot posta fotografii lângă dispozitivele de vot sau cu notificările „votat”, păstrând secretul votului. De fapt, tehnologiile digitale facilitează demonstrarea acțiunii civice. Deşi accentul pus pe interese private sau publice și înclinația spre vot sau abținere este o motivație generică și, probabil, nu ar trebui să depindă de tehnologia votării.

O altă preocupare se referă la valoarea simbolică a actului de votare. Concluziile sunt că „realizarea actului de votare la fel de ușor precum navigarea prin canalele TV de pe canapea, elimină partea ceremonială a alegerilor”, „votul devine la fel de banal ca apăsarea butonului unei telecomenzi, nu un moment comunitar important în viață a unei națiuni, „alegătorii nu mai „ privesccetățenia prin ritualul de a se aduna cu concetățenii la cabinetul de votare ”, lipsită de transformarea „colectivului de persoane individuale în corpul poporului suveran ”. [55] Dimpotrivă, votul electronic ar putea da naștere unor noi ritualuri, cum ar fi postarea în social media cu hashtag-uri comune și, prin urmare, conectarea cu concetățenii. Mai mult, importanța votării nu depinde de distanță, ci de valori. Iar acest lucru poate fi îmbunătățit prin educație civică și conștientizare.

11. Stocarea și numărarea coruptă a votului *versus* verificabilitate și responsabilitate

Rezultatele votului electronic pot fi denaturate la stadiul de înregistrare și numărare a voturilor. Prin urmare, Consiliul Europei a stabilit o listă de linii directoare care să asigure rezultate valide în urma votării electronice. Recomandările precizează că ar trebui luate măsuri pentru a se asigura că (1) doar un număr adecvat de voturi pentru fiecare alegător este alocat, stocat în urna electronică și inclus în rezultatul alegerilor; (2) dacă unui alegător i se permite să voteze electronic de mai multe ori, atunci se ia în considerare doar un vot; (3) dacă un alegător are voie să voteze pe mai multe canale de vot, atunci se ia în considerare doar un vot; (4) în toate celelalte cazuri - un alegător nu votează

[52] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[53] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[54] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[55] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.

mai mult de un vot; (5) în toate cazurile - alegătorul este informat clar despre posibilitățile de vot oferite și despre regulile de numărare a voturilor. [56]

Pentru asigurarea unor rezultate valide, sistemele de vot elecronic au drept scop introducerea posibilităților de verificare. În special, verificarea „end-to-end" (E2E) înseamnă că „alegătorii și eventual auditorii externi ar trebui să poată verifica dacă rezultatul alegerilor publicate este corect, adică corespunde voturilor exprimate de către alegători, chiar dacă dispozitivele de vot și serverele au erori de programare sau sunt rău intenționate. [57] Autorii precizează în plus că o verificare individuală se realizează atunci când un expeditor poate verifica dacă mesajul a ajuns la destinație, dar nu poate stabili dacă acest lucru este valabil pentru ceilalți alegători, în timp ce verificarea universală garantează că este posibil să se verifice în mod public dacă buletinele de vot sunt corecte. Este posibil ca „un sistem de votare verificabilă de la capăt la sfârșit (E2EVV) să elimine frauda electorală, permițând alegătorilor să verifice nu numai că votul lor este exprimat așa cum este prevăzut, dar și înregistrat și numărat corect." [58]

De exemplu, chiar și sistemul de vot electronic estonian poate fi susceptibil la un atac care vizează rezultatele alegerilor. Pentru a ilustra acest lucru, un program de „malware" a demonstrat posibilitatea de a schimba sau bloca un vot fără ca alegătorul să-l observe. Drept răspuns, au fost dezvoltate două mecanisme de verificare avansate: (1) un dispozitiv independent de calcul mobil care descarcă criptograma votului de pe serverul de stocare și îl forțează brut folosind cheide criptare aleatoare, obținute de pe computerul alegătorului printr-un cod QR; (2) un software găzduit de server care generează codul de verificare pentru alegător. [59] Protocolul asigură o securitate mai puternică, necesitând cel puțin două părți să colaboreze in mod malițios pentru a sparge proprietățile de verificare sau confidențialitate.

