

CARNET

Elektroničko glasovanje

CERT.hr-PUBDOC-2019-5-380

Sadržaj

1	UVOD	3
2	ŠTO JE GLASOVANJE	4
2.1	TRANSPARENTNOST	4
2.2	TAJNOST	4
2.3	ANONIMNOST	4
2.4	NEDOKAZIVOST.....	4
2.5	INTEGRITET.....	4
3	ŠTO JE ELEKTRONIČKO GLASOVANJE	6
4	VRSTE ELEKTRONIČKOG GLASOVANJA	7
5	GLASOVANJE PUTEM INTERNETA	8
5.1	POVEĆANJE IZLAZNOSTI	8
5.2	SIGURNOST.....	8
5.3	TRANSPARENTNOST	11
6	ZAKLJUČAK	12
7	LITERATURA	13

Ovaj dokument izradio je Laboratorij za sustave i signale Zavoda za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Ovaj dokument vlasništvo je Nacionalnog CERT-a. Namijenjen je javnoj objavi te se svatko smije njime koristiti i na njega se pozivati, ali isključivo u izvornom obliku, bez izmjena, uz obvezno navođenje izvora podataka. Korištenje ovog dokumenta protivno gornjim navodima povreda je autorskih prava CARNET-a, a sve navedeno u skladu je sa zakonskim odredbama Republike Hrvatske.

1 Uvod

Svi moderni demokratski sustavi temelje se prvenstveno na slobodnim i demokratskim izborima. Bez obzira govorimo li o izravnom izboru predsjednika, o izravnom biranju parlamentarnih predstavnika, biranju stranačkih i neovisnih lista ili nekom drugom mehanizmu izbora zastupnika, osnovna je zadaća izbora na ispravan i nedvojben način utvrditi slobodnu volju građana jer svaka vlast i autoritet proizlaze upravo iz naroda.

Napredak tehnologije omogućio je njeno prodiranje u gotovo sva područja ljudske djelatnosti, što je donijelo brojne i neupitne koristi ne samo za pojedince nego i za društvo u cjelini. Potaknuto velikim uspjesima tehnologije u najrazličitijim područjima, sve se češće postavlja pitanje modernizacije izbora i uvođenja nekog od oblika elektroničkog glasovanja. Kao najčešći argument zagovornika elektroničkog glasovanja navode se povećanje izlaznosti na izbore, čime bi se izbornim rezultatima dao veći legitimitet jer bi odražavali volju većeg dijela građana; omogućavanje glasovanja građanima koji iz nekog razloga nisu u mogućnosti osobno posjetiti izbornu mjesto ili iz zdravstvenih razloga nisu sposobni samostalno zaokružiti željenog kandidata na papirnatim listićima, čime bi se postigla veća ravnopravnost građana i zaštitilo njihovo pravo sudjelovanja u demokratskim izborima; a nezanemariva dobit bilo bi i znatno smanjenje troškova vezanih uz provedbu izbora, što u konačnici izravno ide u korist svim građanima kao poreznim obveznicima.

2 Što je glasovanje

Za razumijevanje elektroničkog glasovanja i ispravno vrednovanje njegovih različitih oblika nužno je prije svega razumjeti osnovne kriterije koje svaki sustav glasovanja mora zadovoljiti ako želi osigurati valjano izražavanje slobodne volje građana kroz rezultat glasovanja.

2.1 Transparentnost

Osnovni uvjet demokratskih izbora je transparentnost cjelokupnog izbornog procesa. Svaki od koraka mora biti lako razumljiv svim sudionicima izbora te podložan neovisnoj provjeri. Bez transparentnosti sudionici izbora gube povjerenje u izborni proces te se uvelike povećava rizik da izborni gubitnici neće prihvatiti rezultate izbora.

2.2 Tajnost

Kako bi se jamčila sloboda izbora, glasovanje prije svega mora biti tajno. Tajnost omogućuje izražavanje stvarne volje bez nadzora i bez utjecaja drugih osoba. Zbog toga se na glasačkim mjestima osiguravaju odvojene kabine, zaštitni paravani ili drugi mehanizmi kojima je cilj zaštita tajnosti glasovanja i onemogućavanje uvida u osobni izbor građanina. Izborna povjerenstva bilježi je li pojedini građanin pristupio glasovanju, ali nakon što je predan, glasački listić nije moguće ponovo izdvojiti i povezati s određenom osobom.

