Sustavi za elektroničko glasovanje

Uglješa, Karmen

SVEUČILIŠTE U ZAGREBU

FILOZOFSKI FAKULTET

ODSJEK ZA INFORMACIJSKE I KOMUNIKACIJSKE ZNANOSTI

SMJER ISTRAŽIVAČKA INFORMATIKA

AK. GOD. 2018./2019.

Karmen Uglješa

Sustavi za elektroničko glasovanje

diplomski rad

Mentor: dr.sc. Krešimir Pavlina, izv. prof.

Zagreb, rujan 2019.

Sadržaj

1. Uvod

Kada se u obzir uzme vrijeme koje je prošlo otkad su začeti pojmovi demokracije, biračkog prava i izbora, elektroničko glasovanje pojava je koja je aktualna tek u vrlo kratkom periodu; ipak, čini se kako će se s vremenom sve više država oslanjati na njega u svojim izbornim procesima. Dok su neke države uspješno implementirale sustave za elektroničko glasovanje te ih koristi sve veći broj glasača, druge se još uvijek trude naći sustav koji će odgovarati infrastrukturi i potrebama građana. Velik se broj država, građana, ali i stručnjaka ipak protivi uvođenju elektroničkog glasovanja, smatrajući, ne bez razloga, da ono sa sobom nosi velike sigurnosne rizike – u slučaju napada na sustav, identiteti glasača mogu biti otkriveni i povezani s glasovima, rezultati izmijenjeni, a integritet izbora ugrožen. Međutim, ovi rizici nisu svojstveni jedino elektroničkom glasovanju – različite papirnate i mehaničke metode glasovanja, uključujući obične papirnate glasačke listiće, bušene kartice, strojeve s polugom i optičko skeniranje, mogu na različite načine biti metom zlonamjerne interferencije ili manipulacije, no mnoge od njih nastavljaju se koristiti diljem svijeta. Ne postoji sustav za glasovanje koji je u potpunosti zaštićen od svih teoretskih i stvarnih prijetnji; međutim, izrada smjernica, preporuka i standarda prvi je korak prema izgradnji stabilnog i održivog sustava, nakon čega je potrebno smisliti i implementirati jake zaštitne mjere i sigurnosne protokole kojima će se štititi osnovni principi glasovanja.

Cilj je ovog rada istražiti razvoj sustava za elektroničko glasovanje te prikazati implementacije sustava na stvarnim primjerima. Prije svega, obrazloženo je zašto je glasovanje općenito važna aktivnost u demokratski uređenim državama i kako bi elektroničko glasovanje moglo pridonijeti izbornom procesu. Zatim slijedi pregled metoda glasovanja koje su se koristile, ili i dalje koriste, diljem svijeta – opisan je način korištenja, ali i njihove slabe točke. Tema ovog rada, elektroničko glasovanje, obuhvaćena je posebnim poglavljem u kojem su, prije svega, prikazane smjernice i preporuke objavljene u Europi i Sjedinjenim Američkim Državama kojima se nastoji regulirati i standardizirati korištenje elektroničkog glasovanja; nakon toga slijedi opis općih značajki sustava za elektroničko glasovanje koje proizlaze iz navedenih smjernica, uz prikaz entiteta koji se najčešće pojavljuju u generičkom modelu sustava. Kako je sigurnost jedna od najvažnijih stavki prilikom izrade sustava, opisane su i najčešće kriptografske metode kojima se štite razni podaci koji su potrebni u procesu glasovanja; nakon toga navedene su prednosti i mane sustava za elektroničko glasovanje. Kao primjeri konkretnih sustava, njihovih načina korištenja, ali i nedostataka, opisane su tri države koje koriste elektroničko glasovanje – Sjedinjene Američke Države,

Estonija i Belgija. Naposljetku, iako Republika Hrvatska nema konkretne planove o uvođenju elektroničkog glasovanja, povremeno o toj temi zažive rasprave, stoga je dan pregled trenutačnih mogućnosti te mišljenja i komentara predstavnika političkih stranaka, državne uprave te telekomunikacijskih agencija.

2. Izbori, referendumi i važnost glasovanja

Izbori su niz postupaka kojima biračko tijelo odabire jednog od više ponuđenih kandidata za obnašanje određene političke funkcije. Općenito, u demokratskim državama svaki državljanin iznad određene dobi ima pravo glasovanja na izborima; u Republici Hrvatskoj minimalna je dob za mogućnost glasovanja 18 godina[1]. Izbori se, ako nisu prijevremeni, održavaju u redovitim razmacima te na više razina upravljanja – najčešće na lokalnoj i državnoj – te uglavnom uključuju izbor predsjednika države, zastupnika u parlamentu, članova vijeća nacionalnih manjina i sl., što je slučaj u Hrvatskoj[2], te ekvivalente tih izbora u drugim državama.

Biračko tijelo ima pravo sudjelovanja i na referendumima. Referendum je izravno glasovanje o pitanjima koja su uglavnom vezana za promjenu ustava, prijedloge zakona ili pak djelokrug lokalne i regionalne samouprave[3], što znači da se također može održavati na lokalnoj i državnoj razini. Budući da se referendumi uglavnom raspisuju radi zakonskih promjena, ne održavaju se u redovitim razmacima, već prema potrebi. Dok su u nekim državama (poput Hrvatske) referendumi iznimno rijetki, u drugima su oni vrlo često korištena metoda rješavanja državnih pitanja; primjer je takve države Švicarska koja je u periodu od 1848. do 1994. godine održala 430 referenduma[4].

Iz svega navedenog jasno je da su izbori i referendumi, ili točnije glasovanje, temelj demokratskog društva. Da bi glasovanje bilo valjano, mora zadovoljiti sljedeće kriterije[5]:

- transparentnost (razumljivost svakog koraka svim sudionicima i podložnost neovisnoj provjeri);
- tajnost (izražavanje stvarne volje, bez utjecaja drugih osoba);
- anonimnost (izostanak potpisa i drugih identifikacijskih oznaka glasača);
- nedokazivost (nemogućnost dokazivanja za koga je pojedini glasač glasovao);
- integritet (osiguravanje ostalih uvjeta kojima se jamči valjanost rezultata).

Biračko tijelo (najčešće narod) glasovanjem izravno utječe na svoju dobrobit, stoga je poželjan što veći odaziv. Kako bi se to ostvarilo, poduzimaju se razne mjere povećanja odaziva birača, poput političkih kampanja ili uvođenja obveznog glasovanja. Uz motiviranje

[1] Zakon o izborima zastupnika u Hrvatski državni Sabor, čl. 14.
[2] „Izbori / Referendumi“.
[3] „Općenito“.
[4] Trechsel i Kriesi, „Switzerland: the referendum and initiative as a centrepiece of the political system“, 190.
[5] CARNet, CERT, „Elektroničko glasovanje“, 4-5.

biračkog tijela, mnogo se pozornosti pridaje i prilagođavanju i mijenjanju postojećih tehnologija te uvođenju novih, pristupačnijih sustava glasovanja koji bi glasačima olakšali proces glasovanja; osim toga, primjena tehnologije u cijelom izbornom procesu povećala bi administrativnu učinkovitost i političku transparentnost te smanjila troškove[6].

[6] „Overview“.

3. Tehnologije u glasovanju

Postoji nekoliko glasačkih metoda koje su se koristile tijekom povijesti, od kojih se većina u određenoj mjeri oslanja na papir. Tijekom 20. stoljeća rapidno su se pojavile nove tehnologije kojima je cilj bio ubrzati prebrojavanje glasova, povećati sigurnost i zaštititi tajnost glasovanja te su se počele implementirati u različitim državama. Iako se za svaku od metoda mogu navesti općenite prednosti i nedostaci, implementacija, dizajn i korištenje pojedinačnih sustava najpreciznije će pokazati u kojoj će mjeri biti uspješni. U ovom su poglavlju stoga opisane najčešće i najraširenije metode glasovanja uz opće karakteristike.

3.1. Papirnate metode

Pokušaji automatizacije, ubrzanja i olakšavanja procesa glasovanja stari su gotovo koliko i ono samo – u antičkom Rimu koristilo se dopisno glasovanje, što je najraniji primjer glasovanja na daljinu koje se oslanjalo na neku vrstu komunikacijske infrastrukture da bi funkcioniralo[7]. Metoda koja se tada koristila, i koja je i danas najraširenija, glasački su listići. Glasački je listić list papira na kojem su navedena imena mogućih kandidata, od kojih glasač izabire dogovoreni broj. Otkad su u Sjedinjenim Američkim Državama glasački listići prvi put korišteni 1629. godine[8], način na koji su se koristili nekoliko se puta mijenjao. Isprva ova metoda nije bila regulirana – listiće, koji su se mogli naći u novinama ili su ih dijelile političke stranke, glasači su sami ispunjavali i donosili na biračko mjesto, što je lako moglo dovesti do niza problema poput povrede privatnosti, ubacivanja više od jednog listića i izbornih prijevara. Da bi se ti rizici smanjili, s vremenom su stranke počele tiskati vlastite listiće; međutim, najčešće su bila navedena imena samo onih kandidata koje je određena stranka podržavala te su listići bili tiskani na način da je bilo teško dopisati ime željenog kandidata čije ime nije bilo navedeno. Način korištenja ove metode uvelike je unaprijeđen 1858. godine, kada je australska vlada osigurala glasačke listiće na biračkim mjestima. Svaki je glasač imao na raspolaganju jedan glasački listić, listići su bili identični, ni na koji se način nije moglo vidjeti kako je tko glasao te su bila navedena imena svih mogućih kandidata, čime je bilo olakšano glasovanje za kandidate iz različitih stranaka[9]. Ovime su učinjeni prvi koraci prema nekima od najvažnijih svojstava današnjih sustava za glasovanje: anonimnosti i integritetu. Međutim, glasački su listići daleko od optimalnog načina glasovanja – neki su od

[7] Gibson et al. „A review of e-voting: the past, present and future“, 279.
[8] Jones, „A Brief Illustrated History of Voting“.
[9] FairVote, „The history of the paper ballot“.

nedostataka: golemi troškovi tiskanja i distribucije listića, velika mogućnost pogreške pri prebrojavanju te neprilagođenost osobama sa smetnjama poput poteškoća s vidom.

Korak prema automatizaciji metode glasovanja putem glasačkih listića učinjen je pojavom bušenih kartica, na kojima glasači izbuše rupu pokraj imena ili broja odabranog kandidata. Ova se metoda u SAD-u koristila od 60-ih godina 20. stoljeća[10] te je postojala u dva oblika, *Votomatic* i *Datavote*. *Votomatic* je imena kandidata i upute za korištenje sadržavao u zasebnoj knjižici uz uređaj za glasovanje, a na samoj su se kartici nalazili brojevi uz mjesta na kojima se mogla izbušiti rupa. *Datavote* je, s druge strane, sadržavao imena kandidata na listiću uz pripadajuća mjesta gdje se rupa trebala izbušiti. Nakon završetka glasovanja glasovi bi se brojali ručno ili pomoću stroja za tabeliranje, što bi ubrzalo proces. Iako su bušene kartice bile najkorištenija metoda na mnogim američkim izborima, sadržavale su neke nedostatke: ostaci papira nakon bušenja nakupljali su se u rupama te je zbog toga bilo sve teže izbušiti rupu za željenog kandidata. Također, prilikom ručnog brojanja bilo je teško utvrditi je li rupa dovoljno perforirana da bi glas bio valjan. Ovi su nedostaci dijelom bili uzrok problema koji su, potpomognuti upitnim dizajnom glasačkih listića, kulminirali na američkim predsjedničkim izborima 2000. godine, kad se na službene rezultate čekalo više od mjesec dana[11], nakon čega su se bušene kartice u SAD-u koristile znatno rjeđe.

Uz bušene kartice, u drugoj polovici 20. stoljeća koristila se i tehnologija optičkog skeniranja, što se može smatrati prvim oblikom elektroničkog glasovanja (još uvijek, međutim, temeljenog na papiru). Listići su uz imena kandidata sadržavali simbole poput pravokutnika, kruga ili strelice te se glasalo tako da su se simboli iscrnili ili upotpunili; listići bi se zatim ubacili u uređaj za tabeliranje koji bi identificirao označen simbol, a glasovi su se spremali u bazu podataka i zbrajali[12]. Najraširenija je tip optičkog čitanja optičko prepoznavanje oznaka (engl. *optical mark recognition*, OMR), budući da je najpogodniji za jednostavne sustave glasovanja, primjerice zatvorene liste, u kojima je moguć samo jedan izbor. Za listiće na kojima se ručno upisuju brojevi, slova ili imena dodatnih kandidata te kompleksnije sustave glasovanja (primjerice preferencijalno glasovanje) koristi se optičko prepoznavanje znakova (engl. *optical character recognition*, OCR), odnosno inteligentno prepoznavanje znakova (engl. *intelligent character recognition*, ICR). Optičko skeniranje uvelike ubrzava proces glasovanja te ostavlja mogućnost ručnog prebrojavanja glasova u slučaju da se uređaj pokvari; međutim, nekoliko stručnjaka dokazalo je mogućnost prijevare sustava, mijenjanjem

[10] „Punchcards“.
[11] „Bush v. Gore“.
[12] „Optical Scanning Sytems“.

konfiguracijske datoteke uređaja za tabeliranje u korist određenog kandidata [13] ili manipulacijom memorijske kartice[14].

3.2. Mehaničke metode

U mehaničke (i, kasnije, digitalne) metode ubrajaju se one koje ne oslanjaju na papirnati trag, što uključuje niz različitih sustava, od pikula koje su se koristile na predsjedničkim izborima u Gambiji 2016. godine[15], do strojeva s polugom, korištenih najviše u SAD-u. Na strojevima s polugom uz imena kandidata nalazile su se poluge od kojih je glasač trebao okrenuti jednu, pripisanu kandidatu za kojeg se opredijelio. Prilikom ulaska u kabinu, glasač je okretao posebnu ručicu pri čemu bi se navukla zavjesa te osigurala anonimnost; nakon okretanja poluge za željenog kandidata, ostale bi se poluge zaključale, čime bi se spriječila mogućnost višestrukog glasovanja. Nakon okretanja ručice za otvaranje zavjese, glasovanje je zaključeno te se poluge vraćaju na početni položaj. Svaka je poluga imala brojčanike koji bi se okretanjem poluge pomicali za jedno mjesto[16]. Budući da se glas broji već izlaskom iz kabine, ova metoda omogućuje objektivno prebrojavanje glasova i brze rezultate[17]; međutim, u slučaju kvara stroja, ne postoji nikakav papirnati trag te je nemoguće povratiti glasove[18].

3.3. Digitalne metode

Ubrzan razvoj tehnologije te sve raširenije korištenje interneta doveli su do toga da se cijeli izborni proces (i glasovanje i zbrajanje rezultata) sve više oslanja na računala. Pojavom uređaja za izravno elektroničko bilježenje glasova (engl. *direct-recording electronic (DRE) voting machine*) potpuno je eliminiran papirnati trag. Na tipičnom DRE uređaju nalazi se dodirni zaslon na kojem su ispisana imena kandidata (uz posebne tipke za osobe s posebnim potrebama te tipkovnicu u slučaju upisivanja kandidata koji nije naveden), što se može nazvati vrstom elektroničkog glasačkog listića. Nakon glasovanja, podatak se sprema u memorijsku komponentu uređaja (tvrdi disk, CD-ROM, memorijska kartica i sl.). Nakon zatvaranja glasovanja, podaci s različitih glasačkih lokacija zbrajaju se na središnjem

[13] Jones, „Example Attack Documentation: Optical Scan Configuration File“.
[14] Pynchon, „Florida: The Harri Hursti Hack and its Importance to our Nation“.
[15] Duggan, „Gambians cast votes with marbles instead of ballots“.
[16] „Mechanical Voting Systems“.
[17] Jones, „The evaluation of voting technology“, 6.
[18] Ibid.

računalu, do kojeg putuju na prijenosnoj memoriji ili preko mreže[19]. DRE uređaj je, uz optičko skeniranje, postao najčešća metoda glasovanja u SAD-u otkad je 2002. godine, nakon kontroverznih predsjedničkih izbora, izglasan Zakon o pomoći Americi pri glasovanju (engl. *Help America Vote Act*, HAVA)[20] te se počeo koristiti i u drugim državama poput Brazila, Venezuele i Indije.