Pentru a asigura stocarea securizată a datelor privind votul și numărarea voturilor, poate fi utilă folosirea tehnologiilor avansate de votare electronică. Unul dintre care este blockchain - un registru distribuit deschis, rezistent la modificarea datelor, datorită unei înregistrări de date criptografice care necesită un consens de rețea peer-to-peer pentru a modifica datele. Un alt sistem de vot este „Prêt à Voter" care folosește lista de candidați aleatorie și codificată criptografic. Permite simultan un calcul automat al rezultatelor alegerilor, permite unui alegător să verifice un vot individual și protejează secretul votului. Atât soluțiile blockchain, cât și *Prêt à Voter* „se asigură că niciuna dintre părți nu este capabilă să controleze, să șteargă sau să modifice toate datele și, prin urmare, să denatureze rezultatele votării." [60] Cu toate acestea, rămâne riscul ca tehnologia blockchain „nu protejează informațiile care circulă pe internet și nu face ca serverele și infrastructura să fie mai rezistente la amenințări avansate persistente." [61] Ținând cont de aceasta, o soluție rezonabilă ar fi încercarea unui sistem de vot la scară mai mică sau votarea fără caracter obligatoriu.

În afară de instituirea unui sistem de votare electronică sigur din punct de vedere al securității cibernetice și de a permite funcția de verificare end-to-end, este rezonabil să se efectueze în mod implicit supravegherea/controlul condus de organele de conducere electorale și de societatea civilă. Motivul este că manipulările complexe ale votului electronic ar putea denatura și distorsiona datele privind votul. Astfel, simularea alegerilor electronice australiene arătat că, folosind manipularea bazată pe MOV și minimizarea schimbării primelor de preferințe, un atacator poate evita o renumărare automată și poate schimba cu succes câștigătorul alegerilor. [62] Prin urmare, autorii consideră că

[56] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[57] Küsters, R., & Müller, J. 2017. Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 21-41. Cham, Switzerland: Springer.

[58] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

[59] Kubjas, I., Pikma, T., & Willemson, J. 2017. Estonian Voting Verification Mechanism Revisited Again. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp. 306-317. Cham, Switzerland: Springer.

[60] Khutkyy, D. 2020. E-voting in Ukraine: Advancements, Challenges and Perspectives. *Brussels Ukraïna Review, April*, 11-13.

[61] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[62] Blom, M., Stuckey, P.J., & Teague, V.J. 2019. Election Manipulation with Partial Information. In: Krimmer, R. et al (eds.) *Electronic Voting: Fourth International Joint Conference, E-Vote-ID 2019*. Pp. 32-49. Cham, Switzerland: Springer.

limitarea auditului alegerilor presupune un risc major. În mod ideal, astfel de audituri ar trebui să acopere setul de date complet al voturilor. Specific, „un audit de comparare a buletinelor de vot necesită numărarea independentă a tuturor buletinelor virtuale, nu doar a eșantionului, pentru a verifica dacă calculatoarele electorale au adăugat corect totalurile.” [63]

Consiliul Europei a stabilit un set cuprinzător de standarde complexe. În special, acestea presupun ca: (1) sistemul de votare electronică să fieauditat; (2) sistemul de audit trebuie să fie deschis și cuprinzător și să prezinte un raport activ cu privire la problemele și amenințările potențiale; (3) sistemul de audit ar trebui să înregistreze orele, evenimentele și acțiunile; (4) instrumentele și procedurile automatizate ar trebui să permită analizarea și raportarea datelor într-un mod rapid și precis, permițând astfel o acțiune corectivă rapidă; (5) sistemul de audit ar trebui să furnizeze rapoarte controlabile privind verificările încrucișate ale datelor, atacurilor de sistem sau de rețea, detectarea și raportarea intruziunilor, manipularea datelor, tentative de fraudă și fraudă; (6) sistemul de votare electronică ar trebui să mențină surse de timp sincronizate fiabile; (7) precizia sursei de timp ar trebui să fie suficientă pentru păstrarea marcajelor pentru pistele de audit și datele de observare, precum și pentru menținerea limitelor de timp pentru înregistrare, nominalizare, vot sau numărare; (8) concluziile obținute în urma procesului de audit ar trebui luate în considerare la viitoarele alegeri electronice. [64]

Pe lângă verificabilitate, sistemul de vot electronic ar trebui să aibă responsabilitate. Responsabilitatea nu numai că permite să se verifice dacă o proprietate dorită este garantată, de exemplu, rezultatul alegerilor este corect, dar, de asemenea, se asigură că partidele cu un comportament necorespunzător pot fi identificate dacă este cazul. [65] Autorii explică faptul că responsabilitatea consolidează stimulul tuturor părților de a-și îndeplini rolurile, deoarece acestea pot fi identificate în cazul în care se comportă greșit și apoi s-ar putea confrunta , de exemplu, cu sancțiuni financiare sau legale severe sau își pot pierde reputația.

