info@apti.ro
www.apti.ro

30 Iunie 2015

Votul electronic
probleme numeroase și grave și beneficii aproape inexistente

1. Introducere și terminologie[1]

Înainte de a intra în detalii despre diversele metode de vot electronic, trebuie stabilită terminologia necesară. Acest lucru este necesar pentru că, de obicei, termenul de *vot electronic* este folosit drept un termen generic pentru multiplele modalități de vot care au în componență diverse componente electronice. În realitate, pot fi identificate patru modalități principale de vot care au în componența lor cel puțin o etapa care este executată pe cale electronică. În practică, pot fi întâlnite multiple variații ale fiecăreia dintre aceste patru modalități principale, dar fără a ne pierde în detalii, acestea patru sunt:

Numărare electronică: în cazul acestui tip de vot, doar numărarea voturilor se face folosind un sistem electronic. Tot restul se realizează prin metodele tradiționale: alegătorul intră în cabina de vot cu un buletin de vot de hârtie, își marchează alegerea pe buletinul de vot și, la final, introduce buletinul de vot în urnă.

Mașini de vot electronice care funcționează cu hârtie: în acest tip de vot, buletinul de vot cu opțiunea alegătorului este produs de o mașină de vot electronică. Aceasta înseamnă că alegătorul intra în cabina de vot unde găsește o mașină de vot electronica pe care o folosește pentru a face alegerea dorită. Mașina de vot generează un buletin de vot având marcata opțiunea alegătorului. Alegătorul ia buletinul de vot generat de mașina de vot și îl introduce în urnă. Urna poate fi o urna clasică, care stochează buletinele de vot până la încheierea scrutinului și al cărui conținut este numărat în mod tradițional, de către oameni. Totuși, de obicei rostul folosirii unei mașini de vot electronice care generează un buletin de vot este ca acest buletin de vot să poată fi ușor de interpretat în mod automat de către un alt sistem electronic. Așadar, o variație a acestui tip de vot folosește scannere, cu diverse nivele de automatizare, pentru scanarea buletinelor de vot și raportarea rezultatului numărătorii, buletinele de vot fiind păstrate pentru eventuale verificări.

Mașini de vot electronice cu înregistrare directă (*Direct-recording electronic* - *DRE* - *voting machines* în lb. engleză): acest tip de vot este pasul următor de la metoda precedentă. În acest tip de vot, alegătorul intra în cabina de vot unde găsește o mașină de vot electronica, la fel ca în cazul precedent, doar că în cazul mașinilor de vot DRE, mașina de vot înregistrează opțiunea alegătorului

1 Întreaga secțiune preluată din *O trecere în revistă a sistemelor de vot electronic folosite în lume*, 28 Mai 2015, http://apti.ro/votul-electronic-in-lume

și contorizează direct, pe cale electronică, alegerea făcută. Nu se mai generează nici un buletin de vot și nu se mai folosește o urnă. Pentru a putea verifica corectitudinea înregistrării votului, atât de către alegător cât și de organizatori în ipoteza unei renumărări, mașinile de vot DRE pot avea implementat un sistem de verificare de către alegător pe baza unei urme de audit pe hârtie (în engleză: *voter verification paper audit trail - VVPAT*). Deși exista multiple moduri de implementare a unui sistem VVPAT, toate se bazează pe imprimarea pe hârtie a opțiunii alegătorului și stocarea acestei hârtii pentru a putea fi făcute eventuale renumărări.

Ce trebuie observat aici este ca un sistem DRE cu VVPAT este identic din punct de vedere funcțional cu un sistem bazat pe mașini de vot electronice care funcționează cu hârtie care este cuplat cu un sistem de numărare automată pentru ca ambele numără voturile în mod automat și ambele produc o urma de audit pe hârtie.

Vot la distanța online/pe Internet: în acest tip de vot, alegătorul nu mai trebuie să meargă la cabina de bot pentru a vota, ci-și poate face alegerea folosind orice dispozitiv care se poate conecta printr-o rețea publica la sistemul de vot online care primește și contorizează opțiunile alegătorilor.

2. Adoptarea și abandonul sistemelor de vot electronic în lume

La nivel internațional, situația privind adoptarea diverselor tipuri de sisteme de vot electronic este fluidă. În funcție de cum este privită problema și cum sunt alcătuite diversele statistici poate părea că votul electronic are o răspândire mai mare decât în realitate. Motivul pentru aceasta este că multe state au cochetat cu ideea, începând de la discuții, trecând prin diverse soluții de test mai reduse sau mai ample și terminând cu adoptarea votului electronic doar pentru anumite categorii de cetățeni sau doar la nivel local/regional. Din acest motiv, am selecționat 16 state reprezentative fie prin istoria lor când vine vorba de implementarea democrației, fie prin adoptarea unor soluții radicale când vine vorba de sisteme de vot electronic. Acestea sunt: Australia, Belgia, Brazilia, Canada, Elveția, Estonia, Finlanda, Franța, Germania, Irlanda, India, Marea Britanie, Norvegia, Olanda, Statele Unite ale Americii și Suedia.