2.3 Anonimnost

Nužan uvjet slobode glasovanja je i anonimnost kojom se sprječava da drugi saznaju rezultat glasovanja pojedinog građanina. Glasački listići se ne potpisuju i ne sadrže identifikacijske oznake pomoću kojih bi se naknadno moglo utvrditi za koga je pojedini glasač glasovao tako da su građani slobodni glasovati i protiv opresivne vlasti bez bojazni od eventualnih negativnih posljedica.

2.4 Nedokazivost

Manje očigledan, ali jednako važan kriterij je i sprječavanje da pojedini glasač može naknadno dokazati za koga je glasovao. Naime, ako bi glasači nakon obavljenog glasovanja mogli dokazati za koga su točno glasovali, otvorio bi se prostor nedozvoljenim radnjama kao što su kupovanje glasova ili prisile glasača. Bez mogućnosti dokazivanja za koga su glasači doista glasovali, učinkovitost pokušaja kupovine glasova je uvelike smanjena te se svodi na puko nagovaranje bez mogućnosti provjere i bez garancije da su glasači doista ispoštovali dogovor.

2.5 Integritet

Osim navedenih kriterija, svaki izborni proces mora osigurati i niz drugih uvjeta kojima se jamči integritet izbora i valjanost rezultata. Većina zakona glasačko pravo ograničava na punoljetne, poslovno sposobne građane što znači da je prilikom glasovanja potrebno utvrditi identitet osobe, utvrditi njeno pravo pristupanju izbora, evidentirati sam izlazak

na izbore te spriječiti višestruko pristupanje glasovanju. Također je nužno nadzirati sam proces ispunjavanja i predavanja listića kako bi se spriječile eventualne manipulacije npr. ubacivanjem većeg broja listića i sl.

3 Što je elektroničko glasovanje

Elektroničko glasovanje širok je pojam koji obuhvaća više različitih sustava glasovanja, pri čemu je zajedničko svojstvo uporaba elektroničkih uređaja ili računala u barem nekoj od faza glasovanja. Elektronički sustavi glasovanja pojavili su se 1960-ih godina uvođenjem perforiranih kartica. Umjesto zaokruživanja željenog kandidata na glasačkom listiću, svaki glasač posebnim alatom na unaprijed pripremljenim karticama uklanja perforaciju uz željeni izbor, a po završetku glasovanja računalo opremljeno čitačem kartica prebrojava glasove i ispisuje rezultat.

Već iz ove prve implementacije elektroničkog glasovanja vidljivo je da uporaba elektroničkih uređaja donosi razne prednosti. Računalno prebrojavanje glasova znatno je brže, a zahtijeva manji broj zaposlenih osoba. Istovremeno, ako se ukaže potreba, perforirane je kartice naknadno moguće i ručno provjeriti.

Napredak tehnologije doveo je do razvoja različitih sustava elektroničkog glasovanja i omogućio brojne druge prednosti. Jedan od problema klasičnog papirnato glasovanja je svakako i izrada dovoljnog broja glasačkih listića te njihova odgovarajuća distribucija na birališta. Ovisno o izborima, listiće je ponekad potrebno tiskati na više jezika i osigurati dovoljan broj svake varijante listića na svakom biralištu. Budući da je izlaznost birača nepoznata, a svakom se biraču mora osigurati pravo glasa, potrebno je pripremiti više listića pri čemu znatan broj listića neće biti iskorišten. Ovaj financijski i logistički problem u potpunosti se zaobilazi primjenom sustava izravnog bilježenja glasova kao što su npr. sustavi sa zaslonima osjetljivima na dodir. Popis kandidata i sve relevantne informacije prikazane su na zaslonu, a nakon uspješnog odabira sustav bilježi rezultat i po potrebi ispisuje papirnatu potvrdu kojom glasač može provjeriti ispravnost.