12. Discreditarea campaniei de vot *versus* legitimitate și încredere

Indiferent dacă a avut loc sau nu o tentativă de hacking asupra alegererilor elctronice , este esențial ca o comunitate sau o societate să fie de acord cu faptul că votul electronic a fost efectuat în mod corespunzător, afirmându-i legitimitatea. Nu este suficient ca alegerile să îndeplinească cerințele votului universal, egal, gratuit și secret *de facto*, dar pentru ca democrația să existe, alegătorii trebuie să creadă că aceste cerințe au fost îndeplinite și nu trebuie să se pună problema corectitudinii proceselor de vot printre alegători. [66] Acest lucru este esențial în special pentru votul electronic inițial. Întrucât „o primă experiență negativă - sau o vulnerabilitate tratată necorespunzător - poate întoarce părțile electorale împotriva tehnologiei, iar încrederea devine dificil de recuperat”. [67] Votul manipulat poate dăuna nu numai atitudinilor față de o anumită tehnologie de vot, ci și a democrației în sine. Astfel, frauda electorală la scară largă poate să submineze încrederea în democrație. [68]

În acest sens, activitățile de comunicare regulate bazate pe transparență, sunt vitale pentru menținerea atitudinii de încredere a publicului. Când în 2017 a fost identificată o vulnerabilitate critică în sistemul cărților de identitate estone, autoritățile naționale au adoptat o politică de maximă transparență cu privire la impactul vulnerabilității și la

[63] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[64] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.
[65] Küsters, R., & Müller, J. 2017. Cryptographic Security Analysis of E-voting Systems: Achievements, Misconceptions, and Limitations. In: Krimmer, R. et al (eds.) *Electronic Voting: Second International Joint Conference, E-Vote-ID 2017*. Pp 21-41. Cham, Switzerland: Springer.
[66] Weill, R. 2017. Election Integrity: The Constitutionality of Transitioning to Electronic Voting in Comparative Terms. In: Prins, C. et al (eds.) *Digital Democracy in a Globalized World*. Pp. 142-159. Cheltenhaum, UK: Edward Elgar.
[67] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.
[68] Russell, M. & Zamfir, I. 2018. *Digital Technology in Elections: Efficiency versus Credibility?* Brussels: European Parliamentary Research Service.

acțiunile întreprinse pentru atenuarea acesteia - această politică a avut succes datorită încrederii publice în autorități și o populație relativ mică.[69]

Recomandările sunt următoarele: (1) statele trebuie să fie transparente în toate aspectele votării electronice; (2) autoritățile electorale competente ar trebui să publice o listă oficială a software-ului utilizat la o alegere electronică; (3) accesul publicului la componentele sistemului de votare electronică și la informațiile acestora, în special documentația, codul sursă și acordurile de confidențialitate, ar trebui să fie dezvăluite părților interesate și publicului larg, cu mult înainte de perioada electorală; (4) implementarea tehnologiilor de vot electronic ar trebui să includă elaborarea de ghiduri detaliate, pas cu pas, inclusiv un manual de procedură; (5) componentele sistemului de votare electronică sunt dezvăluite în scopuri de verificare și certificare; (6) sistemele de votare electronică ar trebui să genereze date de observare fiabile și suficient de detaliate, astfel încât observația electorală să poată fi realizată; (7) ar trebui să fie posibil să se determine în mod fiabil momentul în care un eveniment a generat date de observare; (8) autenticitatea, disponibilitatea și integritatea datelor ar trebui menținute; (9) Observatorii interni și internaționali ar trebui să aibă acces la toată documentația relevantă privind procesele de votare electronică, la testarea software-ului și a hardware-ului și la procesul de evaluare și certificare. [70]

Opinia publică a publicului larg este sensibilă în ceea ce privește încadrarea discuțiilor despre formatul de vot. De exemplu, s-a descoperit că, în Statele Unite, pregătirea alegătorilor cu considerente de fraudă la vot îi determină să favorizezealternativele pe hârtie aparatelor de vot cu ecran tactil; și, invers, considerentele de comoditate îi determină să afișeze o preferință mai mare pentru votarea electronică în raport cu alternativele pe hârtie; a fi expus unor considerente de fraudă / comoditate cauzează abateri semnificative de la tendința alegătorilor de a prefera sisteme cu care sunt deja familiarizați. [71] Prin urmare, discuțiile despre votarea pe hârtie, electronică la fața locului sau pe internet ar trebui să fie bine echilibrate și obiective.