[19] „Direct Recording Electronically".
[20] „Voting Equipment".

4. Elektroničko glasovanje

Ne postoji usuglašena definicija elektroničkog glasovanja. Sustavi za elektroničko glasovanje (e-glasovanje) ugrubo su definirani kao sustavi u kojima se „izborni podaci bilježe, pohranjuju i obrađuju prvenstveno kao digitalna informacija“[21]. Sam proces elektroničkog glasovanja također nije jedinstveno definiran; ponegdje je proces samog glasovanja odijeljen od procesa prebrojavanja glasova – elektroničko se glasovanje definira kao elektronički sustav u kojemu se odvija glasovanje te je glas stoga digitalno pohranjen, dok se u slučaju elektroničkog prebrojavanja glasova sam proces glasovanja može odviti i neelektroničkim putem[22]. Druge definicije razlikuju dva tipa elektroničkog glasovanja – ono koje se odvija na uređajima za elektroničko glasovanje na biračkim mjestima, u općinskim uredima ili veleposlanstvima pod nadzorom vladinih predstavnika ili nezavisnih organizacija te ono pri kojemu predstavnici ili organizacije nisu fizički prisutni, a odvija se preko bilo kojeg računala spojenog na internet, telefona, mobitela (SMS-a), terminala i sl.[23]; ako se odvija preko interneta, naziva se još i internetsko ili i-glasovanje (engl. *i-voting*). Kako se danas teži potpunoj digitalizaciji, samo elektroničko prebrojavanje glasova u većini slučajeva nije dovoljno da se neki proces glasovanja nazove elektroničkim – primjerice, u kontekstu rasprave o uvođenju elektroničkog glasovanja u Hrvatskoj jasno je da se misli na sustav koji je u potpunosti u digitalnom obliku[24]. Elektroničko glasovanje, stoga, u većini slučajeva podrazumijeva, uz elektroničko prebrojavanje glasova, i glasovanje na biračkom mjestu ili bilo kojoj drugoj lokaciji gdje je moguće dati svoj glas preko elektroničkog uređaja.

Dok se istraživanja o elektroničkom glasovanju odvijaju od druge polovice 20. stoljeća, konkretni su se sustavi počeli implementirati relativno nedavno te tek njihovo konkretno korištenje može ukazati na nedostatke i probleme koji se mogu pojaviti. Kako bi se ti nedostaci minimizirali od početka, potrebno je smisliti zadovoljavajući i opsežan informacijski sustav kao temelj, što, osim projektiranja samog sustava, uključuje i opsežnu potporu u pravnom, sigurnosnom, financijskom i javnom aspektu – drugim riječima, za uspješnu implementaciju sustava potrebno je pripremiti cjelokupnu infrastrukturu, ali i osigurati zadovoljstvo korisnika.

[21] Lambrinoudakis et al. „Electronic voting systems: Security implications of the administrative workflow“, 2.
[22] Kumar i Walia, „Analysis of electronic voting system in various countries“, 1826.
[23] Buchsbaum, „E-voting: International developments and lessons learnt“, 32.
[24] „Sve što možda ne znate, a trebate znati o dopisnom i elektroničkom glasovanju“.

4.1. Europski standardi

Jednu od prvih regulacija koje su se bavile standardizacijom elektroničkog glasovanja – Pravne, operativne i tehničke standarde za e-glasovanje (*Legal, operational and technical standards for e-voting*) – usvojio je 2004. godine Odbor ministara Vijeća Europe te se sastojala od tri dijela. Prvi dio, *Pravni standardi*, odnosi se na pravne aspekte sustava za elektroničko glasovanje te opisuje sljedeće principe:

1. *Univerzalno pravo glasa*. Sučelje glasačkog sustava mora biti lako razumljivo i upotrebljivo, uvjeti za registraciju birača ne smiju predstavljati prepreku za sudjelovanje u glasovanju, sustavi moraju u potpunosti biti prilagođeni osobama s posebnim potrebama te, osim u slučaju da je e-glasovanje univerzalno dostupno, ovi sustavi samo su dodatna i neobavezna metoda glasovanja.
2. *Jednako pravo glasa*. Glasač ne smije ubaciti više od jednog glasa u elektroničku glasačku kutiju te smije glasovati jedino ako je utvrđeno da još uvijek nije glasovao, sustav mora spriječiti mogućnost da glasač da svoj glas preko više različitih kanala, svaki glas u sustavu mora se brojati i to samo jednom te, ako uz elektronički postoji i neelektronički sustav, mora postojati sigurna i pouzdana metoda koja će zbrojiti sve glasove i dati točan rezultat.
3. *Slobodu glasovanja*. E-glasovanje mora biti organizirano tako da osigurava slobodnu volju glasača, način na koji sustav vodi glasača kroz proces ne smije ga tjerati na nagao i nepromišljen izbor, glasač mora imati mogućnost promjene odabira prije konačnog davanja glasa i mogućnost odustajanja od glasovanja bez da je prethodni odabir vidljiv ikome drugome, sustav ne smije dopustiti bilo kakav utjecaj na glasača tijekom glasovanja, mora dati mogućnost sudjelovanja na izboru ili referendumu davanjem praznog glasa, mora jasno pokazati da je proces glasovanja te mora spriječiti promjenu odabira nakon što je glas već dan.
4. *Tajnost glasovanja*. E-glasovanje mora biti organizirano tako da ni u jednom trenutku tijekom autentifikacije i samog glasovanja ne ugrožava tajnost glasa, sustav mora jamčiti anonimnost svih danih glasova, mora biti dizajniran tako da se rezultati glasovanja ne mogu povezati s pojedinačnim biračem te se moraju poduzeti mjere koje će osigurati da se informacije potrebne za obradu ne mogu iskoristiti za kršenje tajnosti glasa.[25]

[25] Council of Europe, „Legal, operational and technical standards for e-voting“, 9-10.

Uz ove principe, u *Pravnim standardima* također se naglašava poduzimanje potrebnih mjera kako bi se osigurala opća transparentnost i provjerljivost rezultata te pouzdanost i sigurnost sustava. Drugi i treći dio dokumenta, *Operativni standardi* i *Tehnički zahtjevi*, također naglašavaju ove principe, ali iz drugih perspektiva. *Operativni standardi* tiču se same organizacije izbora te su podijeljeni na šest dijelova: *Obavijesti, Glasači, Kandidati, Glasovanje, Rezultati* i *Kontrola*.

Treći dio, *Tehnički zahtjevi*, nalaže kako dizajn sustava za e-glasovanje treba biti poduprt sveobuhvatnom procjenom mogućih rizika pri uspješnom završetku određenog izbora ili referenduma te treba uključivati prikladne zaštitne mjere na temelju te procjene[26]. Tehnički zahtjevi navedeni u dokumentu te njihove najvažnije točke su sljedeće:

1. *Pristupačnost*. Trebaju se poduzeti mjere kojima će se osigurati da programsku podršku mogu koristiti svi glasači te, ako je potrebno, omogućiti alternativne načine glasovanja; korisnici će biti uključeni u dizajniranje sustava za e-glasovanje kako bi identificirali ograničenja i testirali lakoću korištenja; korisnicima će na raspolaganju biti dodatna ili jednakovrijedna sredstva poput posebnih sučelja ili osobne pomoći; prilikom razvoja proizvoda treba uzeti u obzir njegovu kompatibilnost s postojećim, uključujući tehnologije korištene pri pomoći osobama s invaliditetom; prikaz glasačkih opcija treba biti optimiziran za glasača.
2. *Interoperabilnost*. Koristit će se otvoreni standardi kako bi se zajamčilo zajedničko međudjelovanje (interoperabilnost) raznih tehničkih komponenata i servisa sustava za e-glasovanje; prezentacijski jezik za izbore (engl. *Election Markup Language*, EML) jedan je takav otvoreni standard te će se koristiti kad god je to moguće kako bi se zajamčila interoperabilnost; u slučajevima gdje su potrebni specifični zahtjevi, provest će se procedura lokalizacije koja će proširiti ili ograničiti pristup informacijama, istovremeno ostajući u skladu s EML-om.
3. *Operacijski sustav*. Nadležne izborne vlasti trebaju objaviti popis programske podrške korištene na e-izboru ili e-referendumu; treba postojati pričuvni sustav koji će slijediti iste standarde kao izvorni sustav; druge pričuvne metode moraju biti spremne u slučaju odluke nadležnih vlasti; oprema koja će se koristiti tijekom glasovanja mora biti u skladu sa korisničkim potrebama i tehničkim specifikacijama; ključna će se oprema nalaziti na sigurnoj lokaciji, zaštićena od bilo kakvog neovlaštenog korištenja.

[26] Ibid. 15.

4. *Sigurnost (opći zahtjevi)*. U slučaju kvara trebaju se poduzeti tehničke i organizacijske mjere kojima će se sačuvati podaci; sustav treba sačuvati privatnost pojedinaca; potrebno je izvršiti autentifikaciju pojedinca prije izvršavanja bilo koje radnje te će pojedinac na raspolaganju imati samo usluge dostupne na toj razini autorizacije; podaci za autentifikaciju moraju biti zaštićeni tako da ih neovlašteni subjekti ne mogu zloupotrijebiti, izmijeniti ili na drugi način doći do njih te se u nekontroliranom okružju preporučuje autentifikacija na temelju kriptografskih mehanizama; mora se osigurati jedinstvena identifikacija glasača; sustav mora generirati pouzdane i detaljne podatke koji će se koristiti u promatranju izbora.
5. *Kontrola (opći zahtjevi)*. Sustav provjere treba biti implementiran kao dio sustava za e-glasovanje; kontrola sustava za e-glasovanje treba uključivati bilježenje svih podataka o procesu glasovanja (uključujući ukupan broj glasača i ukupan broj glasova, ali i napade na sustav te kvarove sustava), sustav nadzora koji će omogućiti potvrdu da su svi rezultati i procedure u skladu sa zakonskim odredbama te sustav verifikacije koji će omogućiti provjeru točnosti rezultata i otkriti glasačku prijevaru.[27]

Kao dopuna Standardima priloženo je i obrazloženje svakog od navedenih uvjeta i točaka te se u njemu navode i moguće prijetnje, podijeljene po fazama glasovanja u kojima se mogu pojaviti (prije, tijekom i nakon glasovanja). Opće prijetnje (one koje se mogu pojaviti u svim fazama) tiču se krivotvorenja i otkrivanja podataka te hakiranja sustava i mogu ugroziti prethodno navedene uvjete, kao što su sigurnost i provjerljivost, ali i integritet cijelog sustava[28].

Budući da se dokument, koji je stvorila multidisciplinarna skupina specijalista, odnosi na veći broj europskih država čije se mogućnosti organiziranja elektroničkih glasovanja mogu razlikovati u velikoj mjeri, nije bilo moguće ostvariti konkretan model sustava za elektroničko glasovanje: „različite države imale su – osim različitih izbornih sustava, različitih temeljnih pogleda na e-glasovanje, različitih definicija e-glasovanja, različitih iskustava s e-glasovanjem i stručnjaka s različitom razinom stručnosti – različita očekivanja od stručne skupine“[29]. Iz tog razloga dokument ne sadrži mnogo više od preporuka. Na eventualno uvođenje elektroničkog glasovanja također uvelike mogu utjecati javno mišljenje i povjerenje, često podložna promjenama te pod neprestanim utjecajem mišljenja stručnjaka, medija i političara – primjer su stanovnici Irske koji su, prema rezultatima ankete iz 2003. godine, većinom odobravali

[27] Ibid. 15-20.
[28] Ibid. 69.
[29] Buchsbaum, 38.

uvođenje elektroničkog glasovanja; međutim, godinu dana kasnije, nakon što je kao posljedica kontroverza oko tadašnjeg sustava uvedena Komisija za elektroničko glasovanje, prevladala je nepovjerljivost prema e-glasovanju[30]. Što se tiče samog načina na koji su Standardi napisani i organizirani, članak Margaret McGaley i J. Paula Gibsona „*A Critical Analysis of the Council of Europe Recommendations on e-Voting*" navodi svojstva kvalitetno napisanog dokumenta te vrste te tvrdi da ih ovi Standardi nemaju – ističe se nedosljednost u terminologiji (primjerice, brkanje pojmova glasač i birač – engl. *voter* odnosno *elector*), iskoraci van domene e-glasovanja (npr. preporuke o biračkom registru koje su pokrivene u drugim dokumentima Vijeća), predetaljne, ali i nedovoljno detaljne specifikacije, te suvišnosti i ponavljanja. Zbog navedenih nedostataka, ali i zbog konstantnog razvoja novih tehnologija koje bi mogle dovesti do učestalog mijenjanja teksta, smatra se da je dokument teško održiv[31].

4.2. Američki standardi

Dokument koji propisuje standarde u korištenju sustava za elektroničko glasovanje u SAD-u, Dobrovoljne smjernice za glasačke sustave (*Voluntary Voting System Guidelines*), objavio je Odbor za pomoć pri izborima (*Election Assistance Commission*, EAC) 2005. godine. EAC i njegove smjernice nastali su kao posljedica ranije izglasanog zakona HAVA koji je nalagao zamjenu starih glasačkih metoda (poput bušenih kartica i strojeva s polugom) novijim sustavima, odnosno optičkim skeniranjem i DRE uređajima; također je zahtijevao kreiranje glasačkih standarda i testiranja kojim će se certificirati razni glasački sustavi. Zbog toga su, za razliku od europskih standarda, EAC-ove smjernice nešto više od preporuka – savezne države mogu birati hoće li ih usvojiti u potpunosti, prilagoditi ih svojim uvjetima ili se povući[32], no moraju ih slijediti kako bi sustavi koje koriste dobili certifikat.

EAC-ove smjernice iz tog su razloga opsežan su dokument, sadržan u dva sveska, koji navodi skup specifikacija i zahtjeva prema kojima glasački sustavi moraju biti testirani kako bi se utvrdilo omogućuju li temeljnu funkcionalnost, pristupačnost i sigurnost koje su potrebne kako bi se osigurao njihov integritet; dokument također određuje kriterije ocjenjivanja za nacionalnu certifikaciju glasačkih sustava[33]. Sukladno tome, dokument je podijeljen u dva

[30] McGaley i Gibson, „A Critical Analysis of the Council of Europe Recommendations on E-Voting", poglavlje 2.2.
[31] Ibid. poglavlje 4.6.
[32] Hale i Brown, „Adopting, adapting, and opting out: State response to federal voting system guidelines", 429.
[33] US Election Assistance Commission, „Voluntary voting system guidelines. Vol. II", X.

sveska. Važno je napomenuti da dokument obuhvaća i sustave s optičkim skeniranjem, stoga su elektronički sustavi samo jedna od metoda na koje se zahtjevi odnose.

Prvi svezak, Smjernice za izvedbu glasačkih sustava (*Voting System Performance Guidelines*), sadrži detaljne zahtjeve koje sustavi moraju zadovoljavati te je podijeljen na devet poglavlja i četiri priloga. U prvom poglavlju definirani su ciljevi i područje primjene Smjernica, dok se ostala poglavlja bave konkretnim zahtjevima.