Uporaba elektroničkih uređaja može uvelike poboljšati i dostupnost glasovanja osobama s invaliditetom. Veličina znakova na ekranu može se prilagoditi slabovidnim osobama, pretvaranjem teksta u govor i uporabom slušalica omogućuje se samostalno glasovanje i slijepim osobama, odabir pritiskom na dio zaslona olakšava glasovanje osobama ograničene pokretljivosti ili osobama koje nisu sposobne rabiti olovku. Svako uvođenje asistivne tehnologije u sustav glasovanja pohvalno je jer omogućava veću dostupnost glasovanja osobama s invaliditetom i osigurava im ustavom zajamčena prava.

Interaktivnost svojstvena elektroničkim sustavima i računalima pruža i iznimno korisnu mogućnost utvrđivanja stvarne volje glasača na kojoj počiva vjerodostojnost izbora. Na svakim izborima određen dio glasačkih listića proglašava se nevažećim bilo zato što je zaokružen veći broj kandidata od dopuštenoga, nije zaokružen niti jedan kandidat ili listić na neki drugi način ne odgovara propisima te iz njega nije moguće nedvojbeno utvrditi pravu volju glasača. Elektronički uređaji mogu glasaču pružiti neposrednu povratnu informaciju i upozoriti ga na neispravnost listića prije nego on bude bespovratno predan. Glasač tako može slobodno odlučiti želi li ispraviti pogrešku ili se radi o slobodnoj odluci predavanja nevažećeg listića čime glasač želi iskoristiti svoj glas, ali ga ne želi dati ni jednom od kandidata.

4 Vrste elektroničkog glasovanja

Po načinu glasanja, sustave elektroničkog glasovanja možemo podijeliti na sustave koji koriste papirnate listiće, sustave koji izravno bilježe glasove te sustave koji glasove prenose javnim mrežama.

Sustave elektroničkog glasovanja koji još uvijek koriste papirnate glasačke listiće karakterizira ručno ispunjavanje papirnatih listića uz korištenje tehnologije pri prebrojavanju glasova. Uz sustave s perforiranim karticama, prvi su se u uporabi pojavili sustavi s optičkim prepoznavanjem odabira (tzv. *marksense*). Ovi se sustavi već dugo uspješno koriste u automatiziranom ocjenjivanju standardiziranih testova kao što su npr. ispiti na fakultetima. Glasači bilježe svoj odabir na posebno predviđenom mjestu na listiću, obično zacrnjivanjem pravokutnika, kruga ili drugog predviđenog oblika uz svaki izbor. Sustav za optičko prepoznavanje zatim čita takav listić, može glasaču prikazati rezultat prepoznavanja i zatražiti potvrdu ispravnosti, te prosljeđuje glas za lokalno ili centralizirano prebrojavanje.

U ovu kategoriju spadaju i sustavi za elektroničko označavanje listića koji obično sadrže zaslon osjetljiv na dodir i razne asistivne tehnologije kojima se osobama s invaliditetom omogućava lakše ispunjavanje papirnatih glasačkih listića kao i sustavi temeljeni na digitalnoj olovci koja pomoću kamere u tijelu olovke prepoznaje glasačev odabir prilikom zaokruživanja listića.

Sustavi koji izravno elektronički bilježe glasove slični su sustavima za elektroničko označavanje listića time što najčešće koriste zaslon osjetljiv na dodir te omogućuju uporabu velikog broja asistivnih tehnologija. Ključna razlika je u tome što umjesto ispisivanja papirnato listića, glasačev izbor bilježe izravno u digitalnom obliku u memorijskim komponentama sustava. Po završetku glasovanja, sustav izravno proizvodi rezultat prebrojavanja glasova, bilježi ga na prijenosnu memoriju te ispisuje u papirnatom obliku. Temeljna prednosti ovih sustava su brzina prebrojavanja glasova, izbjegavanje troškova izrade i distribucije glasačkih listića te mogućnost korištenja asistivnih tehnologija. Temeljni nedostatak je relativna lakoća kojom se takvi uređaji mogu kompromitirati (1) i nemogućnost bilo kakvog nadzora ili ljudske provjere rezultata (2).