Atitudinile politice și ale profesioniștilor cu privire la tehnologia și politica votului electronic sunt, de asemenea, importante pentru stabilirea credibilitățăii voturilor pe internet. În special, este rezonabil să implicămspecialiști, activiști și factori de decizie în etapele inițiale ale dezvoltării politicilor de votare electronică, experții să ia parte in procesul decizional și să se comunice clar modul încare sfaturile lor au fost luate în considerare.. În perioada de votare, publicarea codului sistemului de votare electronică, care să ofere rezultate instantanee și având o atitudine deschisă privind auditul civic poate crea încredere. În plus, este important să se explice aspecte tehnice, politice și sociale ale votării și jurnaliștilor și liderilor de opinie și să le ilustreze cu infografice și materiale video în mod concis. Susținerea din partea elitelor politice în stabilirea neutralității politice va facilita, de asemenea, a tranziția cătrevotul electronic. [72]

[69] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[70] Council of Europe. 2017. *Guidelines on the implementation of the provisions of Recommendation CM/Rec(2017)5 on standards for e-voting*. 14 June.

[71] Alvarez, R.M., Levin, I., & Li, Y. 2018. Fraud, Convenience, and E-voting: How Voting Experience Shapes Opinions about Voting Technology. *Journal of Information Technology & Politics, 15, 1*, 94-105, DOI: 10.1080/19331681.2018.1460288

[72] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.

Concluzii

Așa cum a dovedit această analiză, votarea electronică are riscuri multiple, dar pot fi mitigate. Pentru fiecare problemă particulară dezvăluită de specialiștișipracticieni a fost elaborată una sau mai multe soluții corespunzătoare. Prin urmare, dacă s-a decis introducerea votului electronic, este o chestiune de diligență sporită pentru atenuarea riscurilor.

Numeroase provocări sunt asociate cu partea tehnică a hardware-ului și software-ului sistemului de vot - funcționarea defectuoasă, hackingul, compromiterea registrelor de alegători, identificarea greșită a alegătorilor, divulgarea votului, stocarea și numărarea coruptă a voturilor. Însă soluțiile avansate de securitate cibernetică și măsurile organizatorice ar trebui să fie suficiente pentru a proteja sistemul de vot pe internet. Având în vedere complexitatea sistemului de votonline, eforturile de protejare și de hacking ar putea părea o „cursă de înarmare" eternă. Cu toate acestea, atragerea hackerilor etici de „bună credință" pentru a contesta și îmbunătăți sistemul ar trebui să ofere organismelor de management al votului un avantaj suplimentar. În orice caz, unele țări au demonstrat un nivel ridicat de fiabilitate a sistemului de votare online în viață reală.

Alte abuzuri potențiale se referă la tehnici „politice" specifice" de influențare a votului, a administratorilor de vot și a alegătorilor. Acestea includ încadrarea problemelor într-o anumită direcție, părtinirea discursului media online, excluderea alegătorilor, presiunea asupra alegătorilor și cumpărarea voturilor. Acestea necesită măsuri preventive sistematice pe linia acțiunii legislative, transparență publică, supraveghere civică, aplicarea legii și responsabilitate publică. Întrucât guvernele alături de o societate civilă activă dețin o autoritate finală consolidată, împreună au forțe necesare pentru a pune în aplicare măsurile de contra-abuz.

Și, în sfârșit, unele prejudecăți și manipulări afectează alegătorii individuali în special și publicul, în general, având astfel un caracter „social". Acestea se referă la polarizarea grupului, denaturarea realității sociale, presiunea grupului, rutina de vot, absenteismul și discreditarea campaniei. Aceste provocări necesită activități majore în avans, care vizează crearea unui spațiu de discuție conectat, lansarea de educație civică, campanii de sensibilizare și mobilizare, completate de discuții ample ale experților și comunicare cu publicul bazată pe transparență. Acesta este probabil cel mai dificil domeniu de acțiune, deoarece depinde de schimbarea atitudinilor individuale și transformarea opiniei publice generale. Cu toate acestea, schimbările societale se întâmplă, deși de obicei treptat.