Să facem o scurtă trecere în revistă a folosirii votului electronic în aceste țări[2]:

a) Australia – Au fost desfășurate teste începând din 2001[3]. La nivel federal a fost respinsă folosirea votului electronic în 2014[4][5][6]. La nivel regional, în statul New South Wales a adoptat folosirea unui sistem de vot electronic bazat pe mașini de vot începând cu 2007[7] și un sistem de vot la distanță pe Internet începând cu 2010[8].
b) Belgia – Una dintre primele țări care au introdus un sistem de vot electronic. Introducerea

2 Pentru mai multe detalii, vezi *O trecere în revistă a sistemelor de vot electronic folosite în lume*, 28 Mai 2015, http://apti.ro/votul-electronic-in-lume

3 *2001 System Review Executive Summary*, 19 Iun 2002, http://www.elections.act.gov.au/elections_and_voting/electronic_voting_and_counting/2001_system_review_executive_summary

4 *Australia rejects electronic voting - are US elections rigged?*, 20 Noi 2014, http://www.itwire.com/government-tech-news/govenrment-tech-policy/66192-australia-rejects-electronic-voting-are-us-elections-rigged

5 *Interim Report*, 9 Mai 2014, http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Interim_Report

6 *Final Report*, 2015, http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Electoral_Matters/2013_General_Election/Final_Report

7 *Blind and visually impaired will be able to cast secret ballots*, 15 Aug 2007, http://www.abc.net.au/worldtoday/content/2007/s2005681.htm

8 *i-Voting system sought for NSW elections*, 21 Iun 2010, http://www.zdnet.com/article/i-voting-system-sought-for-nsw-elections/

acestuia a avut loc în 1991[9]. Implementarea sistemului crescut până în 1999, când a ajuns la 44% din utilizatori și s-a stabilizat la acest nivel. Belgia folosește un sistem de vot electronic cu mașini bazate pe hârtie și numărătoare electronică.

c) Brazilia – Una dintre cele 3 țări care folosesc votul electronic la nivel național. Introducerea acestuia a avut loc în 1996[10]. Brazilia folosește un sistem de vot electronic cu mașini de vot electronic cu înregistrare directă și fără urmă de audit pe hârtie. În 2009 a fost adoptată o lege care obliga la implementarea unui sistem care să producă urmă de audit pe hârtie, dar în 2011, *Curtea Supremă a Braziliei* a suspendat implementarea acestui sistem[11].
d) Canada – La nivel național, nu este folosit votul electronic. *Elections Canada*, autoritatea electorală permanentă din Canada a publicat în 2010 un studiu comparativ[12] pe tema sistemelor de vot electronic folosite în Europa și America de Nord, studiul având o poziție ambivalentă față de oportunitatea implementării votului electronic. La nivelul provinciilor, situația variază de la provincie la provincie și chiar de la localitate la localitate. La acest nivel au fost produse o serie de rapoarte foarte critice la adresa votului electronic[13][14].
e) Elveția – Au fost desfășurate teste începând cu 2004[15]. Testele au început în cantoanele Geneva (2004), Neuchâtel (2005) și Zürich (2005) și au evoluat pornind de la aceste prime 3 sisteme implementate în cantoanele menționate. În 2008 a fost introdus pentru prima dată votul la distanță pe Internet iar în 2014 acest tip de vot a devenit disponibil pentru toți cetățenii aflați în afara țării[16].
f) Estonia – A doua dintre cele 3 țări care folosesc votul electronic la nivel național și singura țară din lume care folosește votul pe Internet la nivel național. Estonia este autoarea mai multor premiere mondiale în acest domeniu: în 2005 a devenit prima țară care a folosit la nivel național votul pe Internet cu ocazia alegerilor locale iar în 2007 a devenit prima țară care a folosit la nivel național votul pe Internet cu ocazia alegerilor generale[17].
g) Finlanda – A fost desfășurat un test în 2008 cu ocazia alegerilor locale din 3 orașe[18]. A fost folosit un sistem de vot electronic cu mașini de vot electronice cu înregistrare directă și fără urmă de audit pe hârtie. 232 de alegători s-au lovit de o problemă de utilizabilitate din cauza căreia voturile lor nu au fost contorizate. Ca rezultat, *Curtea Supremă Administrativă din Finlanda* a ordonat reorganizarea alegerilor în acele 3 orașe.
h) Franța – Este folosit votul pe Internet doar pentru cetățenii din afara țării.[19]
i) Germania – A fost folosit un sistem de vot electronic cu mașini de vot electronice cu înregistrare directă și fără urmă de audit pe hârtie din 1999 până în 2008. În 2008, *Curtea Constituțională a Germaniei* a declarat respectivul sistem de vot electronic neconstituțional, punând astfel capăt votului electronic în Germania[20].
j) India – Ultima dintre cele 3 țări care folosesc votul electronic la nivel național. La fel ca Brazilia, India folosește un sistem de vot electronic cu mașini de vot electronic cu