Drugo poglavlje sadrži funkcionalne zahtjeve, odnosno precizno definira što se od sustava traži da obavlja[34]. Zahtjevi su podijeljeni po fazama glasovanja. Cjelokupne mogućnosti sustava primjenjuju se kroz cijeli izborni proces i uključuju sigurnost, točnost, oporavak od pogrešaka, fizički integritet, mogućnost kontrole sustava, sustav za upravljanje izborima, prebrojavanje glasova i listića, zaštitu podataka prilikom prijenosa preko telekomunikacijskih mreža te čuvanje podataka (u periodu od 22 mjeseca nakon izbora[35]). Predglasačke mogućnosti sustava odnose se na funkcije koje se moraju izvesti prije otvaranja izbora te uključuju pripremu i instalaciju listića i programske podrške te test spremnosti sustava. Mogućnosti sustava tijekom glasovanja uključuju otvaranje anketa te davanje glasa (ubacivanje listića). Postglasačke mogućnosti sustava uključuju zatvaranje glasovanja, dobivanje izvješća svakog pojedinačnog uređaja, biračkog mjesta i okruga, objedinjena izvješća te osiguravanje revizijskog traga. U funkcionalne zahtjeve spada i održavanje, odnosno mogućnost korištenja bez smanjenja učinkovitosti nakon prijevoza i skladištenja na dulje vrijeme.

Treće poglavlje sadrži zahtjeve koji se tiču uporabljivosti i pristupačnosti sustava te koji će korisnicima pomoći da ga koriste što učinkovitije. Uporabljivost je definirana kao mjera učinkovitosti i zadovoljstva korisnika određenim proizvodom u izvršavanju određenog zadatka; u ovome slučaju korisnici su glasači, proizvod je glasački sustav, a zadatak je pravilna zabilježba glasa[36]. Pod zahtjeve uporabljivosti navedene su razne funkcionalne mogućnosti – nešto detaljnije od općih zahtjeva iz drugog poglavlja – poput informiranja korisnika da nije izvršio odabir ili je odabrao prevelik broj opcija te prilike da promijeni odabir; za DRE uređaje posebno je naglašena mogućnost navigacije između pojedinih anketa prije konačnog davanja glasa. Također se zahtijeva mogućnost prikaza listića na bilo kojim jezicima koje zahtijeva zakon te proces mora biti dizajniran tako da umanji bilo kakve kognitivne, perceptivne ili interaktivne poteškoće. Što se tiče pristupačnosti, zahtijeva se

[34] US Election Assistance Commission, „Voluntary voting system guidelines. Vol. I“, 19.
[35] Ibid. 28.
[36] Ibid. 47.

dostupnost barem jednog glasačkog mjesta prilagođenog osobama s posebnim potrebama, uključujući probleme s vidom, sluhom ili govorom, kognitivne poteškoće te smanjenu okretnost i spretnost.

Četvrto, peto i šesto poglavlje odnose se na elektroničku opremu, programsku podršku i telekomunikacije. Navedene su minimalne vrijednosti za određene izvedbene i fizičke značajke te značajke dizajna, izgradnje i održavanja koje moraju imati oprema i sve njezine komponente, uključujući pisače, zaslone, glasačke kutije, memorijske kartice i sl.[37]. Određenu programsku podršku koja će se koristiti bira proizvođač opreme, no naglašeno je da podrška mora osigurati izvršenje funkcionalnih zahtjeva i mogućnosti iz drugog poglavlja[38]. Što se tiče telekomunikacija, mrežne komponente uključuju lokalne mreže (engl. *local area network*, LAN), mreže širokog područja (engl. *wide area network*, WAN), radne stanice (stolna računala, sustave za tabeliranje i sl.) i poslužitelje te se od njih očekuje jednostavnost, fleksibilnost (posebice u usmjeravanju, kako bi se zadržalo kratko vrijeme odziva) i održivost (odnosno dostupnost osigurana dovoljnim brojem resursa i količinom povezanosti)[39].

Sedmo poglavlje tiče se sigurnosti. Navedeno je kako ne postoji skup sigurnosnih standarda koji može nadjačati sve postojeće i teoretske prijetnje[40], međutim opisani su opći ciljevi koje se propisivanjem standarda želi postići, a to su: zaštita ključnih elemenata glasačkog sustava, uspostava i održavanje kontrole, zaštita sustava od manipulacije i prijevare, identificiranje neovlaštenih promjena u sustavu te zaštita tajnosti tijekom procesa glasovanja. Brojni standardi navedeni u ovom poglavlju odnose se na sve aspekte sustava, uključujući kontrolu pristupa te mjere fizičke, programske i telekomunikacijske sigurnosti.

Osmo i deveto poglavlje odnose se na osiguranje kvalitete i upravljanje konfiguracijom. Osiguranje kvalitete osmišljeno je kao neprekidan proces kojim bi se smanjila ovisnost kvalitete o testovima sustava koji se izvršavaju tek na kraju životnog ciklusa. Dužnost je proizvođača smisliti i implementirati program osiguranja kvalitete, a minimalni zadaci koji se od programa očekuju su definiranje procedura nabave i pregleda dijelova i materijala potrebne kvalitete, izrada dokumentacije za opremu i programsku podršku, definiranje zahtjeva za pravilnu izgradnju i sastavljanje opreme te instalaciju programske podrške, definiranje procedura provjere prihvatljivosti i utjecaja na okoliš te čuvanje podataka potrebnih za

[37] Ibid. 67.
[38] Ibid. 91.
[39] Ibid. 105.
[40] Ibid. 113.

dokumentiranje inspekcija[41]. Upravljanje konfiguracijom sličan je proces, definiran kao skup aktivnosti i praksa koji osigurava potpuno razumijevanje i kontrolu komponenta sustava, od početnog razvoja sve do trenutnog održavanja i poboljšanja; konkretne procedure nisu navedene, već je na proizvođaču da ih odredi[42]. Specificiranje ovih procedura neophodno je za dobivanje EAC-ovog certifikata.

Drugi svezak, Smjernice za testiranje i nacionalnu certifikaciju (*National Certification Testing Guidelines*), dopunski je dokument koji sadrži pregled i detalje procesa testiranja radi dobivanja certifikata[43]. Gotovo svi zahtjevi navedeni u prvom svesku u jednom su trenutku podložni testiranju. Drugi je svezak namijenjen prvenstveno proizvođačima, laboratorijima za testiranje te izbornim dužnosnicima koji ovjeravaju glasačke sustave[44].

U EAC-ovim smjernicama mnogi se zahtjevi i smjernice spominju više puta – primjer je sigurnost koja je navedena kao opći zahtjev, ali naglašena i u posebnom poglavlju iz fizičkog, programskog i telekomunikacijskog aspekta. Iz ovog razloga (detaljnog pogleda iz više perspektiva), ali i zbog svoje preskriptivne prirode, EAC-ove su smjernice opsežniji dokument od standarda propisanih od Vijeća Europe. Ipak, kako je u SAD-u ujednačavanje kvalitete i vrsta glasačkih sustava i opreme jedan od glavnih zadataka EAC-a, propisan i zakonom, a europske se države samovoljno (i prema mogućnostima) okreću elektroničkom glasovanju, za pretpostaviti je kako su EAC-ove smjernice mjerodavnije od standarda Vijeća.

4.3. Opće značajke sustava za elektroničko glasovanje

Svi zahtjevi, standardi, smjernice i preporuke iz prethodnog poglavlja mogu se objediniti u neke opće značajke sustava za elektroničko glasovanje, često navođene u mnogim predloženim modelima sustava, studijama slučaja i sličnim radovima. Temelj ispravnog i održivog modela elektroničkog glasovanja leži u ispravnoj identifikaciji glasača, ispravnom procesu bilježenja glasa, te ispravnom prebrojavanju glasova nakon zatvaranja glasovanja – ako se greška potkrade tijekom bilo koje od tih triju faza, integritet cijelog izbornog procesa može biti ugrožen.

Iz tog razloga među prvim značajkama najčešće se navode preciznost i provjerljivost. Sustav se može smatrati preciznim ako u njemu nije moguće promijeniti odabir, oduzeti glas od

[41] Ibid. 147.
[42] Ibid. 153.
[43] US Election Assistance Commission. „Voluntary voting system guidelines. Vol. II“, XII.
[44] Ibid.

konačnog zbroja ili ubrojiti nevažeći glas[45]. Matematički gledano, krajnji rezultati izbora moraju biti zbrojevi namijenjenih glasova koje su dali svi glasači koji su sudjelovali, što znači da rezultati moraju biti točan zbroj glasova u (elektroničkoj) glasačkoj kutiji te svaki glas u toj kutiji mora ispravno predstavljati izbor glasača[46]. Ne postoji sustav koji je u stanju spriječiti sve vrste krivo označenih listića[47]; ipak, značajka provjerljivosti postoji kako bi se greške svele na minimum. Pojedinačna provjerljivost odnosi se na mogućnost glasača da se uvjeri u ispravnu zabilježbu svojeg glasa, a univerzalna provjerljivost na mogućnost provjere zbroja svih danih glasova[48]. Iz tog je razloga u sklopu nekih sustava uključen poseban sustav provjere, VVPAT (engl. *Voter-Verified Paper Audit Trail*), kojim se provjerava ispravnost preuzimanja i pohrane glasova, otkrivaju prijevare i kvarovi te omogućuje nadzor cjelokupnog sustava[49].

Ipak, iduća značajka elektroničkih sustava izostanak je papirnatog traga. Postojanje papirnatog traga značilo bi mogućnost da se glasača poveže s njegovim odabirom, čime se ugrožavaju tajnost i integritet izbora, ali i povećanu mogućnost kupnje glasova. Nijedan sustav glasovanja ne može spriječiti kupnju glasova, no potrebno je u što većoj mjeri smanjiti privlačnost takvih aktivnosti, što je cilj koji se može smatrati dosegnutim kad kupac ne može biti siguran u uspjeh svojih namjera[50].

S ovime je povezana i iduća značajka elektroničkih sustava – privatnost. Privatnost jamče sustavi koji sprečavaju treću stranu da poveže glasača s njegovim odabirom te glasaču ne pružaju mogućnost da dokaže svoj odabir[51]. Postojanje papirnatog traga, primjerice u slučaju korištenja VVPAT-a, korisno je za preciznost i provjerljivost, međutim istovremeno povećava mogućnost povrede privatnosti. Također, sustavi za elektroničko glasovanje pod stalnom su prijetnjom računalnih napada kojima su najčešći ciljevi krađa osobnih podataka i izborna prijevara, stoga je neophodno osigurati privatnost kriptografskim algoritmima.

Naposljetku, sustav mora potvrditi identitet glasača kako bi se utvrdilo ima li pravo glasa, što znači da je provjera podobnosti također jedna od značajki koje sustav mora imati. Pravo glasa imaju oni glasači koji ispunjavaju prethodno definirane kriterije, što svaki sustav za

[45] Anane, Freeland i Theodoropoulos, „e-Voting Requirements and Implementation“, poglavlje 2.1.
[46] Gerck, et al. „The business of electronic voting“, 251.
[47] Ibid.
[48] Anane, Freeland i Theodoropoulos, poglavlje 2.1.
[49] CARNet, CERT, LS&S, „Sigurnost elektroničkog glasovanja“, 14.
[50] Gerck, et al. 252.
[51] Anane, Freeland i Theodoropoulos, poglavlje 2.1.

glasovanje mora prepoznati te u isto vrijeme osigurati da svaki glasač može dati glas dogovoreni broj puta[52] (najčešće jednom).

Osim navedenih značajki koje se odnose na opću sigurnost i anonimnost, ponegdje se navode i značajke sustava kao implementiranog proizvoda. Prije svega, sustav mora biti skalabilan, odnosno mora biti u mogućnosti prilagoditi se veličini pohrane, broju korisnika i ostalim parametrima, te mora biti praktičan, odnosno ne smije sadržavati pretpostavke i zahtjeve koji bi se teško mogli implementirati u većim razmjerima[53]. Sustav također mora moći podržati više korisnika u isto vrijeme, održavati više istovremenih izbornih procesa, biti dostupan u bilo koje doba te imati visoku dostupnost tijekom izborne kampanje[54].

4.3.1. Entiteti

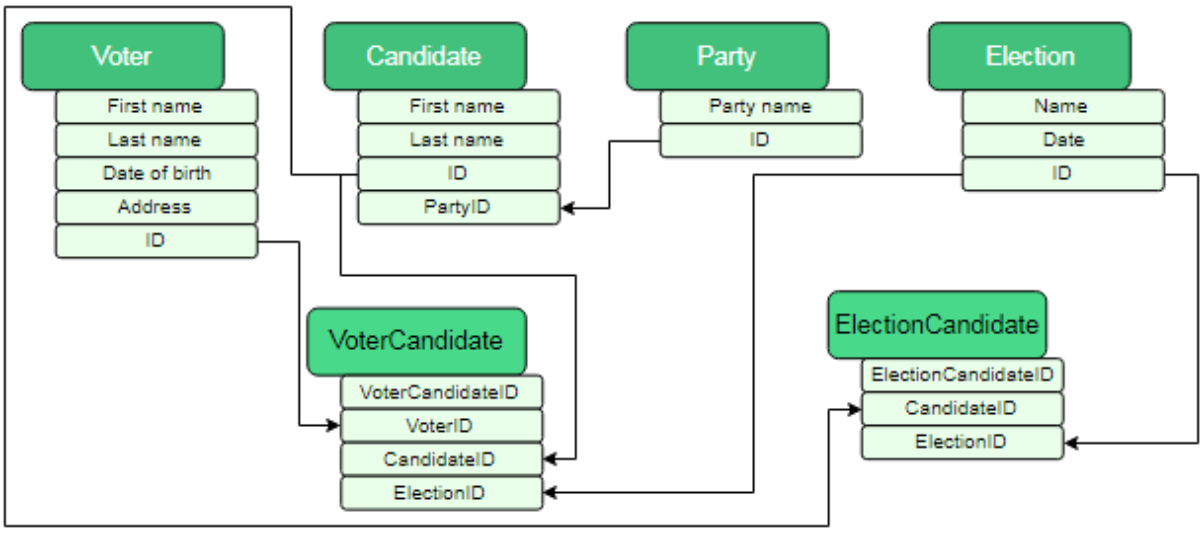
Generički model glasovanja najčešće se sastoji od sljedećih entiteta: glasač (engl. VOTER), kandidat (CANDIDATE), administrator (AUTHORITY) i neprijatelj (ADVERSARY)[55], od kojih su VOTER i CANDIDATE entiteti koji se lako mogu opisati u bazi podataka. Konkretni modeli glasovanja mogu se ipak razlikovati; razlike su najčešće u entitetu AUTHORITY, koji se, ovisno o modelu, može podijeliti na više podvrsta. Tako je u jednom modelu AUTHORITY podijeljen na entitet administratora (ADMINISTRATOR) i brojača glasova (TALLIER)[56]. I samo glasovanje, odnosno izbor, može tvoriti entitet (ELECTION), u slučaju održavanja više istovremenih izbora, što je navedeno kao primjer u drugom modelu[57].

Iako svaki od entiteta predstavlja vitalni dio glasačkog modela (uključujući i ADVERSARY, čije je namjere, mogućnosti i ciljeve potrebno dobro poznavati i eliminirati ili u što većoj mjeri umanjiti), glasovanje bi teško imalo smisla bez entiteta VOTER. Ovaj entitet predstavlja glasače (koji su primarni korisnici sustava) te kao atribute sadrži osobne podatke koji su potrebni za identifikaciju glasača, kao što su ime, prezime, datum rođenja, adresa i sl., no i jedinstvenu identifikacijsku oznaku kojom će se jedan element, odnosno glasač, jedinstveno identificirati i razlikovati od drugih; u velikom broju slučajeva to je niz znamenki koje tvore jedinstveni identifikacijski broj.

