Miha JESENŠEK, Andrej A. LUKŠIČ***

IZVIRNI ZNANSTVENI ČLANEK

ZAUPANJE MED POLITIKO, STROKO IN JAVNOSTJO

Odprtokodne in nekatere druge rešitve kot temelj zanesljivih, transparentnih in družbeno sprejemljivih e-volitev[1]

Povzetek. *Besedilo predstavlja sociotehnološke vidike izvedbe zanesljivih, transparentnih in družbeno sprejetih e-volitev. Ključni elementi so: dvotočkovni sistem preverjanja istovetnosti in varen prenos podatkov, možnost ponovne oddaje glasu po sistemu Zadnji glas velja, anonimnost glasu, odprtokodna metoda razvoja ter jasen in pregleden uporabniški vmesnik in podporni sistem, ki temelji na dvosmerni komunikaciji. Le z vključitvijo politike, stroke in javnosti v načrtovanje in izvedbo e-volitev dosežemo pozitivno implementacijo le-teh v praksi.*

Ključni pojmi: *e-volitve, e-glasovanje, glasovanje na daljavo, odprta koda, zaprta koda, zaupanje, politika, stroka, javnost.*

Uvod

E-glasovanje (elektronsko glasovanje) je glasovanje s pomočjo elektronskih medijev, med katere sodijo telefoni, mobilni telefoni, internet, elektronske glasovalne postaje (kioski), sistemi direktnih elektronskih zapisov (DRE oz. *touchscreen* glasovanje)[2] ipd. Rešitev, ki se na državni ravni predvideva v Sloveniji[3] – glasovanje prek interneta in mobilnega telefona –, spada v to kategorijo, vendar hkrati tudi v ožjo kategorijo glasovanja na daljavo (*remote voting*), zato jo lahko imenujemo e-glasovanje na daljavo.[4] Uporablja se tudi

** Miha Jesenšek je član St. Antony's Collegea Univerze v Oxfordu. Na Fakulteti za orientalske študije iste univerze je kandidat za magisterij s področja novih medijev in družbenih omrežij na Kitajskem.*

*** Dr. Andrej Lukšič, izredni profesor na Fakulteti za družbene vede, Univerza v Ljubljani.*

[1] Avtorja se za pripombe ob branju rokopisa zahvaljujeta Alešu Koširju, Mitarju Milutinoviču, Juretu Petroviču, Tadeju Gregorčiču in Sebastjanu Koklu.

[2] E-glasovanje s pomočjo elektronskih glasovalnih naprav, ki so nameščene na volišču, med drugim uporabljajo v Avstraliji, Belgiji, Braziliji, Indiji, ZDA in drugod po svetu.

[3] Stroka je leta 2004 previdno svetovala postopno uvedbo tovrstnih storitev (Grad et al., 2004) oz. za e-glasovanje na daljavo ni videla prepričljivih rešitev (Turk, 2004), z ustanovitvijo Vladne delovne skupine za izvedbo e-volitev julija 2007 pa se zdi, da so e-volitve v Sloveniji vse bližje.

[4] Uporabljena literatura se večinoma nanaša na e-glasovanje na daljavo, kjer je smiselno, pa so uporabljeni tudi primeri e-rešitev na voliščih.

strokovni izraz e-volitve, ki glasovanje omejuje na institucionalizirane izvedbe glasovanja.

Glasovanje na daljavo ni nova iznajdba. Pri nas in drugod po svetu ga poznamo kot glasovanje po pošti. Tudi e-glasovanje na daljavo je že bilo izvedeno v praksi. Leta 1997 je ameriški astronavt David Wolf svoj glas s pomočjo e-pošte oddal iz vesoljske postaje Mir, tri leta kasneje so prek interneta glasovali člani Demokratične stranke v Arizoni (ZDA), istega leta je 250 članov ameriškega vojaškega osebja poskusno oddalo svoj glas z oddaljenih lokacij. V letih 2002 in 2003 je Anglija uvedla poskusna e-glasovanja na daljavo (prek interneta in telefona) na lokalni ravni, istega leta so tako glasovali tudi v Kanadi, Franciji in Švici. Nekateri Nizozemci so leta 2004 e-oddaljeno glasovali v Evropski parlament, leto kasneje pa so v Estoniji e-volili na daljavo na lokalnih volitvah ipd. Podobnih primerov na lokalnih ravneh je po svetu veliko, še bolj pa se uveljavlja elektronsko glasovanje na daljavo v primeru glasovanj v organizacijah in podjetjih. Estonci so letos (2007) kot alternativo na svojih državnozborskih volitvah prvi na svetu ponudili glasovanje po internetu.