Sustavi koji glasove prenose javnim mrežama dijele sva svojstva sustava za izravno bilježenje glasova uz dodatak uporabe javnih mreža i interneta za prijenos glasova ili rezultata prebrojavanja glasova. Ovaj se prijenos može odvijati u stvarnom vremenu, u grupama glasova više puta u toku dana ili samo jednom nakon zatvaranja birališta. Samo glasovanje može se ograničiti na uređaje na biračkim mjestima, može uključivati telefonsko glasovanje, a može uključivati i glasovanje putem interneta pri kojem se rabe uređaji u vlasništvu birača.

5 Glasovanje putem interneta

Javna rasprava o elektroničkom glasovanju danas gotovo bez iznimke zapravo podrazumijeva glasovanje putem interneta. U želji da se što više potakne izlaznost građana na izbore, a ohrabreni nezaustavljivim prodorom tehnologije u sve pore društvenog života, mnogi zagovornici glasovanja putem interneta upravo u njemu vide rješenje mnogih problema, od znatno povećanog sudjelovanja građana u izborima do velikih novčanih ušteda u njihovoj provedbi.

Nekoliko država razmatralo je mogućnost glasovanja putem interneta i provelo ograničene pokuse u sklopu redovnih izbora, ali su svi pokušaji u konačnici odbačeni zbog sigurnosnih razloga. Jedina država koja u potpunosti omogućava glasovanje putem interneta je Estonija, koja je ovaj oblik glasovanja uvela pilot projektom na lokalnim izborima 2005. godine. Osim što je unikatan primjer u svijetu, Estonija je dobar kandidat za usporedbu s Hrvatskom i zbog svoje veličine te zbog toga što je, poput Hrvatske, uvela osobne iskaznice s elektroničkim čipom te razvila sustav sličan sustavu e-Građani na kojem se temelji provedba glasovanja putem interneta.

5.1 Povećanje izlaznosti

Teza o znatnom povećanju izlaznosti na izbore zbog uvođenja glasovanja putem interneta nije onoliko evidentna koliko bi to njeni zagovornici željeli. Iako je udio glasača koji koriste glasovanje putem interneta u Estoniji iz godine u godinu sve veći, ukupna izlaznost na izbore ostaje gotovo nepromijenjena (3). U pilot projektu glasovanja putem interneta na lokalnim izborima 2005. godine sudjelovalo je tako 0,9% od ukupnog broja upisanih birača a u nedavno održanim parlamentarnim izborima 2019. godine ova se brojka popela na 27,9% ukupnog broja birača. Međutim, ukupna izlaznost na parlamentarne izbore pala je sa 67,8% 1992. godine na 63,7% 2019. godine, dok je na lokalnim izborima neznatno porasla s 52,6% 1992. godine na 53,3% 2017. godine (4). Ove brojke ukazuju da je porast broja glasova predanih glasovanjem putem interneta zapravo uzrokovan činjenicom da ljudi sve više vjeruju ovakvom obliku glasovanja i sve više cijene komotnost glasovanja iz vlastitog doma. Glasovanjem putem interneta služe se građani koji bi ionako izašli na izbore te nije došlo do poticanja izlaznosti kod ostalih građana.

Slučajevi u kojima internet ili dopisno glasovanje ipak povećava izlaznost su zemlje koje ovakav oblik glasovanja dopuštaju za svoje građane privremeno odsutne u inozemstvu za vrijeme održavanja izbora. Sjedinjene američke države tako zahtijevaju prihvaćanje glasova pripadnika svojih vojnih snaga privremeno izvan zemlje na barem jedan elektronički način dostave – e-poštom, faksom ili putem sigurne web stranice. Zbog svoje specifične društvene situacije u kojoj veliki dio građana s pravom glasa privremeno ili trajno boravi izvan zemlje, postoje znatne indikacije da bi uvođenjem glasovanja putem interneta Hrvatska ipak uvelike povećala izlaznost na izbore.