[52] Sampigethaya i Poovendran, „A framework and taxonomy for comparison of electronic voting schemes“, 138.
[53] Sampigethaya i Poovendran, 139.
[54] Qadah i Taha, „Electronic voting systems: Requirements, design, and implementation“, 378.
[55] Sampigethaya i Poovendran, 138.
[56] Lee i Kim, „Receipt-free electronic voting scheme with a tamper-resistant randomizer“, 393-394.
[57] Qadah i Taha, 380.

Elementi entiteta CANDIDATE predstavljaju moguće izbore između kojih glasači odlučuju. Ako se na izborima odlučuje između osoba kao kandidata, atributi koje entitet mora imati slični su onima u entitetu VOTER – potrebno je navesti barem ime, prezime i jedinstvenu identifikacijsku oznaku, no najčešće i pripadnost određenoj političkoj stranci, posebice ako se radi o izborima s preferencijalnim glasovanjem. Iz tog razloga potreban je i zaseban entitet koji predstavlja stranku (PARTY) i koji sadrži ime stranke i jedinstvenu identifikacijsku oznaku; ta se oznaka, umjesto imena stranke, pojavljuje u atributu pripadnosti stranci kod entiteta CANDIDATE. Ako se ne radi o izboru, već o referendumu u kojemu glasači biraju između dviju opcija (najčešće odgovori poput *za* i *protiv* ili *da* i *ne*), ove entitete može zamijeniti drugi koji predstavlja te odgovore, OPTION.

U bazi podataka između navedenih entiteta treba stvoriti veze. U generičkom modelu glasovanja za političke kandidate baza se može sastojati od entiteta ELECTION, VOTER, CANDIDATE i PARTY. ELECTION je entitet koji predstavlja zasebne izbore te se može sastojati od primarnog ključa i datuma – primarni je ključ informacija koja će povezati kandidate, odnosno stranke, ali i glasače, s određenim izborom. Kako više glasača i kandidata može sudjelovati na više izbora, ove su veze sadržane u zasebnim tablicama. Model podataka prikazan je na slici (1).



Slika 1: Model podataka u generičkom sustavu za elektroničko glasovanje

Od ostalih entiteta koji su dio generičkog modela, ali nisu sadržani u modelu podataka, entitet AUTHORITY zadužen je za ispravno provođenje izbora; njegovi se zadaci stoga najčešće obavljaju u pozadini te entitet ne predstavlja nužno i pojedinca. Postoje glasački modeli kojima ovaj entitet nije potreban; međutim, ti se modeli ne mogu implementirati za više od nekoliko korisnika i bez velikih troškova koji bi pokrili siguran sustav koji bi zamijenio ulogu

ovog entiteta[58]. A uloga ovog entiteta odnosi se najviše na provjeru identiteta i podobnost glasača, unos novih glasača, određivanje datuma glasovanja, provjeru valjanosti (elektroničkog) listića te prebrojavanje glasova.

Naposljetku, ADVERSARY predstavlja zlonamjeran entitet, neprijatelja, čija je namjera manipulacija izborima i/ili prebrojavanjem glasova[59]. Neprijatelj može djelovati izvan i unutar sustava – vanjski neprijatelj može djelovati tako da pokuša kupiti glasove ili drugim metodama prinuditi glasača da glasuje na određeni način, čime je ugrožena privatnost, dok unutarnji neprijatelj (koji ima pristup podacima) može pokušati izmijeniti ili otkriti broj glasova[60], čime su, osim privatnosti, ugrožene i točnost i pouzdanost, te samim time i integritet izbora. Iako su i vanjski i unutarnji neprijatelji svojstveni svim metodama glasovanja, kod sustava za elektroničko glasovanje – u kojima je velik broj povjerljivih informacija, ali i rezultat, potencijalno ugrožen – unutarnji neprijatelj predstavlja prijetnju koja je razlog implementaciji brojnih sigurnosnih standarda te jakih kriptografskih algoritama. Entitet ADVERSARY ne može se definirati unutar modela podataka, no može se predstaviti kao jedan od ranije navedenih entiteta te tako ugroziti sustav. Kako bi se to spriječilo, potrebno ga je uključiti u generički model glasovanja radi, kako je već spomenuto, predviđanja i sprečavanja njegovih namjera i djelovanja. Po uzoru na Lauera koji je opisao i svrstao rizike elektroničkog i internetskog glasovanja, neki od podataka koji se mogu prikupljati o entitetu ADVERSARY su prijetnja, posljedica, vjerojatnost te protumjere[61]; definiranje ovih vrijednosti može pomoći pri odabiru najsigurnijeg i najisplativijeg sustava.

4.3.2. Faze glasovanja

Kao i entiteti, i faze glasovanja razlikuju se od modela do modela. Njihov broj i trajanje ovise ponajviše o opsegu glasovanja – primjerice, radi li se o internim izborima u određenoj ustanovi ili političkim izborima na razini države. Opseg glasovanja utječe na vrijeme provedeno na autentifikaciju pojedinca, identifikaciju mogućih sigurnosnih prijetnji te ulaganje u zaštitu sustava i podataka, vrijeme potrebno za ujedinjenje i prebrojavanje glasova i sl. Ipak, većina modela elektroničkog glasovanja na bilo kojoj razini ne razlikuje se mnogo od modela klasičnog glasovanja te se može podijeliti u tri faze: fazu registracije, fazu glasovanja te fazu prebrojavanja glasova.

[58] Riera, „An introduction to electronic voting schemes“, 3.
[59] Sampigethaya i Poovendran, 138.
[60] Ibid.
[61] Lauer, „The risk of e-voting“, 181.

Faza registracije pripremna je faza u kojoj se provodi niz aktivnosti kojima se poduzimaju sve mjere kako bi druga i treća faze bile ispravno provedene. Jedna od aktivnosti koje uključuje ova faza jest stvaranje, objavljivanje i ažuriranje popisa birača. U nekim je državama, poput Hrvatske, evidencija birača i njihovih podataka (dijelom) dužnost i suradnja policijskih uprava i drugih institucija te registracija birača nije potrebna (osim iznimaka poput prebivanja izvan države i sl.); u drugim državama, primjerice u SAD-u[62], birač je sam dužan obaviti registraciju. Potrebno je objaviti i listu kandidata između kojih će glasači birati. U ovoj je fazi potrebno odrediti i biračka mjesta te na njima osigurati, dostaviti i instalirati glasačku opremu. Također je potrebno odabrati odgovarajuće sigurnosne računalne protokole – ovo je opsežna aktivnost koja uključuje implementaciju kriptografske metode za osiguravanje privatnosti i tajnosti glasovanja, a u nekim se modelima spominje i osmišljavanje sredstva autentifikacije korisnika, odnosno glasača, u slučaju da je potrebno više od osobne iskaznice ili putovnice[63].

Faza glasovanja odvija se na dan(e) izbora. Glasači dolaze na ranije određeno biračko mjesto (ako se ne radi o internetskom glasovanju) te se prije samog glasovanja vrši njihova identifikacija na način dogovoren u prethodnoj fazi. Tijekom samog glasovanja glasač ispunjava listić i završava svoje glasovanje, a ranije osmišljenim sigurnosnim računalnim protokolima osigurana je tajnost. Završetkom glasovanja glasač dobiva potvrdu da je njegov glas uspješno pohranjen. Izvan ove faze prihvaćanje glasova nije moguće, osim u posebnim slučajevima glasovanja unaprijed.

Faza prebrojavanja glasova počinje nakon završetka faze glasovanja. Svi glasovi pohranjeni u elektroničkoj glasačkoj kutiji te se mogu zbrojiti na licu mjesta i slati u središnju jedinicu gdje se pridodaju ostalim rezultatima, ili se šalju bez prethodnog zbrajanja. Provjerava se valjanost svakog listića i odvajaju se oni nevažeći. Razlog činjenici da se ova aktivnost najčešće odvija u ovoj fazi, a ne u prethodnoj već nakon pohranjivanja glasa, taj je što je sadržaj listića kriptiran zahvaljujući implementiranim sigurnosnim protokolima – u ovoj se fazi dekriptira njegov sadržaj te se pridodaje vrijednost rezultatima.

4.4. Kriptografske metode

Kako je već spomenuto, kriptografija se kod sustava za elektroničko glasovanje koristi iz nekoliko razloga – kriptiranje glasova, odnosno glasačkih listića i kutija, sprečavanje

[62] „Register to Vote and Check or Change Registration“.
[63] Ikonomopoulos et al. „Functional requirements for a secure electronic voting system“, 512.

mijenjanja glasova i programske podrške, verifikacija identiteta glasača prije glasovanja te pomoć pri prebrojavanju i provjeri rezultata nakon izbora[64]. Kriptografija se temelji na kriptiranju i dekriptiranju poruke, odnosno skrivanju njezinog sadržaja promjenom njezina oblika (najčešće pomoću ključa i algoritma) te ponovnom otkrivanju, što radi osoba koja zna odgovarajući ključ i algoritam. Razni kriptografski algoritmi i njihovi koraci javno su dostupni, međutim briga o tome da ključ ostane nepoznat presudna je u tome da kriptirana informacija ostane skrivena[65].

Kriptografske *hash* funkcije (u hrvatskom rjeđe poznate kao funkcije kompresije, sažimanja ili raspršivanja) matematički su algoritmi koji niz znakova bilo koje duljine komprimiraju u niz znakova (najčešće nasumičnih slova i/ili brojeva) fiksne duljine. Kako bi korištenje *hash* funkcije bilo optimalno, ne bi trebala postojati dva ista *hash* rezultata te bi funkcija trebala biti jednosmjerna[66], što znači da bi je bilo nemoguće obrnuti i tako doći do sadržaja poruke. *Hash* funkcije definirane su tako da izmjena samo jednog znaka u nizu nakon kompresije daje potpuno drugačiji rezultat, čime se smanjuje (u idealnom slučaju ionako mala) vjerojatnost da će treća, neautorizirana strana otkriti sadržaj. *Hash* algoritmi koriste se u mnogim područjima, poput provjere autentičnosti ili detekcije netočnih ili promijenjenih podataka. Iz tog su razloga *hash* funkcije korisne u sustavima za elektroničko glasovanje – štite identitet i osobne podatke glasača te osiguravaju tajnost glasovanja kriptirajući glasačev odabir. Primjena *hash* funkcija kod elektroničkih sustava može biti i šira od ovoga – budući da se kroz *hash* algoritme mogu sažeti i programi i operacijski sustavi, nadležna izborna tijela mogu na ovaj način provjeriti je li sustav ispravan prije instalacije odnosno je li odabrana prikladna verzija programa, ili postoje li potencijalne zlonamjerne modifikacije u programu[67].

Digitalni potpis (engl. *digital signature*) metoda je kojom se utvrđuje autentičnost elektroničkog dokumenta; dokument je autentičan ako je poznat njegov autor i ako je moguće dokazati da nije neovlašteno izmijenjen[68]. Taj je dokument, ili poruka, u slučaju elektroničkog glasovanja glasačev listić koji sadrži njegov odabir. Nakon što je poruka provedena kroz *hash* funkciju, korisniku su potrebna dva tipa ključa, privatni i javni, koje može dobiti korištenjem algoritma digitalnog potpisa; na *hash* rezultat korištenjem privatnog ključa korisnik stvara digitalni potpis koji se šalje ili objavljuje zajedno s potpisanom porukom[69]. Privatni ključ

[64] „The Important Uses of Cryptography in Electronic Voting and Counting".
[65] Ibid.
[66] Preneel, „Analysis and design of cryptographic hash functions", 18.
[67] „The Important Uses of Cryptography in Electronic Voting and Counting".
[68] CARNet, CERT, LS&S, „Digitalni potpis", 4.
[69] Ibid.

služi korisniku kako bi se poruka kriptirala, a javni ključ služi primatelju koji pomoću njega može utvrditi vjerodostojnost poruke i digitalni potpis pošiljatelja. Za svaku poruku digitalni potpis može biti drugačiji, čime je znatno otežano krivotvorenje korisnikovog potpisa[70]. Poseban oblik digitalnog potpisa jest slijepi potpis (engl. *blind signature*), kod kojeg se sadržaj poruke skriva od potpisnika[71]. To je slučaj s elektroničkim glasovanjem – osim glasača pojedinca, nikome nije predviđeno da vidi koga ili što je glasač odabrao, uključujući administratora, koji je ovlašten za davanje digitalnog potpisa. Tipičan model glasovanja koji sadrži slijepi potpis sastoji se od dvaju sudionika, korisnika (glasača) i administratora, te od triju faza – inicijalizacije, registracije i glasovanja. U fazi inicijalizacije administrator priprema privatni i javni ključ, dok u fazi registracije mora identificirati glasača te mu pružiti pristup listiću, koji je potpisan slijepim potpisom; u fazi glasovanja glasač daje svoj glas koji se anonimnim kanalima šalje administratoru, koji zatim listić ovjerava[72].

Anonimnost tih kanala osigurana je korištenjem još jedne metode – miješane mreže (engl. *mix networks* ili skraćeno *mix-nets*). Miješane mreže oblik su anonimne komunikacije u kojoj poruke putuju preko jednog ili više posredničkih poslužitelja (engl. *proxy servers*), od kojih svaki sadrži ključ kojim će se poruke dodatno kriptirati te koji ih zatim šalju idućem poslužitelju, ali pomiješanim i nepredvidivim redoslijedom. Poruka se kriptira ključem svakog od poslužitelja prije nego što je poslana, kako bi se putem do cilja mogla na svakom poslužitelju dekriptirati odgovarajućim ključem. Nakon što poruka stigne do cilja, poruka je dekriptirana, no njezinom pošiljatelju nije moguće ući u trag zbog pomiješanog puta poruke, odnosno nepredvidivosti poslužitelja kroz koje je prošla[73]. Iz tog je razloga očita uloga miješanih mreža u sustavima za elektroničko glasovanje – budući da je izvorni podatak o glasu kriptiran i prije prolaska kroz miješanu mrežu, a ponovno kriptiran prolaskom kroz nju, čak i nakon gornjih slojeva dekripcije ne može se povezati kriptirani glas sa izvornim oblikom ni sa identitetom glasača[74].