Sfera de proliferare a voturilor pe internet poate fi ilustrată prin aplicarea sa specifică la alegerile electronice ale funcționarilor publici. Întrucât alegerile oficiale electronice pentru funcțiile publice sunt obligatorii, împuternicesc câștigătoriișideschid calea către influențarea directă a politicilor naționale, acestea sunt considerate eforturi „de mare interes". De la alegerile anticipate obligatorii din 2003, unele țări au încercat și au abandonat deja alegerile electronice, în principal din cauza problemelor de securitate cibernetică. Și deși aceste cazuri au fost discutate pe scară largă, mai ales în lumina problemelor întâmpinate, unele dintre aceste țări iau în considerare reintroducerea alegerilor electronice. Mai mult, numărul de țări care practică alegerile electronice, deși este modest în număr absolut, este cu siguranță mai mare decât numărul de țări care le-au abandonat. Chiar și mai multe țări iau în considerare introducerea alegerilor electronice în viitor, iar numărul acestora este în creștere. Guvernele lor învață de la predecesori, efectuează studii de fezabilitate, adoptă politici bazate pe dovezi, testează sisteme avansate de blockchain și *Prêt à Voter*, efectuează teste-pilot și lansează discuții cu experți și public. Și deși durează ani de zile, având în vedere avantajele incluzive, temporale, financiare și reputaționale pe termen lung, votarea pe internet reprezintă o investiție sustenabilă.

Anexe

Tabelul 1: Țările care au folosit anterior, dar au abandonat voturile politice electronice obligatorii în timpul alegerilor funcționarilor publici (două din luna mai 2020)

Sursă: Dacă nu se specifică altfel – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Țara	Ani practicați	Scara votului electronic	Alegători eligibili	Motive pentru abandonare
Olanda	2004 2004 2006[73]	Sub-național Uniunea Europeană Național	Alegătorii din anumite circumscripții (Rijnland) Alegătorii din afara țării Alegătorii din afara țării	2008: preocupări de securitate cibernetică enunțate de activiști civici și internalizate de guvern[74]
Norvegia	2011 2013	Sub-național Național	Alegătorii din anumite circumscripții (10 municipalități) Alegătorii din anumite circumscripții (12 municipalități)	2014: preocupările guvernului în privința securității cibernetice și a impactului acestora asupra prezenței la vot[75]

Tabel 2: Țări care au folosit anterior, au abandonat, dar consideră reintroducerea voturilor electronice obligatorii la alegerile funcționarilor publici (două din luna mai 2020)

Sursă: Dacă nu se specifică altfel – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Țara	Ani practicați	Scara votului electronic	Alegători eligibili	Starea curentă
Elveția (experiență)[76]	2003-2018 2008-2018	Sub-național Național	Alegătorii din anumite circumscripții (până la 13 cantoane) Alegătorii din străinătate (din circumscripții particulare – până la 13 cantoane)	2019: Motiv pentru întrerupere – controversă politică privind problemele de securitate cibernetică[78]
Elveția (încercare)[77]	2019	Național	Unii alegători din circumscripții electorale	2019: Au fost aprobate probele sistemului electronic de votare

[73] Caarls, S. 2010. *E-Voting Handbook: Key Steps in the Implementation of E-Enabled Elections*. Strasbourg: Council of Europe.
[74] Loeber, L. 2014. *E-voting in the Netherlands; past, current, future?* Conference Paper. October. URL: https://www.researchgate.net/publication/301547849_E-voting_in_the_Netherlands_past_current_future
[75] Trechsel, A., Kucherenko, V., & Silva, Federico. 2016. *Potential and challenges of e-voting in the European Union*. EUDO Report 2016/11. Firenze: European University Institute.
[76] Germann, M., & Serdült, U. 2014. Internet Voting for Expatriates: The Swiss Case. *JeDEM: eJournal of eDemocracy and Open Government, 6, 2,* 197-215. DOI: https://doi.org/10.29379/jedem.v6i2.302
[77] Geiser, U. 2019. E-voting suffers another setback amid expat Swiss concerns. *SWI: Swissinfo.ch*. 27 June. URL: https://www.swissinfo.ch/eng/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918
[78] Geiser, U. 2019. E-voting suffers another setback amid expat Swiss concerns. *SWI: Swissinfo.ch*. 27 June. URL: https://www.swissinfo.ch/eng/digital-democracy_e-voting-suffers-another-setback-amid-expat-swiss-concerns/45059918

Țara	Ani practicați	Scara votului electronic	Alegători eligibili	Starea curentă
Franța (experiență)[79]	2012-2016	Național	Alegătorii din străinătate	2017: Motiv pentru întrerupere - probleme de securitate cibernetică
Franța (încercare)[80]	2020	Local	Alegătorii din străinătate	2020: Au fost efectuate teste non-obligatorii ale unei platforme de vot pe Internet

Tabel 3: Țările care utilizează în prezent voturile politice electronice obligatorii la alegerile funcționarilor publici (cel puțin 6 din luna mai 2020)