---

9 *Electronic Voting in Belgium Past and Future*, 7 Dec 2010, http://homes.esat.kuleuven.be/~decockd/slides/electronic.voting.in.belgium.past.and.future.20101207.pdf
10 *Case Study Report on Brazil Electronic Voting: 1996 to Present*, https://www.ndi.org/files/4_Brazil.pdf
11 *Printed vote*, http://english.tse.jus.br/electronic-voting/printed-vote
12 *Comparative Assessment of Central Electoral Agencies*, Mai 2014, http://www.elections.ca/content.aspx?section=res&dir=rec/tech/comp&document=index&lang=e
13 *British Columbia Independent Panel on Internet Voting: Recommendations Report to the Legislative Assembly of British Columbia*, Feb 2014, http://www.internetvotingpanel.ca/docs/recommendations-report.pdf
14 *City of Toronto RFP #3405-13-3197: Internet Voting for Persons with Disabilities - Security Assessment of Vendor Proposals*, 14 Feb 2014, https://s3.amazonaws.com/s3.documentcloud.org/documents/1310860/toronto-internet-voting-security-report.pdf
15 *Key dates*, http://www.bk.admin.ch/themen/pore/evoting/00774/index.html?lang=en
16 *E-voting*, https://www.ch.ch/en/online-voting/
17 http://www.vvk.ee/voting-methods-in-estonia/engindex/reports-about-internet-voting-in-estonia/
18 *A Report on the Finnish E-Voting Pilot*, 29 Nov 2009, https://effi.org/system/files?file=FinnishEVotingCoEComparison_Effi_20080801.pdf
19 https://vimeo.com/49293923
20 https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2009/03/cs20090303_2bvc000307en.html

înregistrare directă și fără urmă de audit pe hârtie[21]. În 2012, *Comisia Electorală a Indiei* a decis asupra introducerii unui sistem care să producă urmă de audit pe hârtie[22].

k) Irlanda – A fost desfășurat un test în 2002. A fost folosit un sistem de vot electronic cu mașini de vot electronice cu înregistrare directă și fără urmă de audit pe hârtie. În 2009 a fost decisă renunțarea la votul electronic[23] iar în 2010 a fost decisă casarea mașinilor de vot achiziționate[24].

l) Marea Britanie – Au fost desfășurate mai multe teste ale unor sisteme de vot electronic de diverse tipuri, de la sisteme bazate pe mașini de vot electronice care funcționează cu hârtie combinate cu numărare electronică, la sisteme bazate pe mașini de vot cu înregistrare automată și la sisteme de vot la distanță pe Internet, în funcție de circumscripție. După o serie de rapoarte foarte critice apărute ca rezultat al alegerilor din Anglia și Scoția din 2007[25] și al alegerilor locale din Londra din 2008[26], ideea votului electronic a fost abandonată la nivel național[27]. La nivel local, Londra a folosit, din nou, în 2012, un sistem de numărare electronică[28].

m) Norvegia – Au fost desfășurate mai multe test al unui sistem de vot la distanță pe Internet începând din 2008[29]. În 2014, Norvegia a pus capăt acestor test, punând astfel capăt și votului electronic în Norvegia[30].

n) Olanda – Alături de Belgia, una dinte primele țări care au introdus un sistem de vot electronic. A fost folosit un sistem de vot electronic cu mașini de vot electronice cu înregistrare directă și fără urmă de audit pe hârtie. După scandalul din jurul mașinilor de vot la alegerile generale din 2006, în 2007, Olanda a renunțat la votul electronic[31].

o) Statele Unite ale Americii – Au fost, și sunt folosite în continuare, o multitudine de sisteme de vot electronic, în funcție de circumscripție. În 2000, cu ocazia alegerilor preliminare pentru candidatul partidului Democrat din Arizona a avut loc primul vot pe Internet din lume[32]. De asemenea, și scandalurile s-au ținut lanț, cele mai cunoscute fiind cele privind notoriile mașini de vot *Diebold*.

p) Suedia – Suedia nu a implementat niciodată un sistem de vot electronic, dar subiectul votului electronic a tot fost dezbătut de mai mult de 10 ani[33].