Homomorfna kriptografija (engl. *homomorphic encryption*) također se koristi kako bi se sačuvala tajnost glasovanja. Homomorfna kriptografija omogućuje izravno računanje nad kriptiranim podacima bez da je potreban pristup privatnom ključu[75]. Za elektroničko glasovanje to znači da se glasovi mogu zbrajati u elektroničkoj glasačkoj kutiji dok su još

[70] „The Important Uses of Cryptography in Electronic Voting and Counting“.
[71] CARNet, CERT, LS&S, „Digitalni potpis“, 9.
[72] Fan i Sun, „An efficient multi-receipt mechanism for uncoercible anonymous electronic voting“, 1612.
[73] Furukawa, Mori i Sako, „An implementation of a mix-net based network voting scheme and its use in a private organization“, 142.
[74] „The Important Uses of Cryptography in Electronic Voting and Counting“.
[75] „Introduction.“

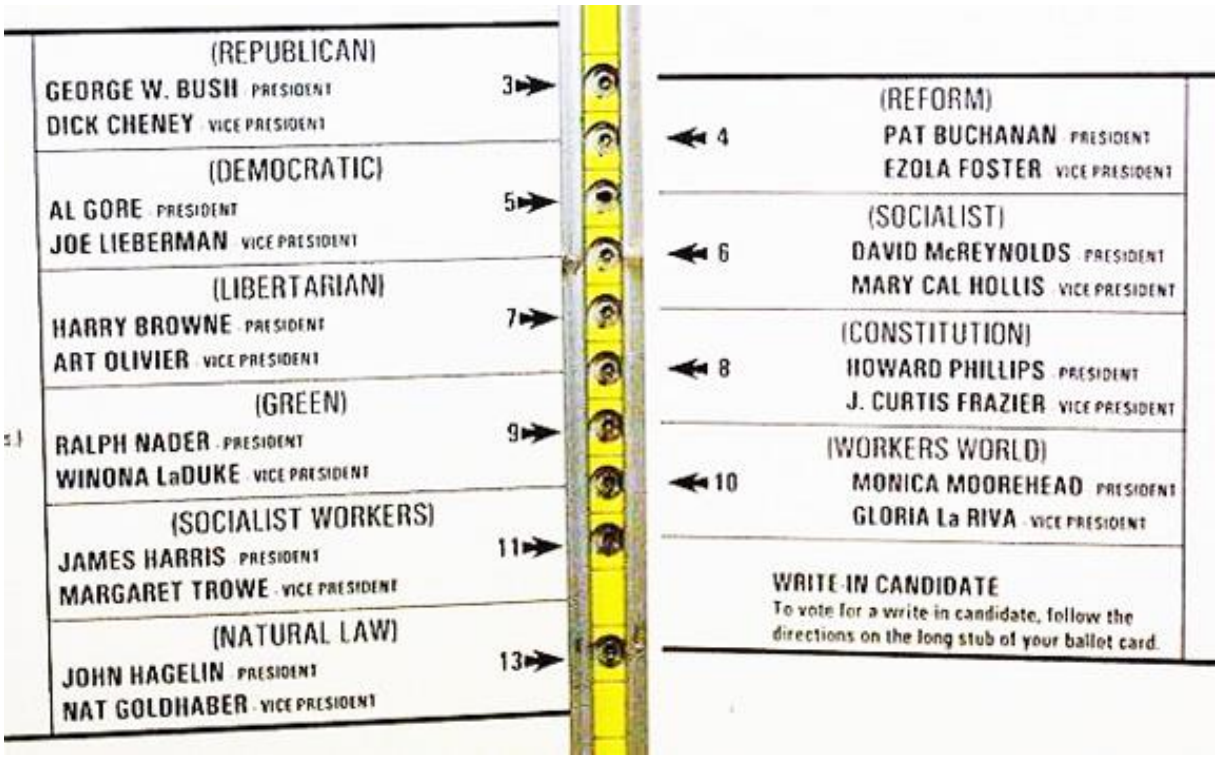
uvijek kriptirani[76], čime se ubrzava proces prebrojavanja glasova, a anonimnost i tajnost su sačuvane. Nakon glasovanja nadležna izborna tijela dekriptiraju i objavljuju konačan rezultat, a moguće je objaviti i dokaz da je dekriptiranje ispravno izvršeno, što zatim glasači i promatrači mogu provjeriti[77].

4.5. Prednosti sustava za elektroničko glasovanje

Korištenje tehnologije – računala i interneta – donijelo je mnoga poboljšanja u gotovo svim područjima djelovanja, pa tako i u mnogim administracijskim i birokratskim procesima koji se izravno tiču građana neke države. Kao što je poznato, temelj demokracije leži u izborima i pravu glasa, stoga je važno poduzeti sve moguće mjere kako bi se povećao odaziv birača na referendume i izbore, posebice one na državnoj razini. Kako se tehnologije razvijaju, smišljaju se i novi načini manipulacije, hakiranja i zlouporabe, stoga se ni za jedan sustav za glasovanje ne može reći da je u potpunosti zaštićen od prijetnji. Da bi se uvelo elektroničko glasovanje, prednosti moraju nadjačati nedostatke za barem jednu od dviju grupa koje su pod njegovim izravnim utjecajem, a to su glasači i vlasti[78]. Kvalitetno osmišljeni, osigurani i praktični sustavi za elektroničko glasovanje sadrže određene prednosti kojima značajno mogu pridonijeti boljem, bržem i učinkovitijem obavljanju svih vrsta poslova koji stoje iza izbornog procesa, te privući glasače da iskoriste svoje biračko pravo.

Jedna od prednosti koju sustavi za elektroničko glasovanje imaju nad ostalim metodama glasovanja jest lakoća korištenja. Za uvođenje svakog novog sustava potrebno je uložiti u edukaciju glasača kako bi pravovremeno mogli biti upoznati s načinom korištenja sustava, no današnje društvo u velikoj mjeri koristi računala u mnogim aspektima života, stoga je očekivana brza prilagodba korisnika. Jednom kad je sustav u upotrebi, njegovo sučelje te vođenje glasača kroz proceduru na način koji je istovremeno intuitivan i nedvosmislen (i imati opciju prikazivanja na više jezika) mogu korisniku pružiti veću sigurnost korištenja nego papirnati listići ili bušene kartice; vraćajući se na kontroverzne predsjedničke izbore 2000. godine u SAD-u, jedan od okruga koristio je listiće čiji je zbunjujući dizajn prikazan na slici (2), što bi se teško moglo realizirati na računalu:

[76] „The Important Uses of Cryptography in Electronic Voting and Counting“.
[77] Okediran et al. „A comparative study of generic cryptographic models for secure electronic voting“, 45.
[78] „Arguments in Favor“.



Slika 2: Dizajn glasačkog listića na američkim predsjedničkim izborima 2000.

Udaljeno glasovanje (glasovanje telefonom) i internetsko glasovanje kao podvrste elektroničkog glasovanja također omogućuju lakoću korištenja, ali i pristupačnost – ona sadrže potencijal da se smanje dugački redovi na biračkim mjestima i olakša proces skupinama glasača kojima je otežana mogućnost glasovanja – bolesnima, glasačima u inozemstvu, samohranim roditeljima, osobama s posebnim potrebama i ostalima koji iz određenih razloga ne mogu doći na tradicionalno biračko mjesto[79]; osobama s posebnim potrebama na ovaj je način osigurana veća tajnost glasovanja, čime se naposljetku poštuje jednako pravo glasa, jedan od temeljnih principa koje sustavi za elektroničko glasovanje moraju poštovati. Udaljeno i internetsko glasovanje također sadrže potencijal povećanja odaziva birača, posebice onih u dobi od 18 do 30 godina, budući da ta skupina, do koje je najteže doprijeti, najviše koristi tehnologiju – računala, internet i telefone – koja se ovdje koristi[80].

Pristupačni sustavi, lagani za korištenje, povlače za sobom učinkovitost. Koristeći uređaje za elektroničko glasovanje, glasači se mogu pouzdati u to da će se njihov glas računati; tako će se izbjeći problemi koji se često pojavljuju kod drugih metoda, primjerice popunjavanja rupa ostacima papira kod bušenih kartica i, posljedično, otežanom ili polovičnom bušenju listića za

[79] „A Comparative Assessment of Electronic Voting“.
[80] Ibid.

koje je kasnije teško odrediti jesu li valjani, što na kraju vodi do neizvjesnih i diskutabilnih rezultata izbora. Također, uređaji mogu biti programirani tako da spriječe glasača da odabere premalo ili previše kandidata, čime bi se povećala opća učinkovitost glasovanja[81].

Korištenje računala za prebrojavanje glasova znači brže i pouzdanije prebrojavanje glasova i stoga točnije rezultate. Kako je već navedeno, pomoću homomorfne kriptografije moguće je zbrajati glasove već na licu mjesta, u elektroničkoj glasačkoj kutiji na biračkom mjestu, a slučaju da se glasovi šalju u središnju jedinicu prije objedinjenog prebrojavanja, i taj je način brži nego što bi to bilo ručno prebrojavanje glasova, koje sa sobom nosi i rizik pogreške.

Naposljetku, nedostatak papirnatog traga kao značajka ovih sustava također predstavlja prednost tako što je smanjena mogućnost povezivanja glasača s njegovim odabirom, odnosno povećana tajnost i anonimnost, stoga se smanjuje i količina zlouporabe u smislu kupovanja glasova. Osim rizika, korištenje VVPAT-a povisilo bi i troškove[82], a glasaču ne bi u potpunosti pružilo informaciju da je njegov glas zabilježen, što je informacija koja je glasaču najbitnija[83].

4.6. Nedostaci sustava za elektroničko glasovanje

Prednosti svakog izuma, modela i sustava, pa tako i onog za elektroničko glasovanje, zapravo su ciljevi smišljeni tijekom planiranja i mogu se unaprijed odrediti, a neke se nedostatke također unaprijed može predvidjeti i eliminirati. Međutim, tek nakon implementacije i tijekom upotrebe na vidjelo dolaze stvarni problemi i mane sustava. Također, ono što se smatra prednošću, u određenoj situaciji ili kontekstu može predstavljati nedostatak.

Primjerice, izostankom papirnatog traga eliminiraju se i troškovi tiskanja i distribucije; međutim, potrebno je izdvojiti financijska sredstva za računala, kojih, ovisno o veličini grada ili države u kojoj se uvode, može biti mnogo te trenutačna financijska nemogućnost može prevladati nad eventualnom dugoročnom koristi. Financijska su sredstva potrebna i za sam razvoj i održavanje sustava, odnosno brojne jednokratne i ponavljajuće troškove poput dozvola za licence, izgradnje infrastrukture, sigurnosnih revizija i sl.[84] Usto, u slučaju kvara opreme ili programske podrške, nepostojanje papirnatog traga moglo bi značiti nepovratni gubitak glasova, čime je ozbiljno ugrožen integritet izbora.

[81] „Arguments in Favor“.
[82] Castro, „Stop the presses: How paper trails fail to secure e-voting“, 1.
[83] Ibid. 7.
[84] „Benefits, Risks and Costs“.

Već spomenuta edukacija korisnika o korištenju sustava također može predstavljati kompliciran zadatak i veći trošak, a ne može jamčiti veći odaziv birača. Studije o korištenju elektroničkog glasovanja u nekim zemljama (primjerice u Švicarskoj[85]) pokazuju da ono nužno ne povećava izlaznost, iako se može primijetiti učestalije korištenje elektroničkog glasovanja – razlog je tomu taj što elektroničko glasovanje koriste birači koji su svejedno namjeravali glasovati; učinili bi to bez obzira na dostupnost elektroničkog glasovanja. Štoviše, uvođenje novih tehnologija može obeshrabriti i tako odbiti određene skupine glasača, primjerice glasače starije životne dobi[86], te se može stvoriti i određena količina skepticizma i nepovjerenja glasača.

Sustavi za elektroničko glasovanje podložni su različitim vrstama grešaka, računalnih napada i prijevara. Postoje razni rizici koji prijete sustavima za elektroničko glasovanje (posebice DRE uređajima koji se nalaze na biračkim mjestima) koji mogu ugroziti proces glasovanja i integritet izbora –zloćudni programi poput trojanskog konja koje može instalirati, primjerice, proizvođač, i koji mogu kompromitirati cijeli izborni proces; proces razvoja sustava koji iz određenog razloga ima status poslovne tajne te je zbog toga nad njime nemoguće vršiti testiranja; nepostojanje standarda, što također onemogućuje odgovarajuće testiranje sustava; nedostatak nadzora konfiguracije, što može dovesti do promjena u konfiguraciji i samim time kompromitirati sustav; te neispravna programska podrška koja može dovesti do grešaka poput višestrukog glasovanja[87].

Internetsko glasovanje također sa sobom nosi određene rizike; štoviše, smatra se podložnijim napadima od elektroničkog glasovanja na biračkim mjestima[88], budući da se glasovanje odvija na mjestima i uređajima koji nisu pod kontrolom nadležnih izbornih tijela, stoga sigurnost uvelike ovisi o uređaju koji se koristi za glasovanje te mreži na koju je spojen. Napadi se mogu dogoditi na klijentskom uređaju, gdje, primjerice, virus može promijeniti glasačev odabir prije enkripcije ili autentifikacije. Napadi se mogu dogoditi i na komunikacijskoj razini, gdje napadač može glasaču poslati naizgled autentičnu, ali lažiranu internetsku stranicu te mu tako oduzeti, odnosno ukrasti glas, te na glavnom poslužitelju, gdje napadač može izvesti napad uskraćivanjem resursa (DoS napad, engl. *denial of service attack*)[89].

[85] Germann i Serdült. „Internet voting and turnout: Evidence from Switzerland“, 9.
[86] Roseman i Stephenson, „The effect of voting technology on voter turnout: Do computers scare the elderly?“, 45.
[87] Lauer, 181.
[88] Burmester i Magkos, „Towards secure and practical e-elections in the new era“, 67.
[89] Ibid.

Jasno je da su sigurnosni rizici najveći nedostatak sustava za elektroničko glasovanje. Mogućnost krađe glasa, ali i identiteta, može uliti nepovjerenje i odbiti glasače od korištenja ove metode. Također, dok su kod drugih metoda, temeljenih na papiru, moguće prijevare manjih razmjera, kod elektroničkog glasovanja velika je mogućnost prijevare velikih razmjera, zbog automatizacije i mrežne povezanosti[90], što sve zajedno dovodi do zaključka da svi osnovni principi glasovanja – transparentnost, tajnost, anonimnost, nedokazivost i integritet – mogu biti ugroženi.

[90] Ibid. 66.

5. Sustavi za elektroničko glasovanje u svijetu

Od pojave DRE uređaja i internetskog glasovanja, brojne su države eksperimentirale s uvođenjem elektroničkog glasovanja, a još ih je više razmatralo, ili razmatra i danas. Ne postoje konkretni i potpuno ažurni podaci o elektroničkom glasovanju diljem svijeta – posebice jer se u nekim slučajevima i optičko skeniranje smatra tipom elektroničkog glasovanja – no nekoliko država već dulje vrijeme službeno provodi izbore na ovaj način, a to su Indija, Brazil, Venezuela, Estonija (koja jedina koristi internetsko glasovanje u znatnoj mjeri) i SAD (gdje ipak ne podržavaju sva područja elektroničko glasovanje, zbog različitih zakona svake savezne države). Prema podacima iz 2018. godine, veći broj država u nekom je periodu testirao sustave za elektroničko glasovanje – Ujedinjeno Kraljevstvo, Australija, Filipini, Rusija, Mongolija, Finska, Švicarska itd.[91] Postoje i države u kojima je odlučeno da se sustavi za elektroničko glasovanje ipak neće koristiti – to su Francuska, Nizozemska, Njemačka, Paragvaj i Japan[92] (Belgija je ovdje također navedena kao jedna od zemalja koje su odustale od elektroničkog glasovanja, no nakon gašenja starog sustava koji se koristio od 1990-ih godina, 2012. je godine uveden novi). Za potrebe ovog rada odabrane su tri države u kojima se koristi elektroničko glasovanje: SAD kojemu implementacija elektroničkog (i bilo kojeg drugog) sustava predstavlja izazov zbog, između ostaloga, veličine i različitih saveznih zakona, Estonija kojoj je u kratko vrijeme od uvođenja internetskog glasovanja do danas pripisan status vodeće države u toj metodi glasovanja, te Belgija koja s nešto većim uspjehom od SAD-a koristi elektronički sustav, no uz veću zadršku od Estonije.