Sursă: Dacă nu se specifică altfel – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Țara	Ani practicați	Scara votului electronic	Alegători eligibili pentru vot electronic	Caracteristici
Armenia[81]	2012, 2013 2017, 2018	Național Național	Personalul diplomatic și familiile acestora, alegătorii din străinătate Personalul diplomatic și familiile acestora, alegătorii din străinătate, alegătorii militari	Rezultatele alegerilor sunt stocate în fișierepredispuse la riscul de abuz
Australia	2007[82] 2011-current[83]	Național Subnațional	Alegătorii militari Alegătorii din anumite circumscripții (New South Wales și Australia de Vest)	Alegerile pe internet au demonstrat: costuri rezonabile; dezirabilitatea (inclusiv capacitatea de a păstra secretul de vot) și efectul asupra comportamentului alegătorilor; încredere în sistemul electoral[84]

[79] Leigh, T. 2017. France drops electronic voting for citizens abroad over cybersecurity fears. *Reuters*. 6 March. URL: https://www.reuters.com/article/us-france-election-cyber/france-drops-electronic-voting-for-citizens-abroad-over-cybersecurity-fears-idUSKBN16D233

[80] The French Ministry for Europe and Foreign Affairs. 2020. French citizens abroad – Approval of electronic voting for consular elections. 15 January. URL: https://www.diplomatie.gouv.fr/en/the-ministry-and-its-network/news/2020/article/french-citizens-abroad-approval-of-electronic-voting-for-consular-elections-15

[81] Manougian, H. 2020. Did You Know Armenia Allows Internet Voting? (But It's only for Some). *EVN Report*. 13 February. URL: https://www.evnreport.com/politics/did-you-know-armenia-allows-internet-voting-but-it-s-only-for-some

[82] Lundie, R. 2016. Electronic voting at federal elections. *Parliament of Australia.* URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting

[83] Goodman, N., & Smith, R. 2016. Internet Voting in Sub-national Elections: Policy Learning. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 164-177. Cham, Switzerland: Springer.

[84] Lundie, R. 2016. Electronic voting at federal elections. *Parliament of Australia.* URL: https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook45p/ElectronicVoting

Țara	Ani practicați	Scara votului electronic	Alegători eligibili pentru vot electronic	Caracteristici
Canada	2003-current[85]	Sub-național	Alegătorii din anumite circumscripții (Ontario și Nova Scotia)	Numărul și tipul de informații de acreditare (de ex. PIN, data nașterii, întrebarea de securitate și înregistrare în avans cu mai multe credențiale) variază; problemele tehnice și de securitate raportate au fost limitate; alegătorii raportează experiențe pozitive[86]
Estonia	2009, 2014, 2019 2006, 2007, 2011, 2015, 2016, 2019 2005, 2009, 2013, 2017[87]	Uniunea Europeană Național Sub-național	Toți alegătorii	Votarea electronică se efectuează cu șapte zile înainte de votarea pe hârtie în ziua alegerilor; se aplică verificarea „ Vot înregistrat”; votarea electronică este neutră din punct de vedere politic și nu afectează rezultatele alegerilor; există un grad ridicat de încredere în sistem și proceduri[88]
Panama	2014, 2018[89]	National, subnational	Alegătorii din străinătate	Alegătorii au nevoie de o carte de identitate valabilă pentru a vota[90]
Statele Unite ale Americii	2016-curent	National, subnational	Alegătorii din străinătate, alegătorii militari, alegătorii din circumscripții particulare (peste 30 de state)[91]	Soluțiile tehnologice specifice variază de la un stat la altul; experții subliniază preocupările privind securitatea cibernetică[92]

[85] Government of Canada. 2017. Online Voting: A Path Forward for Federal Elections. January. URL: https://www.canada.ca/en/democratic-institutions/services/reports/online-voting-path-forward-federal-elections.html#toc21

[86] Goodman, N., & Smith, R. 2016. Internet Voting in Sub-national Elections: Policy Learning. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 164-177. Cham, Switzerland: Springer.

[87] Valisimed. 2020. Toimunud valimiste arhiiv. URL: https://www.valimised.ee/et/toimunud-valimiste-arhiiv

[88] Vinkel, P., & Krimmer, R. 2016. The How and Why to Internet Voting an Attempt to Explain E-Stonia. In: Krimmer, R. et al (eds.) *Electronic Voting: First International Joint Conference, E-Vote-ID 2016*. Pp. 178-191. Cham, Switzerland: Springer.