---

21 http://eci.nic.in/eci_main1/evm.aspx

22 *New EVMs to have paper trail*, 20 Ian 2012, http://timesofindia.indiatimes.com/india/New-EVMs-to-have-paper-trail/articleshow/11561762.cms

23 *Electronic voting system to be scrapped*, 23 Apr 2009, http://www.rte.ie/news/2009/0423/116606-evoting/

24 *E-voting machines to be disposed of*, 6 Oct 2010, https://www.irishtimes.com/news/e-voting-machines-to-be-disposed-of-1.865193

25 *May 2007 Election Report - Findings of the Open Rights Group Election Observation Mission in Scotland and England*, 20 Iun 2007, https://www.openrightsgroup.org/campaigns/e-voting/e-voting-2007/e-voting-main

26 *May 2008 Election Report - Findings of the Open Rights Group Election Observation Mission in London*, 2 Iul, 2008, https://www.openrightsgroup.org/wp-content/uploads/orglondonelectionsreport.pdf

27 *E-voting*, https://www.openrightsgroup.org/ourwork/successes/evoting

28 *Electronic Counting*, https://www.openrightsgroup.org/issues/e-counting

29 http://aceproject.org/ace-en/focus/e-voting/countries

30 *Internet voting pilot to be discontinued*, 25 Iun 2014, https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/

31 *Dutch pull the plug on e-voting*, 1 Oct 2007, http://www.theregister.co.uk/2007/10/01/dutch_pull_plug_on_evoting/

32 *Arizona Democratic Party Selects Votation.com to Hold World's First Legally-Binding Public Election Over the Internet*., 16 Dec 1999, http://www.thefreelibrary.com/Arizona+Democratic+Party+Selects+Votation.com+to+Hold+World's+First...-a058272337

33 http://www.governments-online.org/documents/InternetVotingSweden.pdf

	Considerat / Folosit în trecut	*Teste / Utilizare parțială*	*Utilizare universală*	***Total (în funcţie de tip)***
Mașini bazate pe hârtie + numărare electronică sau mașini de vot cu înregistrare directă cu urmă de audit pe hârtie		1 (6.25%) Belgia		1 (6.25%)
Mașini de vot cu înregistrare directă fără urmă de audit pe hârtie	4 (25%) Finlanda, Germania, Irlanda, Olanda		2 (12.5%) Brazilia, India	6 (37.5%)
Vot pe Internet	2 (12.5%) Norvegia, Suedia	1 (6.25%) Franța	1 (6.25%) Estonia	4 (25%)
Amestec de mai multe tipuri de sisteme de vot electronic		5 (31.25%) Australia, Canada, Elveția, Marea Britanie, Statele Unite ale Americii		5 (31.25%)
Total (în funcţie de utilizare)	6 (37.5%)	7 (43.75%)	3 (18.75%)	

Tabelul 1. Statistica folosirii sistemelor de vot electronic în funcție de tipul de sistem folosit și de amploarea folosirii respectivelor sisteme de vot electronic

3. Problemele sistemelor de vot electronic

Ținând cont de ce am văzut până aici, se pune, în mod firesc, problema „Dar de ce au renunțat atât de mulți la votul electronic, de tot sau aproape de tot?”. Foarte pe scurt, răspunsul la acestă întrebare este „Pentru că beneficiile au fost mult supraevaluate iar problemele au fost mult subestimate, dacă nu total ignorate.” Să vedem acum răspunsul detaliat.

3.1. *Probleme conceptuale*

Votul electronic prezintă probleme încă de la nivel de concept, indiferent sau aproape indiferent de detaliile de implementare sau de operare ale unui astfel de sistem. Cele mai semnificative astfel de probleme sunt:

a) <u>lipsa abilității de a verifica sistemul</u>: Într-un sistem de vot electronic, este foarte dificil, dacă nu de-a dreptul imposibil, în funcție de modul de implementare al sistemului, să fie reverificate rezultatele de la un capăt la celălalt. În cazul sistemului de vot pe hârtie, rezultatele pot fi verificate pentru că buletinele de vot sunt păstrate și pot fi oricând renumărate. Într-un sistem de vot electronic, în funcție de tipul de sistem, s-ar putea să nici nu existe o manifestare fizică a buletinelor de vot. Acest lucru este adevărat în cazul sistemelor de vot electronic cu mașini de vot electronice cu înregistrare directă și fără urmă de audit pe hârtie sau în cazul celor de vot pe Internet. În cazul acestor sisteme, trebuie ca alegătorii să aibă încredere oarbă în faptul că datele stocate în format electronic nu vor fi modificate în mod abuziv iar organizatorii nu sunt în măsură să efectueze renumărări pentru că singurele înregistrări rămase în urma votului sunt cele electronice, care pot fi manipulate