5.2 Sigurnost

Nažalost, jedna od rijetkih stvari iz područja računalne sigurnosti koja uživa gotovo univerzalni konsenzus je stav da je glasovanje putem interneta nemoguće adekvatno osigurati i zaštititi od neželjenih utjecaja zlonamjernih napadača (5). Usprkos nedvojbenim sigurnosnim nedostacima sustava za elektroničko glasovanje, odlikuje ih

velika prednost zbog činjenice da su uređaji fizički smješteni na samim izbornim mjestima, pod stalnim nadzorom osoblja zaduženog za provedbu izbora te podložni organiziranim i aktivnim inspekcijama. Glasovanje putem interneta se pak temelji na uporabi korisničkih uređaja kao što su računala, tableti i mobilni telefoni u nepreglednom mnoštvu marki, modela i operacijskih sustava, svaki sa svojim sigurnosnim propustima i problemima. Nadalje, ti su uređaji u posjedu korisnika, nisu podložni kontrolama ili inspekcijama te su podložni raznovrsnim udaljenim napadima kojima je moguće kompromitirati izbore čak i uz pretpostavku da je poslužiteljski, kontrolirani dio sustava u potpunosti zaštićen i osiguran od svakog napada.

U praksi se sve češće povlače usporedbe između elektroničkog glasovanja i internetskog bankarstva. Oba procesa su naizgled identična – potrebno je računalom se spojiti na sigurnu web stranicu, na siguran način potvrditi svoj identitet, odabrati željene opcije na zaslonu, kliknuti na gumb za potvrdu i gotovo – te se nameće pitanje „ako je sigurno kupovati i obavljati bankovne transakcije putem interneta, zašto bi bilo manje sigurno glasovati online?“.

Odgovor na ovo pitanje krije se u slabo poznatoj činjenici da ni bankovne transakcije preko interneta nisu zaista sigurne, a kad bi i bile potpuno sigurne, zahtjevi sigurnosti, privatnosti i transparentnosti demokratskih izbora temeljno su drugačiji od zahtjeva internetskog bankarstva.

Novčane transakcije putem interneta relativno su sigurne za krajnje korisnike, ali su istovremeno vrlo rizične za trgovce i financijske institucije. Banke, kartičarske kuće i *online* trgovci godišnje gube milijarde dolara na prijevare u internetskim transakcijama usprkos znatnim ulaganjima u sigurnost i u službe za otkrivanje i sprječavanje prijevара. Krajnji korisnici su pod dojmom da je sustav siguran zato što se ovi gubici ne naplaćuju izravno od korisnika nego se na nevidljiv način prelijevaju na sve korisnike u obliku povećanih naknada, kamata i ostalih troškova.

Velika većina napada koji ugrožavaju novčane transakcije primjenjiva je i na glasovanje putem interneta. Krađa vjerodajnica kao što su imena, brojevi računa, brojevi kreditnih kartica, lozinke ili odgovori na sigurnosna pitanja omogućuju napadačima krađu identiteta i obavljanje transakcija u korisnikovo ime. Izvori napada mogu biti doista raznoliki kao npr. virus, *phishing* kampanja putem e-pošte, zloćudni softver sakriven unutar neke druge aplikacije i sl. Nakon što je računalo zaraženo, zloćudni softver može prikriveno čekati pravi trenutak i aktivirati se samo onda kad korisnik pristupi internetskom bankarstvu. Najbolji primjer ovakvog napada je Zeus virus (6) koji je do sada zarazio milijune računala u svijetu, a koji ciljano napada internetsko bankarstvo, bilježi sve što korisnik unese te zatim u tajnosti provodi nedozvoljene transakcije dok korisniku prikazuje lažne podatke na zaslonu i prikriva tragove svog djelovanja. Kod ovakve vrste napada potpuno je nevažno koliko je sigurna veza s poslužiteljem banke jer se prijevara odvija na uređaju korisnika te su sigurnim kanalom poslani već izmijenjeni podaci. Ako znamo da banke, koje ulažu značajna sredstva u sigurnost ipak podliježu računalnim napadima, potpuno je jasno zašto je nemoguće zaštititi pojedinačne korisnike koji često znaju malo ili gotovo ništa o sigurnosti i dobrim praksama zaštite.