Kljub dejstvu da tehnologija, ki omogoča oddaljeno e-glasovanje, obstaja že nekaj časa in je bila večkrat uresničena tudi v praksi, je povprečni volivec do nje zadržan. Skrbijo ga varnost, zanesljivost, anonimnost, zaupnost, neoporečnost, transparentnost in razumljivost sistema oddaljenega e-glasovanja. Povprečni volivec v klasičnem papirnem glasovanju najde zadovoljivo stopnjo omenjenih lastnosti, zato sistemu in rezultatom volitev zaupa. E-glasovanje na daljavo takega zaupanja volivcev (še) nima, zato ga je potrebno čim prej vzpostaviti – le tako bo lahko tehnološko dobra rešitev zaživela tudi v praksi. Sistem e-volitev na daljavo mora vsebovati (1) dvotočkovni sistem preverjanja istovetnosti in varen prenos podatkov, (2) možnost ponovne oddaje glasu po sistemu *Zadnji glas velja* in anonimnost, (3) odprtokodno metodo razvoja in (4) jasen in pregleden uporabniški vmesnik ter podporni sistem, ki temelji na dvosmerni komunikaciji.

Rešitve, ki omogočajo izvedbo e-volitev, je potrebno natančno in razumljivo predstaviti ter jih razložiti, pri tem pa je treba poudariti pomen odprte kode (in predstaviti šibke točke zaprte kode), uporabniškega vmesnika ter dvosmerne komunikacije med akterji, ki mora biti vzpostavljena od začetka do konca projekta. Hkrati je v projektu potrebno povezati vse, ki vstopajo v proces volitev: politiko, stroko in javnost. »Brez najširše privolitve za uvajanje elektronskih volitev, še posebno pa elektronskega glasovanja, bo politika o elektronskih volitvah v vseh dimenzijah v Sloveniji neizvedljiva« (Lukšič, 2007: 86). E-volitve na daljavo so zanimivo sociotehnološko[5] vprašanje, ki za svojo uspešno implementacijo povezuje znanja s področja novih tehnologij in družboslovnih ved.

[5] *O sociotehnološki naravi e-volitev govorita tudi Randell in Ryan (2006) ter Mercuri in Camp (2004).*

Klasične volitve : e-volitve – vprašanje zaupanja

Skupni imenovalec razumevanja demokratičnih volitev je preplet svobodno izražene volivčeve volje, poštenosti, tajnosti in anonimnosti glasovanja.[6] Od sistema izvedbe volitev pričakujemo, da (1) omogoča vsakemu volivcu oddati le en glas, (2) volivec odda glas po svoji volji in anonimno, (3) je volilna skrinjica pred glasovanjem prazna, (4) se po koncu volitev h končnemu rezultatu ne prištevajo/odvzemajo glasovi in (5) so oddani glasovi pravilno prešteti. Zakon o volitvah v Državni zbor v 10. in 64. členu natančno določa osnovne zahteve: »Volivcu morata biti zagotovljeni svoboda in tajnost glasovanja. Nihče ne sme biti klican na odgovornost zaradi glasovanja, niti se ne sme od njega zahtevati, naj pove, ali je glasoval, kako je glasoval oziroma zakaj ni glasoval. /.../ Prostor, kjer se glasuje, mora biti urejen tako, da je zagotovljeno tajno izpolnjevanje glasovnice. Volišče mora biti opremljeno na način, ki preprečuje opazovanje volivca pri izpolnjevanju glasovnice« (ZVDZ-UPB1, 2006).

Tajno glasovanje temelji na vnaprej pripravljenih glasovalnih lističih, ki vsebujejo ime kandidatov oz. izpisano vprašanje in možne odgovore ter prostor, kjer volivec izrazi (s pisalom označi) svojo voljo. Sistem je star in preizkušen (izhaja iz Avstralije, kjer so ga začeli uporabljati okoli leta 1850) ter omogoča ločevanje volivčeve identitete od izražene volilne želje. Celoten postopek izvedbe volitev z volilno komisijo in opazovalci na čelu, predvsem pa s svojo jasnostjo, razumljivostjo in transparentnostjo[7] (volilni imenik, fizično preverjanje identitete volivca, volilni odbor in opazovalci, zapečatene volilne skrinjice, fizično štetje izpolnjenih glasovnic in možnost ponovnega štetja, če se pojavi sum, da je prišlo do napake) volivcu ponuja dovolj visoko stopnjo zaupanja v sistem. Utopično bi bilo seveda trditi, da je kateri koli sistem, vključno s klasičnimi papirnimi volitvami, popoln.[8] Mnogi ugotavljajo, da je naše razumevanje sistema kot »dovolj« popolnega v veliki meri odvisno od predstave, ki jo imamo o tem, kaj se v resnici dogaja. »Ni pomembno zgolj, da je sistem zanesljiv, pomembno je tudi, da ljudje *verjamejo*, da je zanesljiv« (Pieters in Becker, 2006: 3, poudarek v originalu, gl. tudi Oostveen in van den Besselaar, 2004; Pieters, 2006: 284). Končna rešitev mora biti vredna zaupanja, uporabniki pa ji morajo tudi dejansko zaupati (gl. Randell in Ryan, 2006: 50; Xenakis in Macintosh, 2003). Klasične volitve zadovoljivo zadostujejo obema pogojema: so tehnično izpopolnjene in volivci hkrati tudi verjamejo/zaupajo, da je res tako. »Pravilno izvedeno papirno glasovanje po av-