fără a lăsa urme. Chiar și în cazul unui sistem de electronic cu mașini de vot electronice cu înregistrare directă și cu urmă de audit pe hârtie, alegătorii nu au nici un mod de a verifica dacă alegerea făcută și imprimată pe hârtie este în concordanță cu alegerea înregistrată de mașina de vot. La fel, chiar și în cazul celui mai simplu sistem de vot electronic, cel bazat pe numărarea electronică, alegătorii nu au nici un mod de a verifica dacă alegerea făcută este în concordanță cu ce înregistrează mașina care scaneaza buletinul de vot. În aceste ultime două cazuri, organizatorii pot fac renumărări manuale pentru a constata dacă rezultatele contorizare automat corespund celor contorizate automat. Dar dacă acest lucru nu este făcut, și, de obicei nu se face pentru că s-ar pierde beneficiile aduse de contorizarea automată, atunci urma de audit pe hârtie este utilă doar din punct de vedere teoretic dar fără vreo utilitate practică.

b) lipsa abilității de a observa sistemul: Problema complementară lipsei de verificabilitate este lipsa de observabilitate. Lipsa de verificabilitate îi afectează pe alegători și pe cei care ar dori renumărarea voturilor. Lipsa de observabilitate îi afectează pe observatorii procesului electoral. Un sistem de vot electronic este, prin excelență, inobservabil. În cazul sistemelor de vot electronic, observatorii pot observa procedurile administrării sistemului, și, în anumite cazuri destul de limitate, pot audita codul sursa al programelor sistemului de vot electronic. Dar dincolo de asta, observarea sistemului este mult mai limitată pentru că observatorii pot vedea doar ce le permite sistemul să vadă, iar ceea ce le permite sistemul să vadă nu poate fi garantat în nici un fel că este conform cu ceea ce se întâmplă în realitate.

c) nesiguranța arhitecturală a sistemului de vot electronic: Sistemul de vot clasic este un sistem distribuit. Dacă votul este compromis într-o locație, această problemă este izolată în respectiva locație dată fiind natura distribuită a sistemului. Sistemele de vot electronic, în funcție de implementare, pot fi mai mult sau mai puțin centralizate. De cele mai multe ori, totuși, acestea sunt sisteme foarte centralizate, toate dispozitivele care contorizează voturi fiind conectate prin rețea la un sistem central de servere. Asta înseamnă că dacă respectivul sistem central este compromis, întregul scrutin este compromis, nu doar o locație anume. După cum vom vedea mai târziu, când vot discuta despre prolemele tehnice, șansele de compromitere a unui sistem de vot electronic sunt foarte mari. Mai mult decât atât, dacă atacul este suficient de sofisticat, exista riscul ca această viciere a rezultatelor nici măcar sa nu fie detectată, ceea ce amplifică pericolul.

d) compromiterea secretului votului: Aceasta este o problemă care apare doar în cazul sistemelor de vot electronic la distanță pe Internet. Totuși, în acest caz, aceasta poate fi considerată una dintre cele mai mari probleme pentru că, ținând cont de lipsa de verificabilitate și de observabilitate a oricărui sistem de vot electronic, alegătorul nu poate avea nici o garanție că sistemul nu compromite secretul votului. Pentru un vot liber, garantarea secretului votului este absolut esențială. Mai mult decât atât, *Convenția Internațională cu privire la Drepturile Civile și Politice*[34][35], care face parte din *Carta Internațională a Drepturilor Omului*, la care România este semnatară, stipulează, în mod clar, prin Articolul 25(2) că *„Orice cetățean are dreptul și posibilitatea, fără nici una dintre discriminările la care se refera art. 2 și fără restricții nerezonabile de a alege și de a fi ales, în cadrul unor alegeri periodice, oneste, cu sufragiu universal și egal și cu* ***scrutin secret****, asigurând exprimarea libera a voinței alegătorilor."* Așadar secretul votului este un drept fundamental, iar votul pe Internet nu poate garanta acest drept fundamental.