Razvojem tehnologije čak su i vrlo sofisticirani napadi postali lako dostupni i kriminalnim organizacijama ili pojedincima s malim budžetom. Prema nekim istraživanjima (7), napad poput Stuxneta koji su razvile tajne službe radi onesposobljavanja Iranskih nuklearnih

postrojenja i koji se smatra jednim od najsofisticiranijih poznatih računalnih napada u povijesti, danas bi zahtijevao oko dva mjeseca rada i budžet od svega 20.000 dolara. Nije nezamislivo da neka stranačka organizacija, strana obavještajna agencija ili neka treća zainteresirana strana izradi virus nalik na spomenuti Zeus, zarazi tisuće uređaja građana te u trenutku izbora u tajnosti promijeni njihove glasove prije njihovog „sigurnog” slanja na poslužitelj. Omjer od jedne krivotvorene transakcije na tisuću za online bankarstvo ne predstavlja nikakav problem jer sustav redovito kompenzira i do deset puta veće gubitke. Međutim, tolerancija na pogreške je daleko niža pri glasovanju i nije rijetka pojava da rezultat izbora u nekoj izbornoj jedinici ovisi o broju glasova manjem od jedan na tisuću. Uz ključnu razliku da gubitak bankarskih transakcija predstavlja u najgorem slučaju novčanu štetu koja se mjeri u dijelovima postotka ukupnog prihoda i koja se može kompenzirati u budućem poslovanju dok na izborima vrijedi pravilo da pobjednik odnosi sve – mala razlika u glasovima može imati ogromne posljedice i potpuno promijeniti političko usmjerenje grada ili države.

Zbog temeljno različitih zahtjeva sigurnosti, privatnosti i transparentnosti internetskog bankarstva i glasovanja, izborne bi prijave bilo nemoguće otkriti. Bankarstvo primjenjuje niz metoda koje pouzdano otkrivaju novčane prijave i omogućuju naknadno sprječavanje daljnjih šteta, djelomično ili potpuno ispravljanje pogrešaka te obeštećivanje krajnjih klijenata. Izdavanje računa, dvojno knjigovodstvo, financijske revizije i brojne druge metode omogućuju neovisnu provjeru svake transakcije dugo nakon njenog izvršenja. Glasovanje putem interneta, međutim, ne ostavlja nikakav pisani trag poput potpisnih knjiga ili kontrolnih lista pomoću kojih bi se moglo naknadno provjeriti vjerodostojnost rezultata, a koji bi zlonamjerni akter morao uništiti da sakrije tragove svog djelovanja.

Zaštita privatnosti dodatno otežava stvari jer glasovanje zahtijeva apsolutnu zaštitu, a kriteriji tajnosti i nedokazivosti brane bilo kakvo bilježenje rezultata glasovanja vezanih uz konkretnog pojedinca. Za razliku od bankovnih transakcija u kojima obje strane posjeduju podatke o detaljima transakcije te ih svaka strana može dokazati trećim stranama tj. sudu, glasovanje zahtijeva da izborna povjerenstva ne posjeduju sve detalje pojedinog glasovanja nego samo popis glasača koji su glasovanju pristupili i ukupni rezultat izbora. Istovremeno, svaki glasač zna točno kako je glasovao, ali ne smije imati dokaz o tome kojim bi trećim stranama mogao dokazati svoj glas. Ovo u potpunosti isključuje svaki oblik naknadne revizije jer sve kad bi i izborna povjerenstva pouzdano znalo da su glasovi određenih pojedinaca protuzakonito izmijenjeni računalnom prijevaram, ne bi bilo moguće odrediti koje to glasove iz ukupnog broja glasova treba izuzeti ili izmijeniti.

Transakcije u internet bankarstvu su neovisne i ponovljive bez posebnih ograničenja. Glasovanje putem interneta pak zahtijeva da svaki glasač smije glasovati samo jednom. Ali dok sprječavanje dvostrukog glasovanja internetom ne predstavlja poseban problem, otkrivanje i sprječavanje da se isti glasač i fizički pojavi na izbornom mjestu ili pošalje glasački listić i poštom ako to izborni zakoni omogućuju, znatno je složeniji zadatak. Izborna bi mjesta morala imati sigurnu i izravnu vezu sa sustavom glasovanja putem interneta te precizno bilježiti vrijeme pristupanja izborima za svakog građanina kako bi se u slučaju dvostrukog glasovanja moglo odlučiti koji glas izuzeti.