[6] *Tudi Ustava RS določa, da se poslanci »volijo s splošnim, enakim, neposrednim in tajnim glasovanjem« (Ustava RS, 80. člen).*

[7] *Nekateri avtorji, recimo Hall (2006) transparenten volilni sistem definirajo kot sistem, ki podpira preverljivost, ter nadzor, razumljivost in dostopnost s strani javnosti.*

[8] *Spomnimo se le županskih volitev 2006 v Izoli.*

stralskem sistemu postavlja zelo visoke standarde, ki jih mora doseči katera koli konkurenčna volilna tehnologija,« povzema Jonesa Lauer (Lauer, 2004: 179).

Težava e-volitev je jasna in se kaže v dveh točkah. Prvič, nekoč jasen in transparenten sistem oddaje, zbiranja in preštevanja glasov postane povprečnemu volivcu nerazumljiv. Volivec nima dokaza, da je bil njegov oddani glas resnično zabeležen po njegovi volji, hkrati pa tudi niti on niti volilna komisija ne moreta preveriti, kaj se z glasom dogaja v obdobju med oddajo in končno razglasitvijo rezultatov; volivec zato težje zaupa v sistem e-volitev (prim. McGaley in McCarthy, 2004: 154–155; Hall, 2006: 3; Oostveen in van den Besselaar, 2004: 62–63). Posrednik (in ne nazadnje tudi razsodnik) e-volitev postane programska oprema volilnega sistema. V ta sklop sodita tudi strah pred možnimi vdori v sistem in zloraba oddanih glasov. Drugič, volivčevo doživljanje volitev ni več enako, »ritual« odhoda na volitve se spremni v »ritual« odhoda pred računalnik. »Pri oddaji glasu prek interneta ne gre zgolj za »hitrejši in učinkovitejši način voljenja«. Bistveno se spremni izkušnja voljenja in posledično tudi jedro demokracije« (Pieters in Becker, 2006: 3; gl. tudi Oostveen in van den Besselaar, 2004; Mahrer in Krimmer, 2005: 28).

Vprašanje ukinitve ritualne oddaje glasu na volilni enoti najbrž ni odločilno. E-volitve se ponujajo zgolj kot dodatna možnost izbire oz. ponudbe in posameznik se lahko prostovoljno odloči, na kateri način bo glasoval. Tudi iz e-bančništva vemo, da je bil ritual odhoda na banko stvar navade, ki se je sčasoma spremenila. Težavo predstavlja vmesni člen – elektronski volilni sistem, ki je pri e-volitvah posrednik med izraženo željo volivca in končnim rezultatom volitev. Za uspešno izvedbo e-volitev je zato nujno, da novi člen v sistemu zadostuje že vzpostavljenim standardom jasnosti, razumljivosti in transparentnosti klasičnega sistema izvedbe volitev.[9] Le tako bo zaupanje med volivcem in sistemom dovolj veliko in e-volitve bodo tako lahko v praksi uspešno izvedene.

Ključni gradniki sistema e-volitev na daljavo

Dvotočkovni sistem preverjanja istovetnosti in varni prenos podatkov

Eden izmed glavnih problemov oddaljenega e-glasovanja sta vprašanji istovetnosti in anonimnosti oddanega glasu. Zagotoviti je potrebno, da je tisti, ki glas odda, resnično oseba, za katero se predstavlja, in da oddani glas pride do zbirnega strežnika nespremenjen. To se lahko doseže z uporabo veljavnega elektronskega certifikata (digitalnega potrdila), ki služi kot podpis,[10]

[9] *To pa pomeni tudi, da je v skladu tudi s pravnimi normami (gl. Pičman Štefančič, 2006).*

[10] *Elektronski podpis, ki temelji na javni asimetrični kriptografiji, je v praksi edina tehnična rešitev za varne elektronske podpise. Zagotavlja avtentičnost podpisa, tj. v primeru e-volitev zagotavlja, da je lastnik*

dodatnega gesla (PIN), ki ga volivec dobi po pošti skupaj z vabilom na volitve, in uporabo kriptiranega prenosa podatkov[11] med volivčevim računalnikom in zbirnim strežnikom. S certifikatom zagotovimo istovetnost volivca. Dodatno geslo oz. PIN otežuje zlorabo kompromitirane e-identitete volivca iz oddaljenih lokacij in posledično oddajo lažnega glasu, kriptirani prenos podatkov, ki je tudi že uveljavljen v e-bančnih transakcijah in drugih primerih prenosa občutljivih podatkov, pa zagotovi varen prenos oddanega glasu.