5.1. Sjedinjene Američke Države

Notorni predsjednički izbori 2000. godine (na kojima je pobjednik proglašen mjesec dana nakon glasovanja zbog, između ostaloga, poteškoća u glasovanju putem bušenih kartica i kasnije u njihovom prebrojavanju) skrenuli su pozornost na potrebu za procjenom uporabljivosti glasačkih sustava te ubrzali uvođenje elektroničkih sustava diljem SAD-a[93]. DRE uređaji već su bili u upotrebi i prije 2000. godine, no nakon toga njihovo se korištenje ubrzano širilo zemljom, budući da je postojala potreba za drugačijom i, kako se činilo, pouzdanijom i sigurnijom tehnologijom. Međutim, provedena su istraživanja koja su upozoravala na rizike prebrzog prelaska na DRE uređaje zbog neriješenih inženjerskih

[91] Laukkonen, „Which Countries Use Electronic Voting?“.
[92] Ibid.
[93] Herrnson et al. „The current state of electronic voting in the United States“, 157.

izazova, unutarnjih prijetnji, ranjivosti mreže i problema s revizijom[94]. Kako bi se uveo red u provođenju budućih američkih izbora, donesen je zakon HAVA kojim se nastojalo zamijeniti stare i nepouzdane metode glasovanja novijima; HAVA je prepoznavala potencijal elektroničkih sustava, no i brojne nedostatke uzrokovane neusustavljenošću, stoga se ovim zakonom zahtijevala i izrada detaljnih smjernica koje elektronički sustavi moraju poštovati kako bi bili što sigurniji za korištenje. Na sljedećim predsjedničkim izborima, održanim 2004. godine, bilo je, prema anegdotalnim dokazima, znatno manje kontroverznih situacija – prije svega, za razliku od prošlih izbora, „pobjednik je proglašen bez znatnog kašnjenja te nije bilo prosvjeda oko rezultata ili načina na koji su izbori provedeni u bilo kojoj od 50 saveznih država“[95], što znači da elektronički sustavi mogu ispraviti nedostatke koje imaju bušene kartice i druge metode. Međutim, prijavljene su poteškoće s rukovanjem uređajima te neispravna bilježenja glasova[96], što dokazuje da korištenje elektroničkih sustava još nije u potpunosti razrađeno, sigurno i pouzdano. To su potvrdili i kongresni izbori 2006. godine, tijekom kojih se pojavio niz problema – u jednom od okruga na Floridi od oko 18 000 danih glasova na nekim od uređaja nije zabilježen nijedan[97], a nakon revizije predizbora u jednom okrugu na području Ohija otkriveno je da se rezultati, koje korišteni uređaji mogu dati na četiri načina pomoću VVPAT-a, ne podudaraju[98].

Ti su problemi dali povoda daljnjim istraživanjima, no s drugačijim pristupom – umjesto skupnih analiza sustava podijeljenih po vrsti, istraživanja su se odvijala nad pojedinačnim sustavima, čime se jednostavnije moglo otkriti kako korisnici reagiraju na njih, odnosno jesu li konkretni sustavi jednostavni za korištenje, točni i pouzdani[99]. Rezultati su pokazali da, iako iskustva korisnika u određenoj mjeri ovise o nekim njihovim temeljnim karakteristikama, veća točnost pri bilježenju namjera glasača (odnosno manji broj grešaka) i njihovo povjerenje u proces može se postići nekim modifikacijama u sustavu[100]. Neki su proizvođači uzeli rezultate ovih istraživanja u obzir i uveli poboljšanja u svoje sustave; međutim, činjenica da se glasači susreću s problemima prilikom korištenja elektroničkih sustava upućuje na to da je potreban još veći napredak[101].

[94] Kohno et al. „Analysis of an electronic voting system“, 3.
[95] Herrnson et al. 162.
[96] Ibid.
[97] „The United States“.
[98] Election Science Institute, „DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio“.
[99] Herrnson et al. 165.
[100] Ibid. 175.
[101] Ibid.

Internetsko glasovanje smatra se još nepouzdanijim od elektroničkog glasovanja na biračkim mjestima. Prijedlozi o testiranju internetskog glasovanja na pravim izborima također se, neovisno o upozorenjima stručnjaka, često pojavljuju u SAD-u[102]. Ipak, ne razmatra se potpuno uvođenje internetskog glasovanja, ni sada ni u bliskoj budućnosti – trenutno se ono najviše koristi za državljane koji su svrstani pod Zakonom o glasovanju u odsustvu za građane u uniformi i u inozemstvu (engl. *Uniformed and Overseas Citizens Absentee Voting Act,* UOCAVA)[103], dakle građane koji nisu u mogućnosti fizički doći na biračko mjesto, najčešće zbog službenih obveza. Od 50 saveznih država, 24 (brojeći District of Columbia, 25) omogućuje tim glasačima slanje listića preko internetskog portala, mobilne aplikacije ili elektroničke pošte, njih 7 dopušta slanje samo telefaksom, a njih 19 ne dopušta slanje elektroničkim putem, već je potrebno poslati glas poštom[104]. Dosad su osmišljena dva značajnija projekta s ciljem implementiranja njihovih sustava za internetsko glasovanje u SAD-u: SERVE i Operation BRAVO[105]. Cilj projekta SERVE (*Secure Electronic Registration and Voting Experiment*) bio je omogućiti glasačima korištenje bilo kojeg računala s Windows operacijskim sustavom za glasovanje na predizborima i općim izborima 2004. godine, a briga o sigurnosti računala preko kojeg će glasovati pala je na glasače[106]. Zbog očitih sigurnosnih rizika te izvještaja skupine stručnjaka koji je, nakon evaluacije sustava, preporučio trenutno gašenje sustava, ali i izostanke sličnih pokušaja „dok internet i računalne infrastrukture diljem svijeta ne budu preuređene iz temelja, ili dok se ne pojave neočekivana sigurnosna otkrića“[107]. Operation BRAVO (*Bring Remote Access to Voters Overseas*), s druge strane, bio je projekt s ciljem da izbjegne sigurnosne rizike koje sa sobom nosi slanje osjetljivih podataka preko interneta, stoga je glasačima pod UOCAVA-om osigurao glasačke kioske koji su izdavali i papirnate potvrde; elektronički listići bili bi poslani preko virtualne privatne mreže, a potvrde doputovale do okruga Okaloosa na Floridi gdje se projekt i odvijao; otkrivene su diskrepancije između rezultata dobivenih elektroničkim listićima i onim papirnatim, no i osiguravanje velikog broja kioska za sve glasače bio bi velik financijski i logistički problem, stoga je projekt napušten[108].

Današnje stanje također obilježavaju mnogi problemi – primjer su posljednji predsjednički izbori, 2016. godine, kad su zabilježeni kvarovi strojeva i nepostojanje organiziranog

[102] Simons i Jones, „Internet voting in the US“, 76.
[103] „Electronic Transmission of Ballots“.
[104] Ibid.
[105] Simons i Jones, 71.
[106] Ibid. 72.
[107] Ibid.
[108] Ibid.

alternativnog načina glasovanja[109] te uplitanje ruske vlade u cijelu izbornu kampanju i proces[110]. Potonji događaj problematika je koja je mnogo šira od biranja najprikladnijeg sustava glasovanja na američkim izborima, no, uzevši u obzir navedene postojeće probleme s elektroničkim sustavima i samu veličinu države – unutar koje svaka savezna država ima svoje zakone vezane za glasovanje – vrlo je kompliciranо razviti jedinstveni sustav za elektroničko glasovanje koji bi bio pouzdan, lagan za korištenje i zaštićen od različitih vrsta napada.

5.2. Estonija

Estonija se smatra pionirskom državom u korištenju informacijskih i komunikacijskih tehnologija za javne usluge[111], uključujući i glasovanje. Internetsko glasovanje uvedeno je 2005. godine na lokalnim izborima te je Estonija postala prva država u kojoj se glasovalo preko interneta na razini cijele države[112] (za razliku od SAD-a, gdje je uvedeno ranije, no nije omogućeno svim glasačima). Prijedlog o uvođenju internetskog glasovanja prvi je put objavljen 2001. godine, a budući da su već u upotrebi bile razne digitalizirane usluge poput e-bankarstva, bespapirno poslovanje vlade, SMS-parkinga i sl., digitalizirano glasovanje činilo se kao očit korak dalje[113]. Uvođenje internetskog glasovanja većinom su podržavali i političari, gledajući na njega, između ostaloga, kao sredstvo privlačenja novih glasača. Preskočen je korak uvođenja DRE uređaja na biračka mjesta, budući da je Estonija već imala razvijen internetski izborni informacijski sustav kojim se ubrzavala obrada glasova i drugih izbornih podataka, stoga se pod pojmom elektroničkog glasovanja u slučaju Estonije misli isključivo na internetsko (udaljeno) glasovanje. Uvođenju su pogodovale još dvije činjenice: Estonci su mogli glasovati na bilo kojem od biračkih mjesta, ne samo na jednom predodređenom, te su u međuvremenu uvedene osobne iskaznice s čipom, koje su sadržavale dva para ključeva, jedan za autentifikaciju i jedan za digitalni potpis[114], čime je omogućeno elektroničko potvrđivanje identiteta. Danas Estonci mogu glasovati i putem mobitela, pomoću posebne SIM kartice koja također ima mogućnost autentifikacije i digitalnog potpisa; ovaj se sustav zove Mobile-ID[115].

[109] DeMille, „Voting machine issues complicate balloting in Washington County“.
[110] Miller i Entous, „Declassified report says Putin ‘ordered’ effort to undermine faith in U.S. election and help Trump“.
[111] Drechsler i Madise, „Electronic voting in Estonia“, 97.
[112] Springall et al. „Security analysis of the Estonian internet voting system“, 1.
[113] Drechsler i Madise, 99.
[114] Springall et al. 2.
[115] Ibid. 2.

Ipak, postojali su (teoretski) argumenti zašto se internetsko glasovanje ne bi trebalo uvesti. S jedne su strane bili politički – neke su se stranke bojale da će internetsko glasovanje privući birače koji inače ne bi iskoristili svoje biračko pravo te bi se tako ugrozio položaj tih stranaka, što je temeljeno na pretpostavci da će glasači, koji inače ne bi glasovali, glasovati za stranke slabijeg položaja[116]. Drugi su argumenti počivali na bojazni da internetsko glasovanje nije ni pod kakvim nadzorom te se stoga može nekontrolirano kupovati i prodavati glasove te prinuđivati glasače; također, rezultate internetskog glasovanja ne mogu provjeriti sami glasači, stoga je potrebno imati potpuno povjerenje u točnost, istinitost i zaštićenost cijelog izbornog aparata[117]. S tehnološke strane, argumenti protiv uvođenja nisu bili drugačiji od općih potencijalnih rizika koje elektronički sustavi nose sa sobom: mogućnost netočnih ili nepouzdanih podataka, povrede anonimnosti glasača, ili prekida cijelog izbornog procesa zbog, primjerice, velikih sigurnosnih problema[118].

Kako bi se dobio pregled mogućih rizika, Ministarstvo pravosuđa naručilo je nekoliko analiza vezanih za sigurnost i troškove, čiji su rezultati uzeti u obzir pri oblikovanju odredbi za internetsko glasovanje, koje su bile dio čak četiriju izbornih zakona. U nacrtu jednog od zakona predloženo je da glasači koji imaju mogućnost davanja digitalnog potpisa (i koji su, stoga, u mogućnosti da glasuju preko interneta) mogu glasovati četiri do šest dana prije dana izbora na internetskoj stranici Nacionalnog izbornog odbora (est. *Vabariigi Valimiskomisjon,* VVK). Potrebno je potvrditi svoj identitet putem digitalnog potpisa, odabrati željenog kandidata te potvrditi odabir. Kako je odlučeno da se na dan izbora ne može glasovati preko interneta, VVK je dužan lokalnim izbornim odborima poslati popis birača koji su iskoristili svoje biračko pravo preko interneta, kako bi se provjerilo je li neki glasač glasovao i na biračkom mjestu; u slučaju da jest, glas koji je dao preko interneta više ne vrijedi i VVK ga briše iz sustava[119]. Ove odredbe, uz minimalne izmjene, vrijede i danas: glasači mogu dati svoj glas preko interneta od desetog do četvrtog dana prije dana izbora, na dan izbora nije moguće glasovati preko interneta, glasuje se preko službene internetske stranice estonskih izbora te je potrebna osobna iskaznica ili Mobile-ID[120]. Estonski sustav za internetsko glasovanje glasačima omogućuje i promjenu glasa – u tom slučaju sustav prepoznaje da je glasač već glasovao, stoga je potrebna potvrda glasača da će promijeniti svoj glas[121]. Glasači

[116] Madise i Martens, „E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world“, 16.
[117] Ibid. 17.
[118] Ibid.
[119] Drechsler i Madise, 101.
[120] „Internet voting in Estonia“.
[121] „Stages of i-voting in voter application“.

mogu provjeriti i je li nakon glasovanja njihov glas došao do centralnog poslužitelja, kako bi provjerili da je ispravno pohranjen i ispravno odražava njihov odabir; ovo je moguće napraviti najkasnije 30 minuta nakon davanja glasa[122].

Kako se sve veći broj glasača odlučuje glasovati preko interneta – na prvim izborima s internetskim glasovanjem, 2005. godine, 1.9% glasača je dalo glas putem interneta, a na posljednjim, za Europski parlament 2019. godine, 46.7% glasača [123] - provedena su istraživanja koja su istražila rizike i propuste estonskog sustava. Neovisno istraživanje koje je provela skupina stručnjaka (uključujući Harrija Hurstija koji je u jednom eksperimentu dokazao ranjivost sustava za optičko skeniranje korištenog u SAD-u izmijenivši rezultate glasovanja manipulacijom memorijske kartice) uputilo je na odstupanja od procedura i propuste u osiguranju tijekom lokalnih izbora 2013. godine, zbog kojih je sustav bio podložan napadima, prijevarama i greškama [124]; također je stvorena kopija sustava, nad kojom su izvršene različite vrste napada, primjerice napad na klijentsko (glasačevo) računalo i mijenjanje danog glasa. Napadi na estonske internetske usluge izvedeni su i u stvarnosti: 2007. godine cijela je digitalna infrastruktura Estonije bila metom niza kibernetičkih napada iza kojih je, po svemu sudeći, stajala Rusija[125]; u napadima nisu ukradeni osobni podaci, već je povod bio politički, a svrha je bila paralizirati državu i pokazati ranjivost koja nastane snažnim oslanjanjem na tehnologiju. Zaključak spomenutog neovisnog istraživanja jest da se estonski sustav internetskog glasovanja ipak konstantno razvija i poboljšava, no od odlučnog napadača s bogatim resursima ne mogu ga osigurati nikakve mjere zaštite[126].

5.3. Belgija

Elektroničko glasovanje u Belgiji odobreno je zakonom 1994. godine, nakon što je tri godine ranije provedeno eksperimentalno elektroničko glasovanje u dvjema općinama tijekom općih izbora. U početku je 20% općina imalo mogućnost elektroničkog glasovanja, što se do 1999. godine povećalo na 44%, a postojali su planovi da elektroničko glasovanje bude omogućeno u cijeloj državi do izbora 2006. godine[127], što ipak nije ostvareno. U Belgiji je glasovanje obvezno, što znači da svaki izbori iziskuju vrijeme, strpljenje i različite vrste troškova. Jedan

[122] „Checking of an i-vote“.
[123] „Statistics about Internet voting in Estonia“.
[124] Springall et al. 1.
[125] McGuinness, „How a cyber attack transformed Estonia“.
[126] Springall et al. 10.
[127] de Vuyst i Fairchild, „Experimenting with electronic voting registration: the case of Belgium“, 87.

od glavnih razloga za uvođenje elektroničkog glasovanja bio je brže prebrojavanje glasova; drugi argumenti uključivali su smanjenje troškova, eliminaciju nevažećih glasova te dulje vrijeme tijekom kojeg je moguće glasovati na dan izbora[128].