3.2. *Probleme operaționale*

A doua categorie de probleme se referă la problemele care apar ca urmare pregătirii defectuoase sau a operării defectuoase a unui sistem de vot electronic, chiar și unul care, drept exercițiu de gândire

34 *International Covenant on Civil and Political Rights*, www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.asp

35 *Conventia internationala cu privire la drepturile civile si politice*, http://www.oportunitatiegale.ro/pdf_files/Coventia%20internationala%20drepturi%20civile%20si%20politice.pdf

pur teoretic, ar putea fi considerat perfect din punct de vedere tehnic.

a) probleme cu pregătirea sistemului: În foarte multe cazuri, operatorii sistemelor de vot electronic refuză auditarea independentă a acestora, iar când permit auditări independente, auditorilor le sunt impuse constrângeri care nu le permit să efectueze auditări relevante ale respectivelor sisteme. Un exemplu foarte relevant, în această privință, este cazul Braziliei: codul sursă al software-ului care rulează pe mașinile de vot nu este public și potențialii auditori întâmpină dificultăți în a obține orice fel de acces la acesta[36]: *„TSE își rezervă autoritatea finală asupra codului sursă, astfel încât nici o autoritate externă nu a certificat codul folosit în 1996 sau în alegerile ulterioare. Legea electorală cere ca TSE să pună codul sursa final la dispoziția partidelor politice și, după 2003, baroului (Ordem dos Advogados do Brasil - OAB), cu 120 de zile înaintea alegerilor. Activiști și mediul universitar spun ca TSE nu au respectat aceste cerințe cu ocazia alegerilor din 1996, 1998 și 2000. După 2000, în urma creșterii interesului asupra sistemului, TSE a început să permită analizarea codului sursă de către actori externi, dar interviuri cu activiști și asistenți parlamentari indică faptul că doar doua partide – PDT și Partidul Muncitoresc (Partido dos Trabalhadores or PT) – au participat în mod regulat la auditarea sistemului. PDT obișnuiește să aibă informaticieni afiliați cu partidul care să examineze codul sursă, în timp ce PT angajează o companie externă pentru acest lucru. Înainte de alegerile din 2004 baroul a depus un efort semnificativ și a cheltuit sume însemnate de bani pentru a audita codul sursa, angajând o companie externă și examinând software-ul din diverse state, dar de atunci a făcut doar auditări minimale din cauza costurilor și a lipsei unei capabilități interne în acest sens. Există critici din partea societății civile și a experților în informatică vis-a-vis de acest proces de auditare. Informaticienii critică faptul că auditorii trebuie să semneze contracte de confidențialitate și, prin urmare, orice probleme descoperite în decursul auditului nu pot fi făcute publice. Auditorii mai atrag atenția și asuprea faptului că doar câteva zile sunt puse la dispoziție pentru audit iar examinarea codului se face în condiții strict controlate pe calculatoarele TSE-ului, ceea ce este insuficient pentru o examinare cuprinzătoare a codului."* (*Raport de studiu de caz asupra Votului Electronic în Brazilia: din 1996 până în prezent*, paginile 245-246). Există probleme și mai mari de atât. Din același raport: *„Mediul universitar și baroul au raportat și că au existat cazuri în care codul a fost modificat după ce a fost pus la dispoziția auditorilor, ceea ce înseamnă că auditorii nu au auditat versiunea finală a codului. TSE a pretins că a fost necesar să fie făcute modificări din motive tehnice, dar nu a explicat în ce au constat aceste modificări."* (pagina 246, paragraful 2). Din păcate, problemele nu se opresc aici. Același raport relatează cum cercetătorilor care, zică-se, au fost autorizați să auditeze sistemul în 2009, nu li s-a permis accesul la codul sursă al mașinilor de vot, iar celor cărora le-a fost dat acces la sistem în 2012, li s-a dat acces doar pentru 3 zile și doar de la 4 calculatoare care nu aveau disponibile nici măcar instrumente elementare de lucru. Un alt exemplu este cel al Finlandei, unde, înainte de testul care a avut loc în 2008, autoritățile au refuzat să dezvăluie informații despre sistemul de vot electronic. Când, în sfârșit, a fost organizat un audit, organizației *Effi (Electronic Frontier Finland)*, care este o organizație neguvernamentală având ca domeniu de interes protejarea drepturilor digitale, nu i-a fost permis accesul, iar compania finlandeză care a avut rolul de integrator de sistem a cerut participanților la audit să semneze contracte de confidențialitate care limitau în mod drastic abilitatea auditorilor de a comunica problemele descoperite.
b) probleme cu operarea sistemului: În această privință, cel mai relevant exemplu este cel al sistemului de vot electronic din Estonia. Raportul[37] produs de o echipă de internațională de experți independenți care au participat ca observatori acreditați la alegerile din 2013 relatează o lungă serie de lipsuri în securizarea operațională și controale procedurale