5.3 Transparentnost

Koliko god da je sigurnost glasovanja putem interneta veliki rizik i problem za koji se velika većina stručnjaka slaže kako je trenutno nerješiv, transparentnost je daleko veći izazov i problem za koji se čini da ni nema adekvatno rješenje.

Demokratski izbori po definiciji uključuju dvije ili više sučeljenih stranaka koje se u izravnom natjecanju bore za glasove građana i žele izbornu pobjedu. Pri tome je jedna od strana najčešće u politički povoljnijoj poziciji kao stranka trenutno na vlasti i barem teoretski u položaju s kojeg lakše može manipulirati rezultatom izbora. Za bolju legitimnost i uspjeh ne samo izbora nego i budućeg rada izbornog pobjednika važno je da i ostali sudionici izbora prihvate rezultat kao vjerodostojan odraz volje naroda. Najbolji način da se to osigura je izborni proces učiniti što transparentnijim i otvorenijim nadzoru i provjeri. Dobra praksa prihvaćena u svim demokratskim zemljama je dopustiti svim zainteresiranim stranama neovisno i samostalno nadgledanja izbora u svim njegovim fazama – od promatranja postupka glasovanja na izbornim mjestima do kasnijeg prebrojavanja i eventualne naknadne kontrole glasačkih listića. Bitna je i činjenica da kontrolu izbornog procesa može obaviti svaki građanin i bez posebnih edukacija ili stručnih znanja.

Glasovanje putem interneta, kao i drugi oblici elektroničkog glasovanja, uključuje računala i softversku podršku koji se ponašaju kao „crne kutije” – s jedne strane ulaze pojedinačni glasovi građana, a s druge strane izlazi završni rezultat izbora bez mogućnosti promatranja postupka koji se odvija između. Sustave za elektroničko glasovanje u pravilu razvijaju komercijalne tvrtke koje izvorni kod softverskog dijela sustava kao i ostale tehničke detalje sustava smatraju poslovnom tajnom te ne dopuštaju slobodan uvid u funkcioniranje sustava. Bez neograničenog uvida u sve dijelove sustava i bez mogućnosti nadzora sustava za vrijeme izbora, nemoguće je govoriti o transparentnosti. Programske pogreške pojavljuju se i u daleko manje važnim aplikacijama s daleko manjim utjecajem na društvo i neusporedivo manjim interesom za potencijalnu manipulaciju, a jedini način isključenja pogreške je detaljna revizija otvorena svima.

Nažalost, čak i kad bi sustavi glasovanja putem interneta koristili softver otvorenog koda i bili otvoreni nadzoru neovisnih stručnjaka, problem bi i dalje bio u činjenici da nadzor mogu provoditi isključivo stručnjaci. Obični građani ne posjeduju stručna znanja kojima bi mogli provjeriti vjerodostojnost izbora što svakako predstavlja dodatnu prepreku općem prihvaćanju izbornih rezultata.

Navedene nedostatke pokušavaju ispraviti ili ublažiti nove tehnologije kao što je lanac blokova (eng. *blockchain*) koji obećavaju provjerljivost rezultata izbora i nakon glasovanja bez ugroze anonimnosti i tajnosti pojedinačnih glasača te korištenje javnih računala za promatranje izbornog procesa. Spomenute tehnologije svakako predstavljaju pomak u dobrom smjeru, ali još uvijek ne rješavaju temeljni problem garancije sigurnosti pojedinačnih uređaja korisnika putem kojih se vrši glasovanje. Kompromitiranjem ove najslabije karike u lancu sigurnost ostalih faza glasovanja postaje nevažna.