Belgijski sustav za elektroničko glasovanje koji se u početku koristio temeljio se na kartici s magnetnom trakom. Glasač na računalu, čiji je sustav pokrenut s diskete, bira željenog kandidata ili stranku pomoću informatičke olovke te se nakon potvrde odabira njegov odabir zapisuje na magnetnu traku kartice. Glasač zatim ubacuje karticu u kutiju priključenu na (drugo) računalo, koja čita podatak na magnetnoj traci i računa glas. U slučaju revizije ili problema s kutijom ili računalom, moguće je prebrojati glasove tako da se kartice izbroje na drugom uređaju[129]. Belgijski se sustav smatra manje ranjivim u odnosu na DRE uređaje koji se koriste u SAD-u i drugim državama, no ima nekoliko slabih točaka: prije svega, kutija u koju se ubacuju kartice može zapisati glas preko postojećeg i tako izmijeniti glasačev odabir; također, ne može se jamčiti da je programski kod na disketama na kojima je pohranjen sustav bilježenja glasova nepromijenjen[130]. Ipak, stvarni problemi uključivali su većinom tehničke poteškoće: najveći zabilježeni incident dogodio se na izborima 2003. godine kad je jednom kandidatu pribrojeno 4096 glasova previše, zbog promjene jednog bita na memoriji glasačkog računala[131]. Organizacija za europsku sigurnost i suradnju (engl. *Organization for Security and Co-operation in Europe*, OSCE) podnijela je izvještaj nakon belgijskih izbora 2007. godine u kojem je navedeno kako je nedostatak ili nedovoljna količina javne rasprave o uvođenju elektroničkog glasovanja jedan od razloga zašto se sustav nikad nije maknuo s brojke od 44% pokrivenog područja; također, izostanak papirnatog traga upućuje na nedostatak transparentnosti[132]. S vremenom su računala koja su se koristila na izborima postala zastarjela te se sustav više nije činio održivim, stoga je 2012. godine uveden novi sustav koji je proizvela tvrtka Smartmatic, čije se tehnologije koriste u mnogim drugim državama gdje se glasovanje odvija elektroničkim putem. Novi se sustav sastoji od elektroničkog uređaja s dodirnim zaslonom, pisača barkoda, skenera i glasačke kutije, a procedura je sljedeća: nakon identifikacije, glasač dobiva „pametnu“ karticu (engl. *smartcard*) kojom aktivira uređaj za glasovanje. Nakon davanja glasa i potvrde, uređaj na papiru ispisuje podatke od kojih je jedan dio čitljiv ljudima, a drugi je u obliku barkoda; glasač mora presaviti papir tako da se ljudima čitljiv dio ne vidi te pomoću skenera očitati barkod i zatim

[128] De Cock i Preneel, „Electronic voting in Belgium: Past and future“, 77.
[129] Ibid.
[130] Ibid. 78.
[131] Ibid.
[132] Vegas, „The new Belgian e-voting system“, 201.

ubaciti papir u glasačku kutiju. Skener će očitati podatke i pohraniti ih na zaštićene USB-memorije. Na ovaj način glasač može provjeriti je li njegov glas ispravno zabilježen te, u slučaju kvara ili revizije, papir može poslužiti kao VVPAT.[133] Kao kod svih sustava s papirnatim tragom, ovo istovremeno predstavlja rizik kojim se može ugroziti tajnost glasovanja, dok glasaču daje dodatnu odgovornost i brigu skrivanja čitljivog dijela papira. Belgijska vlada dogovorila je korištenje sustava tvrtke Smartmatic na 15 godina[134].

[133] Ibid. 205.
[134] „Smartmatic will introduce its electronic voting solution in Belgium for 15 years".

6. Rasprave o elektroničkom glasovanju u Hrvatskoj

Od nastanka Republike Hrvatske do danas nije bilo konkretnih pokušaja uvođenja elektroničkog glasovanja na državnim izborima i referendumima. Međutim, ideja o elektroničkom glasovanju povremeno se pojavljuje u medijima – posljednji val rasprave dogodio se sredinom 2018. godine, kad je stranka Most nezavisnih lista (u nastavku: Most) tražila izmjenu izbornog zakona, odnosno uvođenje elektroničkog i dopisnog glasovanja, pozivajući se na preporuku Vijeća Europske unije u kojoj je prepoznata potreba da se građanima omogući glasovanje i izvan biračkih mjesta, kako bi se u Hrvatskoj povećao odaziv birača[135]. Uzevši u obzir činjenicu kako se iz Hrvatske iseljava sve veći broj ljudi, najčešće u potrazi za poslom, elektroničko (točnije internetsko) glasovanje omogućilo bi i tim državljanima lakše glasovanje dok prebivaju izvan države. Međutim, tadašnji ministar uprave odgovorio je kako uvođenje elektroničkog glasovanja u Hrvatsku nije moguće „još barem dvije godine“[136]; kao glavni razlozi navedeno je da je zbog sigurnosti potreban internet pete generacije te da trenutni tehnološki uvjeti ne zadovoljavaju sigurnosne kriterije. Hrvatska regulatorna agencija za mrežne djelatnosti (HAKOM) demantirala je, međutim, odgovor Ministarstva rekavši kako je uvođenje elektroničkog glasovanja moguće „već danas“[137]. Najveći teleoperateri u Hrvatskoj također su potvrdili da je uvođenje elektroničkog glasovanja moguće „za mjesec dana“, uz tvrdnju da već imaju razvijen sustav koji nude potencijalnim kupcima[138].

Iz svega navedenog može se, dakle, zaključiti kako Hrvatska ima prikladnu infrastrukturu za uvođenje elektroničkog glasovanja – to potvrđuju stručnjaci iz HAKOM-a i teleoperaterskih tvrtki. Također, osobne iskaznice u Hrvatskoj u sebi sadrže čip na koji se mogu pohraniti dva certifikata – identifikacijski, za elektroničku potvrdu identiteta, i potpisni, koji zamjenjuje vlastoručni potpis i koristi se kao podrška naprednom elektroničkom potpisu[139]; gotovo identičan način identifikacije koristi i Estonija. 2017. godine predstavnici Državnog izbornog povjerenstva sudjelovali su na Drugoj međunarodnoj konferenciji na temu elektroničkog glasovanja, „E-VOTE-ID 2017“ u Austriji, gdje su u nizu izlaganja predstavljena osnovna načela elektroničkog glasovanja te načini na koje se može osigurati elektroničke sustave te

[135] „Most traži hitnu izmjenu izbornog zakona“.
[136] Brečić, „"Elektroničko glasovanje u Hrvatskoj još nije moguće"“.
[137] „Kuščević izjavio da elektroničko glasovanje nije moguće, u HAKOM-u se ne slažu“.
[138] Radaljac, „Teleoperateri demantiraju Kuščevića: Elektronički izbori mogu se realizirati u samo - mjesec dana“.
[139] „Osobna iskaznica (eOI)“.

tako omogućiti povjerenje birača u njih[140]. Navedeno je i da je „primjena elektroničkog glasovanja isključiva volja pojedine zemlje te da uvelike ovisi o političkim odnosno društvenim zbivanjima u toj zemlji“[141], što dovodi do zaključka kako hrvatska infrastruktura i tehničke mogućnosti, ako je vjerovati stručnjacima iz HAKOM-a te suprotno mišljenju Ministarstva uprave, nisu glavni razlog zašto elektroničko glasovanje (još) nije uvedeno u Hrvatsku.

Iako na državnoj razini, kao što je rečeno, nema konkretnih planova o uvođenju elektroničkog glasovanja, u posljednjih nekoliko godina u dva su navrata održani elektronički izbori manjeg opsega – jedni su unutarstranački izbori stranke Održivi razvoj Hrvatske (ORaH), a drugi izbori za predsjednika i zamjenika Hrvatske liječničke komore. Za unutarstranačke izbore u ORaH-u tvrtka Mobility razvila je aplikaciju preko koje su članovi stranke mogli glasati. Oni koji su se odlučili za elektroničko glasovanje, prema riječima arhitekta platforme, prije glasovanja dobili su e-mail s jedinstvenim ključem pomoću kojeg su se prijavili u sustav i obavili glasovanje; ti su ključevi nakon definiranja distribuirani prema kompjutorskom algoritmu neovisno o ljudskom faktoru, kako bi se osigurala tajnost i privatnost[142]. 2019. godine Hrvatska liječnička komora održala je sedmodnevne izbore na sustavu koji je izrađen po uzoru na sustav e-Građani; njezini su članovi mogli glasovati pomoću PIN-a i pametne elektroničke iskaznice koju su dobili prije izbora[143]. U oba su slučaja izbori obuhvaćali mali broj glasača (u ORaH-ovim izborima oko 1700), stoga je – iako je u tehničkom smislu sve prošlo u redu – nemoguće reći kako bi jedan od ovih, ili bilo koji sustav funkcionirao u izborima većeg razmjera; ostaje vidjeti hoće li uvođenje interneta pete generacije učiniti korak prema uvođenju elektroničkog glasovanja u Hrvatskoj.

[140] „Sudjelovanje na Drugoj međunarodnoj konferenciji na temu elektroničko glasovanje „E-VOTE-ID 2017“, Bregenz, 24. – 27. listopada 2017.“
[141] Ibid.
[142] „Mirela Holy provela stranačke izbore na domaćoj aplikaciji“.
[143] „Prvi elektronički izbori protječu po planu“.

7. Zaključak

Svrha je ovog rada bila prikazati opće značajke sustava za elektroničko glasovanje, njihove teoretske prednosti i nedostatke te konkretne primjere triju država koje, s više ili manje uspjeha, koriste elektroničko glasovanje. Može se zaključiti kako ne postoji metoda glasovanja koja u potpunosti štiti identitete glasača, njihove odabire i rezultate izbora od krađe, prijevare ili manipulacije – papirnati glasački listići, primjerice, nose sa sobom očit rizik ugrožavanja tajnosti glasovanja; bušene kartice mogu biti nespretne za korištenje i uzrokovati nejasnoće prilikom prebrojavanja; strojevi s polugom rijetko dolaze s alternativnim načinom glasovanja u slučaju kvara. Gotovo svi navedeni nedostaci moguć su scenarij i kod korištenja sustava za elektroničko glasovanje; čini se da najveći problem kod njih, ipak, predstavlja papirnati trag koji se može smatrati dvosjeklim mačem – ako postoji, potencijalno ugrožava tajnost i privatnost; ako ne postoji, potencijalno ugrožava valjanost rezultata u slučaju kvara ili napada. Sigurnost je također jedna od većih briga kod korištenja ovih sustava – razvojem tehnologije razvijaju se i novi načini napada na različite sustave, a poznato je i da, u trenutku spajanja na internet, i najmoćnije računalo gubi status stopostotne zaštićenosti.

Zašto se pojedine države ipak odlučuju na elektroničko glasovanje? Dok je teško izvući općenite zaključke, neke od glavnih prednosti elektroničkog glasovanja jesu brzina i učinkovitost – ispravan sustav može višestruko skratiti vrijeme potrebno za prebrojavanje glasova, izdvajanje nevažećih listića, ali i samu proceduru glasovanja. Jedino je pitanje koji je sustav ispravan i prikladan za neku državu, ili točnije, je li država prikladna za elektroničko glasovanje – oprečni su primjeri Estonija i Sjedinjene Američke Države. Estonija godinama temelji javne usluge na internetu, stoga je internetsko glasovanje predstavljalo prirodan korak u tom smjeru, dok SAD, unatoč razvijenim smjernicama i preporukama, ima poteškoća s pronalaženjem prikladnog elektroničkog ili internetskog sustava, čemu uzrok možda leži u činjenici da bi taj sustav trebao biti u skladu zakona 50 različitih američkih saveznih država.

Ako se Hrvatska odluči na uvođenje elektroničkog glasovanja, telekomunikacijski stručnjaci potvrdili su da ima potrebnu infrastrukturu i mogućnosti te da ga je moguće uvesti u vrlo kratkom roku. Ono što je, međutim, najvažnije jest da ta infrastruktura i mogućnosti moraju u potpunosti podržavati sustav, budući da se u protivnim može ozbiljno ugroziti integritet izbora – ponovni je primjer Estonija koju je, unatoč stabilnom digitalnom sustavu javnih usluga, na neko vrijeme paralizirao niz kibernetičkih napada. Na pojedinoj je državi, stoga, da odredi je

li dovoljno pripremljena za izazove elektroničkog glasovanja ili će se nastaviti oslanjati na konzervativnije metode.

8. Literatura

1. „A Comparative Assessment of Electronic Voting.“ Elections Canada Online. Dostupno na: https://www.elections.ca/content.aspx?section=res&dir=rec/tech/ivote/comp&document=benefit&lang=e (3.9.2019.)
2. Anane, Rachid, Richard Freeland, i Giorgios Theodoropoulos. "e-Voting Requirements and Implementation," *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services*, str. 382-392. Tokyo, 2007.
3. „Arguments in Favor.“ Electronic Voting. Dostupno na: https://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0001.html (3.9.2019.)
4. „Benefits, Risks and Costs.“ ACE Electoral Knowledge Network. Dostupno na: http://aceproject.org/ace-en/focus/e-voting/benefits-risks-and-costs (3.9.2019.)
5. Brečić, Katarina. „"Elektroničko glasovanje u Hrvatskoj još nije moguće"“. N1, 27.7.2018. Dostupno na: http://hr.n1info.com/Vijesti/a320317/Elektronicko-glasovanje-u-Hrvatskoj-jos-nije-moguce.html (3.9.2019.)
6. Buchsbaum, Thomas M. "E-voting: International developments and lessons learnt." *Electronic Voting in Europe – Technology, Law, Politics and Society* (2004): 31-34.
7. Burmester, Mike, i Emmanouil Magkos. „Towards secure and practical e-elections in the new era.“ U *Secure electronic voting*, ur. Dimitris A. Gritzalis, str. 63-76. Boston, MA : Springer, 2003.
8. „Bush v. Gore.“ Britannica.com. Dostupno na: https://www.britannica.com/event/Bush-v-Gore (3.9.2019.)
9. CARNet, CERT. „Elektroničko glasovanje.“ Dostupno na: https://www.cert.hr/wp-content/uploads/2019/05/NCERT_EleGlas.pdf (3.9.2019.)
10. CARNet, CERT, LS&S. „Digitalni potpis.“ Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-02-182.pdf (3.9.2019.)
11. CARNet, CERT, LS&S. „Sigurnost elektroničkog glasovanja.“ Dostupno na: https://www.cis.hr/www.edicija/LinkedDocuments/CCERT-PUBDOC-2007-04-188.pdf (3.9.2019.)
12. Castro, Daniel. "Stop the presses: How paper trails fail to secure e-voting." *ITIF Reports* (2007).
13. „Checking of an i-vote.“ Valimised. Dostupno na: https://www.valimised.ee/en/internet-voting/checking-i-vote (3.9.2019.)
14. Council of Europe. „Legal, operational and technical standards for e-voting.“ 2004. Dostupno na: http://www.eods.eu/library/CoE_Recommentaion%20on%20Legal,%20Operational%20and%20Technical%20Standards%20for%20E-voting_2004_EN.pdf (3.9.2019.)
15. De Cock, Danny, i Bart Preneel. "Electronic voting in Belgium: Past and future." U *E-Voting and Identity: First International Conference*, ur. Ammar Alkassar, i Melanie Volkamer, str. 76-87. Berlin Heidelberg : Springer, 2007.