[89] Tribunal Electoral. 2020. Elecciones Generales 1994-2019. URL: https://www.tribunal-electoral.gob.pa/eventos-electorales/elecciones-generales-1994-2019/

[90] Fierro, C.N. et. al. 2016. *Electoral Studies in Compared International Perspective. Voting from Abroad in 18 Latin American Countries*. México, Mexico: National Electoral Institute. URL: http://www.undp.org/content/dam/undp/library/Democratic%20Governance/Electoral%20Systems%20and%20Processes/Voting%20from%20Abroad%20in%2018%20Latin%20American%20Countries%20web%20version%20ENG.pdf

[91] Applegate, M., Chanussot, T., & Basysty, V. 2020. *Considerations on Internet Voting: An Overview for Electoral Decision-Makers*. Arlington, VA: IFES.

[92] Parks, M. 2019. In 2020, Some Americans Will Vote on Their Phones. Is That the Future? *NPR*. 7 November. URL: https://www.npr.org/2019/11/07/776403310/in-2020-some-americans-will-vote-on-their-phones-is-that-the-future?t=1588522064124

Tabel 4: Țări care consideră introducerea votului politic electronic obligatoriu la alegerile funcționarilor publici (cel puțin 17 din luna mai 2020)

Sursă: Dacă nu se specifică altfel – IDEA. 2020. ICTS in Elections Database. URL: https://www.idea.int/data-tools/data/icts-elections

Țara	Ani practicați	Scara votului electronic	Alegători eligibili pentru vot electronic	Caracteristici
Austria	2004	Național	Toți alegătorii	A fost efectuat un studiu de fezabilitate[93]
Haiti	2017	Național	Toți alegătorii	A fost efectuat un studiu de fezabilitate[94]
Islanda	2014	Subnațional	Alegătorii din anumite circumscripții (orașul Reykjavik)	A fost efectuat un studiu de fezabilitate[95]
India[96]	2010-2011	Subnațional	Alegătorii din anumite circumscripții	A fost efectuat un proces de votare locală cu caracter obligatoriu[97]
Finlanda[98]	2016-2017	Național, subnațional	Toți alegătorii	A fost efectuat un studiu de fezabilitate
Mexic	2012 2016	Subnațional Național, subnațional	Alegătorii din străinătate Alegătorii din străinătate	A fost efectuat un proces de votare locală cu caracter obligatoriu[99] Au fost elaborate regulamente oficiale[100]
Moldova	2016	Național	Toți alegătorii	A fost realizat un studiu de fezabilitate și a fost elaborată o foaie de parcurs[101]
Noua Zelandă[102]	2016, 2019	Subnațional	Alegătorii din anumite circumscripții	Au fost inițiat probe caracter obligatoriu de votare electronică
Pakistan	2019	Național	Alegătorii din străinătate	Au fost efectuate încercări la scară mică a unui sistem de vot electronic[103]

[93] Bundesministerium Inneres. 2020. Wahlen. Wahlrecht in Österreich, Überblick. URL: https://www.bmi.gv.at/412/start.aspx
[94] Chéry, P.M. 2017. *Analysis of the Feasibility of Electronic Voting in Haiti. Working paper.* 17 February. Copenhagen Consensus Center. URL: http://www.copenhagenconsensus.com/sites/default/files/electronic_voting_chery.pdf
[95] Island.is. 2020. Overview of the proposed solution. URL: https://vefur.island.is/media/pdf-skjol-a-island.is-2014/RegistersIceland-evoting.pdf
[96] Election Commission of India. 2020. Digital Inclusion for citizens in India for democracy. URL: https://eci.gov.in/divisions-of-eci/ict-apps/
[97] Scytl. 2020. State of Gujarat India. Internet voting for municipal elections. URL: https://www.parliament.uk/documents/speaker/digital-democracy/GUJARATINDIA.pdf
[98] Vaalit Val. 2020. Electronic voting in Finland. URL: https://vaalit.fi/en/electronic-voting1
[99] Munive, E.-Y. 2012. Mexican experience of e-voting. *Diplo Internet Governance Community.* 13 July. URL: http://www.diplointernetgovernance.org/profiles/blogs/mexican-experience-of-e-voting
[100] SEGOB. 2016. Acuerdo. *SEGOB*. 1 December. URL: https://www.dof.gob.mx/nota_detalle.php?codigo=5463327&fecha=01/12/2016
[101] Republica Moldova. Comisa Electorala Centrala. 2016. *Feasibility study on Internet Voting for the Central Electoral Commission of the Republic of Moldova. Report and Preliminary Roadmap*. Chisinau, Moldova: Republica Moldova. Comisa Electorala Centrala. URL: https://www.undp.org/content/dam/moldova/docs/Publications/MD-IVOTE-FS-and-Roadmap_cleanENG.pdf
[102] Molineaux, J. 2019. *Solving and creating problems: Online voting in New Zealand*. January. Auckland, New Zealand: Auckland University of Technology. URL: https://thepolicyobservatory.aut.ac.nz/__data/assets/pdf_file/0003/302538/Solving-and-creating-problems-online-voting-in-New-Zealand.pdf