6 Zaključak

Tehnologija prodire i mijenja sve sfere ljudskog života pa tako i razne procese unutar demokratskih izbora. Ali dok je u nekim stvarima pojava računala i elektroničkih uređaja dobrodošla pomoć neupitne koristi, još uvijek postoje elementi glasovanja u kojima uporaba elektroničkih uređaja nije dovoljno sigurna. Korišteni kao dodatak sustavu glasovanja temeljenom na papirnatim listićima, elektronički uređaji za glasovanje zahvaljujući asistivnim tehnologijama mogu biti neprocjenjiva pomoć građanima kojima uobičajena metoda zaokruživanja papirnato glosačkog listića predstavlja problem. Međutim, potpunim izbacivanjem papirnatih listića i isključivim oslanjanjem na elektroničko glasovanje izborni procesi, za sada, postaju nesigurni i netransparentni.

Glasovanje putem interneta kao najočitiji i najpoželjniji oblik elektroničkog glasovanja pogotovo je osjetljivo na rizike udaljenih napada i zlonamjernih manipulacija procesom glasovanja. Prihvatanjem bezgranične raznolikosti vrsta i modela uređaja u privatnom vlasništvu građana kao dopuštenih stanica za glasovanje uvodi se razina nesigurnosti koju ni jedna od ostalih karika u lancu nije u mogućnosti ispraviti.

Kao jedna od glavnih prednosti glasovanja putem interneta smatra se mogućnost povećanja izlaznosti građana na izbore. Iako primjer Estonije, kao jedine zemlje koja redovito dopušta glasovanje putem interneta na svim izborima u 15 godina od uvođenja ovakvog glasovanja nije rezultirao povećanjem izlaznosti, nije isključena mogućnost da bi u Hrvatskoj ovakvo glasovanje ipak polučilo željene rezultate zahvaljujući velikoj dijaspori i velikom broju građana na privremenom radu u inozemstvu.

Nasuprot tome, glasovanje putem interneta bi osim povećanja rizika od zlonamjernih manipulacija stranih i domaćih vlada te drugih zainteresiranih strana zasigurno smanjilo povjerenje građana i ostalih sudionika izbora u izborne rezultate. Negativne posljedice nemogućnosti nadgledanja izbora i nepostojanja mehanizama naknadne provjere i prebrojavanja glasova vjerojatno nadmašuju pozitivne koristi uštede vremena i lakšeg sudjelovanja na izborima za dio građana tehnički sposoban iskoristiti glasovanje putem interneta.

7 Literatura

1. **Langone, Alix.** An 11-Year-Old Hacked Into a Replica of a U.S. Voting System in 10 Minutes This Weekend. *Time*. [Mrežno] 14. kolovoza 2018. [Citirano: 24. travnja 2019.] <http://time.com/5366171/11-year-old-hacked-into-us-voting-system-10-minutes/>.
2. **Newman, Lily Hay.** Voting Machines Are Still Absurdly Vulnerable to Attacks. *WIRED*. [Mrežno] 28. rujna 2018. [Citirano: 24. travnja 2019.] <https://www.wired.com/story/voting-machine-vulnerabilities-defcon-voting-village/>.
3. **Valimised.** Statistics about Internet voting in Estonia. *Elections in Estonia*. [Mrežno] [Citirano: 24. travnja 2019.] <https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia>.
4. —. Voting results in detail. [Mrežno] [Citirano: 24. travnja 2019.] <https://rk2019.valimised.ee/en/voting-result/voting-result-main.html>.
5. **Simons, Barbara.** Report on the Estonian Internet Voting System. *Verified Voting*. [Mrežno] 3. rujna 2011. [Citirano: 24. travnja 2018.] <https://www.verifiedvoting.org/report-on-the-estonian-internet-voting-system-2/>.
6. **Kaspersky Lab US.** Zeus Virus | Zeus Trojan Malware | Zbot and Other Names. [Mrežno] [Citirano: 24. travnja 2019.] <https://usa.kaspersky.com/resource-center/threats/zeus-virus>.
7. **Jefferson, David.** If I Can Shop and Bank Online, Why Can't I Vote Online? *Verified Voting*. [Mrežno] [Citirano: 24. travnja 2019.] <https://www.verifiedvoting.org/resources/internet-voting/vote-online/>.