36 *Case Study Report on Brazil Electronic Voting: 1996 to Present*, https://www.ndi.org/files/4_Brazil.pdf
37 https://estoniaevoting.org/

inadecvate. Iată un citat din sumarul executiv al raportului menționat: *„Observarea modului în care sistemul de I-vot a fost administrat de organizatori a scos în evidență o lipsă de proceduri adecvate atât pentru operațiunile curente, de zi cu zi, cât și pentru tratarea evenimentelor anormale. Aceasta creează oportunități pentru apariția de atacuri și erori și îngreunează munca auditorilor atunci când este vorba de a determina dacă s-au luat măsurile corecte. O analiză îndeaproape a înregistrărilor video publicate de organizatori relevă numeroase neglijențe chiar și când vine vorba de cele mai elementare practici de securitate*[38]*. Aceste înregistrări arată lucrători care descarcă programe esențiale folosind conexiuni la Internet nesecurizate, care scriu parole și coduri PIN secrete în văzul camerelor și care pregătesc programele de de vot pentru distribuție către public pe calculatoare personale nesecurizate, printre altele. Acestea indica un nivel periculos de inadecvat de profesionalism în securitatea administrării sistemului care expune întregul sistem atacurilor și manipulării.”*

3.3. *Probleme tehnice*

În sfârșit, categoria cea mai însemnata de probleme: cele tehnice. Orice expert în securitate informatică va spune că nu există, și nici nu va exista prea curând, vreun sistem informatic care să nu aibă probleme. În cel mai bun caz, nu va avea probleme mari și/sau evidente, dar cu siguranţa le va avea. Un mod foarte plastic prin care este descrisa această problemă este că „singurul calculator în siguranța este unul neconectat la vreo rețea... și care e oprit... și încuiat într-un seif... care se odihnește pe fundul oceanului”. Cu cât un sistem este mai complex, cu atât există mai multe oportunități de apariție a problemelor. Așadar, un sistem de vot electronic, care este prin excelența un sistem foarte complex, nu are cum să fie un sistem sigur.

Aceasta este prima parte a ecuației, cea privitoare la nesiguranța intrinsecă atât de complex ca un sistem de vot electronic, în special dacă ne referim la un sistem de vot pe Internet. Cea de-a doua parte, de care sunt conștienți chiar și mai puțini, este cea a modelului de amenințare căruia trebuie să-i facă față un astfel de sistem. În ultima vreme, războiul cibernetic a căpătat o altă amploare, câteva exemple fiind spionajul chinez împotriva companiilor americane[39], sabotajul american al mașinilor de centrifugare nucleare iraniene[40] sau atacurile britanice asupra unor companii de telecomunicații europene[41]. Un număr din ce în ce mai mare posedă capabilități ofensive de securitate informatică[42] iar investițiile în aceste capabilități cresc cu o viteză alarmantă prin toate mijloacele existente[43]. În aceste condiții, trebuie considerat că un atacator are capacitatea de a obține informații detaliate despre sistemul de vot din diverse surse, cum ar fi cod sursa publicat, inginerie inversă sau orice altă cale. De asemenea, este ușor de presupus că un astfel de atacator are acces facil la suficiente resurse umane și materiale pentru a organiza și executa într-un interval scurt de timp un atac încununat de succes. Când vine vorba de atacuri asupra calculatoarelor alegătorilor, este ușor de presupus că un atacator cu resurse suficiente poate obține foarte ușor accesul la rețele de boți ori de pe piață or dezvoltându-și singur această capabilitate. Raportul anual din 2014[44] al unei mari firme de securitate informatică prezintă o rată de infecție globala cu orice fel de malware de peste 30% din toate calculatoarele (30,42% ca să fim mai exacți). În aceste circumstanțe,

38 https://estoniaevoting.org/photos

39 *APT1 - Exposing One of China’s Cyber Espionage Units*, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

40 *Obama Order Sped Up Wave of Cyberattacks Against Iran*, 1 Iun 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

41 *GCHQ: EU surveillance hearing is told of huge cyber-attack on Belgian firm*, 3 Oct 2013, http://www.theguardian.com/uk-news/2013/oct/03/gchq-eu-surveillance-cyber-attack-belgian

42 *EU nations developing cyber 'capabilities' to infiltrate government, private targets*, 12 Dec 2013, http://www.euractiv.com/infosociety/eu-nations-lack-common-approach-news-532294

43 *Hacking Summit Names Nations With Cyberwarfare Capabilities*, 3 Oct 2013, https://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities

44 http://www.pandasecurity.com/mediacenter/reports/

integritatea calculatoarelor alegătorilor nu este, nici pe departe, garantată. Nu în ultimul rând, dacă presupunem că un atacator nu ar putea să obțină acces la malware-uri deja existente de pe calculatoarele alegătorilor, există întotdeauna alternativa folosirii înfloritoarei piețe de exploit-uri de ziua zero[45]. Așadar, atacurile cărora un sistem de vot pe Internet trebuie să facă față sunt cele care vin din partea unor atacatori sofisticați cum ar fi un stat, o organizație criminală bine finanțată sau o persoană rău-intenționată din interiorul organizației care organizează alegerile.