Țara	Ani practicați	Scara votului electronic	Alegători eligibili pentru vot electronic	Caracteristici
Portugalia	2005	Național	Alegătorii din străinătate	Efectuat un experiment a votului electronic ne-obligatoriu[104]
Rusia[105]	2019	Subnațional	Alegătorii din anumite circumscripții (orașul Moscova)	A fost efectuat o încercare de vot electronic obligatoriu folosind un sistem privat de blockchain
Sierra Leone	2018	Subnațional	Alegătorii din anumite circumscripții	A început să se dezvolte un sistem de votare electronică bazată pe blockchain cu ciclu complet[106]
Spania	2018 2003	Național Subnațional	Toți alegătorii Alegătorii din străinătate din anumite circumscripții (Catalonia)	A fost efectuat un studiu de fezabilitate[107] A fost efectuat un încercare-pilot de vot electronic fără caracter obligatoriu
Turcia	2011	Național	Toți alegătorii	Un studiu de fezabilitate a fost analizat privind sistemul *Prêt à Voter*[108]
Ukraina	2018 2019	Național Național	Alegătorii din străinătate Alegătorii din străinătate	A fost efectuat un experiment de vot electronic fără caracter obligatoriu folosind un sistem bazat pe blockchain[109] Documente relevante au început să fie elaborate[110]
Emiratele Arabe Unite	2011	Național	Toți alegătorii	Au fost efectuate probe fără caracter obligatoriu ale sistemului de vot electronic[111]
Marea Britanie	2002, 2003, 2007	Subnațional	Alegătorii din anumite circumscripții (6 consilii)[112]	Au fost efectuate probe-pilot cu caracter obligatoriu de votare electronică[113]

[103] Haq, H.B., McDermott, R., & Ali, S.T. 2019. *Pakistan's Internet Voting Experiment*. July. URL: https://www.researchgate.net/publication/334558559_Pakistan%27s_Internet_Voting_Experiment
[104] Comissão Nacional de Eleições. 2020. Voto electrónico. URL: http://www.cne.pt/content/voto-electronico
[105] Официальный сайт Мэра Москвы. 2020. Электронные выборы в Московскую городскую Думу. *Официальный сайт Мэра Москвы*. URL: https://www.mos.ru/city/projects/blockchain-vybory/
[106] E&T editorial staff. 2018. Blockchain technology deployed in Sierra Leonean election. *E&T*. 16 March. URL: https://eandt.theiet.org/content/articles/2018/03/blockchain-technology-deployed-in-sierra-leonean-election/
[107] Riera, A. & Cervelló, G. 2013. *Experimentation on Secure Internet Voting in Spain*. URL: https://subs.emis.de/LNI/Proceedings/Proceedings47/Proceeding.GI.47-10.pdf
[108] Adalier, O. et. al. 2011. A Case Study for Turkey: A Secure Paper-Based Electronic Voting System. *International Journal of eBusiness and eGovernment Studies, 3, 1*. URL: https://dergipark.org.tr/en/download/article-file/257068
[109] Suberg, W. 2018. Ukraine Electoral Commission Uses NEM Blockchain for Voting Trial. *Cointelegraph*. 8 August. URL: https://cointelegraph.com/news/ukraine-electoral-commission-uses-nem-blockchain-for-voting-trial
[110] Шишацкий, Е. & Юрасов, С. 2019. Большое интервью с Михаилом Федоровым. *Ліга.Tech*. 5 August. URL: https://tech.liga.net/technology/interview/didjital-strateg-zelenskogo-za-kajdym-reestrom-est-smotryaschiy-ot-kriminala
[111] ICA. 2020. E-Voting UAE: A Case Study. URL: https://www.ica.gov.ae/userfiles/EVoting_UAE_%20A%20Case%20Study.pdf
[112] Barry, C. et. at. 2002. *eVolution not revolution. Electronic Voting Status Report 2*. September. URL: https://www.vec.vic.gov.au/files/RP-EvolutionNotRevolution.pdf
[113] Kobie, N. 2015. Why electronic voting isn't secure – but may be safe enough. *The Guardian*. 30 March. URL: https://www.theguardian.com/technology/2015/mar/30/why-electronic-voting-is-not-secure