16. de Vuyst, Bruno, i Alea Fairchild. "Experimenting with electronic voting registration: the case of Belgium." *The Electronic Journal of e-Government* 3, 2 (2005): 87-90.
17. DeMille, David. „Voting machine issues complicate balloting in Washington County.“ The Spectrum, 9.11.2016. Dostupno na: https://eu.thespectrum.com/story/news/2016/11/08/election-machine-problems-early-washington-county/93470912/ (3.9.2019.)
18. „Direct Recording Electronically.“ ACE Electoral Knowledge Network. Dostupno na: http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b3 (3.9.2019.)
19. Drechsler, Wolfgang, i Ülle Madise. "Electronic voting in Estonia." U *Electronic voting and democracy*, ur. Norbert Kersting i Harald Baldersheim, str. 97-108. London : Palgrave Macmillan, 2004.
20. Duggan, Briana. „Gambians cast votes with marbles instead of ballots.“ CNN, 1.12.2016. Dostupno na: https://edition.cnn.com/2016/12/01/africa/gambia-to-vote-with-marbles/index.html (3.9.2019.)
21. Election Science Institute. „DRE Analysis for May 2006 Primary, Cuyahoga County, Ohio.“ 2006. Dostupno na: http://www.votetrustusa.org/pdfs/Ohio_Folder/esi_cuyahoga_final.pdf (3.9.2019.)
22. „Electronic Transmission of Ballots.“ NCSL. Dostupno na: http://www.ncsl.org/research/elections-and-campaigns/internet-voting.aspx (3.9.2019.)
23. FairVote. „The history of the paper ballot.“ Dostupno na: http://archive.fairvote.org/righttovote/pballot.pdf (3.9.2019.)
24. Fan, Chun-I, i Wei-Zhe Sun. "An efficient multi-receipt mechanism for uncoercible anonymous electronic voting." *Mathematical and Computer Modelling* 48, 9-10 (2008): 1611-1627.
25. Furukawa, Jun, Kengo Mori, i Kazue Sako. "An implementation of a mix-net based network voting scheme and its use in a private organization." U *Towards trustworthy elections*, ur. David Chaum et al., str. 141-154. Berlin, Heidelberg : Springer, 2010.
26. Gerck, Ed, et al. "The business of electronic voting." U *Financial Cryptography - 5th International Conference*, ur. Paul Syverson, str. 243-268. Berlin, Heidelberg : Springer, 2001.
27. Germann, Micha, i Uwe Serdült. "Internet voting and turnout: Evidence from Switzerland." Electoral Studies 47 (2017): 1-12.
28. Gibson, J. Paul, et al. "A review of e-voting: the past, present and future." *Annals of Telecommunications* 71, 7-8 (2016): 279-286. Dostupno na: https://link.springer.com/article/10.1007/s12243-016-0525-8 (3.9.2019.)
29. Hale, Kathleen, i Mitchell Brown. "Adopting, adapting, and opting out: State response to federal voting system guidelines." *Publius: The Journal of Federalism* 43, 3 (2013): 428-451.
30. Herrnson, Paul S., et al. "The current state of electronic voting in the United States." U *Digital Government*, ur. Eduard Hovy et al., str. 157-180. Boston, MA : Springer, 2008.
31. Ikonomopoulos, Spyros, et al. "Functional requirements for a secure electronic voting system." U *Security in the information society*, ur. M. Adeeb Ghonaimy et al., str. 507-519. Boston, MA : Springer, 2002.

32. „Internet voting in Estonia.“ Valimised. Dostupno na: https://www.valimised.ee/en/internet-voting/internet-voting-estonia (3.9.2019.)
33. „Introduction.“ Homomorphic Encryption Standardization. Dostupno na: http://homomorphicencryption.org/introduction/ (3.9.2019.)
34. „Izbori / Referendumi.“ Državno izborno povjerenstvo Republike Hrvatske. Dostupno na: https://www.izbori.hr/site/izbori-referendumi/9 (3.9.2019.)
35. Jones, Douglas W. „A Brief Illustrated History of Voting.“ 2003. Dostupno na: http://homepage.divms.uiowa.edu/~jones/voting/pictures/ (3.9.2019.)
36. Jones, Douglas W. „Example Attack Documentation: Optical Scan Configuration File.“ *Developing an Analysis of Threats to Voting Systems: Preliminary Workshop Summary*. 2005. Dostupno na: https://www.nist.gov/sites/default/files/documents/itl/vote/threatworksummary.pdf (3.9.2019.)
37. Jones, Douglas W. „The evaluation of voting technology.“ U *Secure electronic voting*, ur. Dimitris A. Gritzalis, str. 3-16. Boston, MA : Springer, 2003.
38. Kohno, Tadayoshi, et al. "Analysis of an electronic voting system." U *IEEE Symposium on Security and Privacy*, str. 27-40. Berkeley, 2004.
39. Kumar, Sanjay, i Ekta Walia. "Analysis of electronic voting system in various countries." *International Journal on Computer Science and Engineering* 3, 5 (2011): 1825-1830.
40. „Kuščević izjavio da elektroničko glasovanje nije moguće, u HAKOM-u se ne slažu.“ Nacional. 27.7.2018. Dostupno na: https://www.nacional.hr/kuscevic-izjavio-da-elektronicko-glasovanje-nije-moguce-u-hakom-u-se-ne-slazu/ (3.9.2019.)
41. Lambrinoudakis, Costas, et al. "Electronic voting systems: Security implications of the administrative workflow." U *14th International Workshop on Database and Expert Systems Applications*. Prague, 2003.
42. Lauer, Thomas W. "The risk of e-voting." *Electronic Journal of E-government* 2 (2004): 177-186.
43. Laukkonen, Jeremy. „Which Countries Use Electronic Voting?“ Lifewire, 25.9.2018. Dostupno na: https://www.lifewire.com/which-countries-use-electronic-voting-4174877 (3.9.2019.)
44. Lee, Byoungcheon, i Kwangjo Kim. "Receipt-free electronic voting scheme with a tamper-resistant randomizer." U *Information Security and Cryptology — ICISC 2002*, str. 389-406. Berlin, Heidelberg : Springer, 2002.
45. Madise, Ülle, i Tarvi Martens. "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world." U *Electronic voting 2006: 2nd International Workshop*, str. 15-26. 2006.
46. McGaley, Margaret i Gibson, J. Paul. "A Critical Analysis of the Council of Europe Recommendations on E-Voting." *EVT* 6 (2006): 1-13.
47. McGuinness, Damien. „How a cyber attack transformed Estonia.“ BBC News, 27.4.2017. Dostupno na: https://www.bbc.com/news/39655415 (3.9.2019.)
48. „Mechanical Voting Systems.“ ACE Electoral Knowledge Network. Dostupno na: http://aceproject.org/ace-en/topics/et/eth/eth02/eth02a (3.9.2019.)

49. Miller, Greg, i Adam Entous. „Declassified report says Putin 'ordered' effort to undermine faith in U.S. election and help Trump." The Washington Post, 6.1.2017. Dostupno na: https://www.washingtonpost.com/world/national-security/intelligence-chiefs-expected-in-new-york-to-brief-trump-on-russian-hacking/2017/01/06/5f591416-d41a-11e6-9cb0-54ab630851e8_story.html?utm_term=.015b0bf1d346 (3.9.2019.)
50. „Mirela Holy provela stranačke izbore na domaćoj aplikaciji." Tportal, 31.10.2014. Dostupno na: https://www.tportal.hr/tehno/clanak/mirela-holy-provela-stranacke-izbore-na-domacoj-aplikaciji-20141030 (3.9.2019.)
51. „Most traži hitnu izmjenu izbornog zakona." HRT, 27.7.2018. Dostupno na: https://vijesti.hrt.hr/454154/most-trazi-hitnu-izmjenu-izbornog-zakona (3.9.2019.)
52. Okediran, Oladotun, et al. "A comparative study of generic cryptographic models for secure electronic voting." *British Journals of Science* 1, 2 (2011): 40-52.
53. „Općenito." Državno izborno povjerenstvo Republike Hrvatske. Dostupno na: https://www.izbori.hr/site/izbori-referendumi/referendum/opcenito-123/123 (3.9.2019.)
54. „Optical Scanning Sytems." ACE Electoral Knowledge Network. Dostupno na: http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b2 (3.9.2019.)
55. „Osobna iskaznica (eOI)." Ministarstvo unutarnjih poslova Republike Hrvatske. Dostupno na: https://mup.gov.hr/osobna-iskaznica-eoi/328 (3.9.2019.)
56. „Overview." ACE Electoral Knowledge Network. Dostupno na: http://aceproject.org/main/english/et/et10.htm (3.9.2019.)
57. Preneel, Bart. „Analysis and design of cryptographic hash functions." Doktorska disertacija, Katholieke Universiteit te Leuven, 1993.
58. „Prvi elektronički izbori protječu po planu." Hrvatska liječnička komora, 20.5.2019. Dostupno na: https://www.hlk.hr/prvi-elektronicki-izbori-protjecu-po-planu.aspx (3.9.2019.)
59. „Punchcards." ACE Electoral Knowledge Network. Dostupno na: http://aceproject.org/ace-en/topics/et/eth/eth02/eth02b/eth02b1 (3.9.2019.)
60. Pynchon, Susan. „Florida: The Harri Hursti Hack and its Importance to our Nation." VoteTrustUSA, 21.1.2006. Dostupno na: http://www.votetrustusa.org/index.php?option=com_content&task=view&id=798&Itemid=51 (3.9.2019.)
61. Qadah, Ghassan Z., i Rani Taha. "Electronic voting systems: Requirements, design, and implementation." *Computer Standards & Interfaces* 29, 3 (2007): 376-386.
62. Radaljac, Danko. „Teleoperateri demantiraju Kuščevića: Elektronički izbori mogu se realizirati u samo - mjesec dana." Novi list, 8.9.2018. Dostupno na: http://www.novilist.hr/Vijesti/Hrvatska/Teleoperateri-demantiraju-Kuscevica-Elektronicki-izbori-mogu-se-realizirati-u-samo-mjesec-dana?meta_refresh=true (3.9.2019.)
63. „Register to Vote and Check or Change Registration." USAGov. Dostupno na: https://www.usa.gov/register-to-vote (3.9.2019.)
64. Riera, Andreu. „An introduction to electronic voting schemes." *Unitat de Combinatòria i de Comunicació Digital*. Universitat Autònoma de Barcelona, Departament d'Informàtica, 1998.

65. Roseman, Gary H., i E. Frank Stephenson. "The effect of voting technology on voter turnout: Do computers scare the elderly?" *Public Choice* 123, 1-2 (2005): 39-47.

66. Sampigethaya, Krishna, i Radha Poovendran. "A framework and taxonomy for comparison of electronic voting schemes." *Computers & Security* 25, 2 (2006): 137-153.

67. Simons, Barbara, i Douglas W. Jones. "Internet voting in the US." *Communications of the ACM*, 55, 10 (2012): 68-77.

68. „Smartmatic will introduce its electronic voting solution in Belgium for 15 years.“ Smartmatic. Dostupno na: https://elections.smartmatic.com/smartmatic-will-introduce-its-electronic-voting-solution-in-belgium-for-15-years (3.9.2019.)

69. Springall, Drew, et al. "Security analysis of the Estonian internet voting system." *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* (2014).

70. „Stages of i-voting in voter application.“ Valimised. Dostupno na: https://www.valimised.ee/en/internet-voting/stages-i-voting-voter-application (3.9.2019.)

71. „Statistics about Internet voting in Estonia.“ Valimised. Dostupno na: https://www.valimised.ee/en/archive/statistics-about-internet-voting-estonia (3.9.2019.)

72. „Sudjelovanje na Drugoj međunarodnoj konferenciji na temu elektroničko glasovanje „E-VOTE-ID 2017“, Bregenz, 24. – 27. listopada 2017.“ Državno izborno povjerenstvo Republike Hrvatske. Dostupno na: https://www.izbori.hr/site/medjunarodna-suradnja/sudjelovanje-na-drugoj-medjunarodnoj-konferenciji-na-temu-elektronicko-glasovanje-e-vote-id-2017-bregenz-24-27-listopada-2017/29 (3.9.2019.)

73. „Sve što možda ne znate, a trebate znati o dopisnom i elektroničkom glasovanju.“ Narod.hr, 21.6.2014. Dostupno na: https://narod.hr/hrvatska/sve-sto-mozda-ne-znate-trebate-znati-o-dopisnom-elektronickom-glasovanju (3.9.2019.)

74. „The Important Uses of Cryptography in Electronic Voting and Counting.“ National Democratic Institute. Dostupno na: https://www.ndi.org/e-voting-guide/examples/cryptography-in-e-voting (3.9.2019.)

75. „The United States.“ Electronic Voting. Dostupno na: https://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/electronic-voting/index_files/page0004.html (3.9.2019.)

76. Trechsel, Alexander H., i Hanspeter Kriesi. „Switzerland: the referendum and initiative as a centrepiece of the political system.“ U *The Referendum Experience in Europe*, ur. Michael Gallagher i Pier Vincenzo Uleri, str. 185-208. Macmillan Press Ltd, 1996.

77. US Election Assistance Commission. „Voluntary voting system guidelines. Vol. I“ 2005. Dostupno na: https://www.eac.gov/assets/1/28/VVSG1.0Vol.2.PDF (3.9.2019.)

78. US Election Assistance Commission. „Voluntary voting system guidelines. Vol. II“ 2005. Dostupno na: https://www.eac.gov/assets/1/28/VVSG1.0Vol.2.PDF (3.9.2019.)

79. Vegas, Carlos. "The new Belgian e-voting system." *Electronic Voting* (2012): 199-211.

80. „Voting Equipment.“ NCSL. Dostupno na: http://www.ncsl.org/research/elections-and-campaigns/voting-equipment.aspx (3.9.2019.)

81. Zakon o izborima zastupnika u Hrvatski državni Sabor. // Narodne novine, 116(1999). Dostupno na: https://narodne-novine.nn.hr/clanci/sluzbeni/1999_11_116_1854.html (3.9.2019.)

Sustavi za elektroničko glasovanje

Sažetak

Ovaj rad daje prikaz elektroničkog glasovanja, koje sve veći broj država testira i implementira, s više ili manje uspjeha. Dosadašnje metode glasovanja, kao što su glasački listići, bušene kartice, optičko skeniranje i strojevi s polugom, sadrže određene nedostatke, primjerice sigurnosne rizike ili velike troškove, zbog čega se sve više pozornosti pridaje elektroničkom glasovanju kao novoj metodi glasovanja. Kako bi elektroničko glasovanje u određenoj državi bilo što učinkovitije, razna tijela poput Vijeća Europe objavila su smjernice i standarde za njegovo uvođenje, pri čemu se naglasak stavlja na pristupačnost, transparentnost te ponajviše na sigurnost sustava. Ispravno implementirani sustavi za elektroničko glasovanje mogu uvelike pridonijeti brzini i učinkovitosti izbornog procesa; međutim, na konkretnim su primjerima neispravnost uređaja i simulirani, ali i stvarni napadi pokazali da ni ova metoda ne može u potpunosti štititi tajnost glasovanja i integritet izbora. Od triju država čije je korištenje elektroničkog glasovanja opisano u ovom radu (Sjedinjene Američke Države, Estonija i Belgija) jedino ga Estonija koristi uspješno i učinkovito; razlog vjerojatno leži u činjenici da Estonija dugi niz godina koristi internet za vladine usluge te je elektroničko glasovanje bilo logičan potez. Elektroničko glasovanje u Hrvatskoj na državnoj razini trenutačno postoji jedino kao tema medijskih rasprava; telekomunikacijski stručnjaci, međutim, tvrde da potrebna infrastruktura postoji, stoga preostaje vidjeti hoće li i Hrvatska u budućnosti implementirati, ili barem testirati elektroničko glasovanje.

Ključne riječi: elektroničko glasovanje, izbori, kriptografija

Electronic voting systems

Summary

This paper gives an overview of electronic voting, which is being tested and implemented by an increasing number of countries, with varying degrees of success. Voting methods that have been used so far, such as paper ballots, punch cards, optical scanning and mechanical lever voting machines, each have their own drawbacks, such as safety risks or high financial costs, which is the reason why more attention is being paid to electronic voting as a new voting method. In order for electronic voting to be as efficient as possible, various organizations, such as the Council of Europe, have published guidelines and standards for its implementation, with the focus set on accessibility, transparency and, mainly, the security of the system. Properly implemented electronic voting systems can significantly improve the speed and efficiency of the electoral process; however, concrete examples show how device malfunction and simulated and real cyberattacks can decrease the secrecy and integrity of elections. Out of the three countries whose electronic voting system use has been described in this paper (the United States of America, Estonia, and Belgium), Estonia seems to be the only one using it successfully and efficiently. The underlying reason may be the fact that Estonia has been using the Internet to provide governmental services for a number of years; therefore, the transition to electronic voting was the logical next step. National-level electronic voting in Croatia currently only exists as a public debate topic. Telecommunication experts, however, claim that the country possesses the required infrastructure; whether Croatia will implement, or at least try out electronic voting in the future, remains to be seen.

Keywords: electronic voting, elections, cryptography