Din păcate, sistemele de vot electronic contemporane nu pot face față nici unor atacuri din partea unor atacatori cu resurse mult mai limitate. De exemplu, sistemele de vot care au fost folosite în Finlanda, Germania, Irlanda și Olanda erau fabricate de același producător iar un grup de cercetători în securitate informatică au reușit să demonstreze[46] cât de nesigure sunt, acesta fiind catalistul pentru retragerea din folosința a acestui sistem din Olanda. Un alt grup de cercetători au demonstrat cât de nesigur este sistemul de vot electronic din India[47][48]. La fel s-a întâmplat și în cazul sistemului de vot pe Internet folosit în statul New South Wales din Australia[49]. Exemplele ar putea pot continua dar ne vom opri aici. Ce este important de reținut este ca este dovedit faptul că sistemele de vot electronic nu sunt în măsură să facă față unor atacatori cu resurse limitate, dar atacurile cărora este esențial să le facă față vor veni din partea unor atacatori cu resurse virtual nelimitate, iar când aceste atacuri, inevitabil, vor veni, sistemele de vot electronic nu au nici o șansă să le facă față.

3.4. *Lipsa beneficiilor*

Dincolo de problemele de toate felurile, sistemele de vot electronic nici măcar nu aduc beneficiile scontate. Oricum, secretul votului, integritatea votului, siguranța votului etc. sunt mult mai importante decât prezența la vot și costul votului, dar chiar și așa, dacă am face abstracție de pericolele pe care votul electronic le introduce, beneficiile scontate se dovedesc că nu au un fundament în realitate. Multiple studii au demonstrat că nici prezența la vot nu a crescut odată cu introducerea votului electronic pe Internet și nici costurile organizării alegerilor nu au scăzut.

Studii din Canada[50], Elveția[51] și Norvegia[52], împreună cu statisticile alegerilor din Estonia[53], arată ca participarea la vot a rămas la același nivel după introducerea votului electronic pe Internet, variațiile fiind în marja de eroare a oricărui studiu statistic.

De asemenea, același studiu canadian menționat mai sus, împreună cu ceea ce a fost observat cu ocazia alegerilor din Londra, din 2008, arată că votul electronic nu scade nici costurile organizării alegerilor. Mai exact, în 2008, la Londra, costul numărării electronice a fost cu 1,5 milioane de lire mai mare[54] decât ar fi fost dacă s-ar fi făcut o numărare manuală, iar aceste 1,5 milioane de lire trebuiesc raportate la costul total de 4,5 milioane de lire[55] al scrutinului respectiv, ceea ce înseamnă un cost cu %50 mai mare în cazul folosirii sistemului de numărare automată.

---

45 *Shopping For Zero-Days: A Price List For Hackers' Secret Software Exploits*, 23 Mar 2012, http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

46 http://www.wijvertrouwenstemcomputersniet.nl/images/9/91/Es3b-en.pdf

47 https://jhalderm.com/pub/papers/evm-ccs10.pdf

48 https://indiaevm.org/evm_tr2010-jul29.pdf

49 http://arxiv.org/abs/1504.05646

50 *British Columbia Independent Panel on Internet Voting: Recommendations Report to the Legislative Assembly of British Columbia*, Feb 2014, http://www.internetvotingpanel.ca/docs/recommendations-report.pdf

51 *Three Case Studies from Switzerland: E-Voting*, Mar 2009, http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Gerlach-Gasser_SwissCases_Evoting.pdf

52 *English summary - Chapter 2: Voter turnout and the use of internet voting*, https://www.regjeringen.no/globalassets/upload/kmd/komm/rapporter/isf_internettvalg_english-summary.pdf

53 *Statistics about Internet Voting in Estonia*, http://www.vvk.ee/voting-methods-in-estonia/engindex/statistics

54 https://www.openrightsgroup.org/ourwork/reports/response-to-london-elects-manual-count-vs-electronic-count-cost-benefit-analysis

55 http://www.theyworkforyou.com/wrans/?id=2008-11-26j.233950.h

Singurul beneficiu ale votului electronic este înlesnirea exercitării dreptului la vot pentru anumite categorii de persoane cu dizabilități, în anumite situații.

4. Concluzii și recomandări

Ținând cont de pericolele grave pe care le creează votul electronic, în general, și votul pe Internet, în particular, alegerile putând fii furate sau îngreunate, cât și lipsei aproape totale de beneficii reale, recomandarea noastră este ca ideea adoptării votului electronic să fie abandonată în întregime.

Această concluzie este bazată pe nivelul tehnologiei disponibile la momentul actual. Nu putem prevede ce tehnologii vor apărea în viitor, dar nivelul actual de dezvoltare a tehnologiei nu permite implementarea în siguranța și cu asigurarea tuturor cerințelor, cum ar fi cea de vot secret, a votului electronic.