Možnost ponovne oddaje glasu po sistemu Zadnji glas velja in anonimnost

Pri oddaljenem glasovanju je vprašljiva tudi anonimnost oddanega glasu. Glasovanje nujno ne poteka v zasebnem okolju, ki ga sicer omogočajo klasična volilna mesta. Volivec lahko glasuje iz službenega ali javnega računalnika, kjer delodajalec oz. sistemski administrator lahko posredno vpliva na volivca ali neposredno (npr. z namestitvijo posebne programske opreme) prestreže in prilagodi oddani glas. V domačih okoljih lahko sorodniki oz. navzoči vplivajo na glasovanje volivca. V najslabših primerih lahko pride tudi do trgovine z glasovi. Problem so uspešno rešili že Estonci, in sicer z možnostjo, da je glas mogoče znova oddati. Volivec lahko kadar koli v času, predvidenem za glasovanje, ponovno odda glas. Tako se sam odloči o primerno anonimnem trenutku in mestu za oddajo glasu in se izogne vplivu tretje osebe. V skrajnem primeru lahko tudi fizično pride na volitve (oddaljeno e-glasovanje je predčasno glasovanje in se konča pred začetkom klasične izvedbe volitev). Zadnji oddani glas šteje.

Anonimnost glasu na zbirnem strežniku je zagotovljena z uporabo t. i. sistema dveh ovojnic. Glas se do zbirnega strežnika pošlje v prvi elektronski »ovojnici«, iz katere je razvidna zgolj identiteta volivca. Le-ta se nato odpre in uniči. Vsebina (glas) je shranjena v novi ovojnici, ki ne vsebuje imena volivca – slednja se elektronsko odpre in glas se zabeleži.

Zdi se, da je pri e-volitvah za zdaj še nerešeno vprašanje, kako zaščititi identiteto volivca v času, ko so nerazdružene ovojnice shranjene na strežniku. To velja od časa oddaje e-glasovnice pa vsaj do konca e-glasovanja oz. do trenutka, ko se e-glasovnice razdružijo. Zaradi možnosti ponovne oddaje glasu se to namreč ne more zgoditi v trenutku, ko e-glas prispe na zbirni strežnik.

---

certifikata resnično podpisan pod vsebino in da je vsebina do naslovnika prišla nespremenjena. Problematično je, če lastniku certifikat ukradejo. Situacijo lahko enačimo z ukradenim osebnim dokumentom, s katerim bi lahko lastniku vizualno podobna oseba oddala glas tudi na klasičnem volišču.

[11] Transport Layer Security (in njegov predhodnik SSL) je kriptografski protokol, ki omogoča varno prenašanje podatkov med dvema točkama v internetu.

Premisliti je potrebno tudi, kaj storiti ob morebitni tehnični težavi[12] v času e-volitev. Ker so e-volitve predvidene kot predčasne volitve, se lahko ob skrajnem primeru razveljavijo in volivci volijo na klasičen način.

Metode razvoja sistema e-volitev

Metodo razvoja sistema e-volitev lahko določimo na več načinov. Pri tem se lahko npr. odločamo med zaprtokodno in odprtokodno metodo. Zaprtokodno metodo mnogi enačijo s terminom lastniška programska oprema,[13] odprtokodno pa natančno določa Open Source Initiative (OSI). Namen tega članka ni odpirati debate o lastniški in prosti programski opremi oz. se poglabljati v različne možnosti licenciranja odprte kode. Ključna za izvedbo e-volitev je javno dostopna koda, možnost njene uporabe in možnost aktivnega sodelovanja javnosti pri pregledovanju, testiranju, popravljanju in nadgrajevanju kode. Takšno opcijo načeloma delno omogoča tudi zaprtokodna/lastniška rešitev z objavo kode in hkratno prepovedjo spremembe in uporabe le-te. A omenjene zahteve sistema e-volitev (možnost dostopa, nadgraditve in ponovne uporabe kode) se najlepše dosežejo s pomočjo odprtokodne rešitve po dokumentu OSI. Odprta koda je smiselna, standardizirana, razširjena in preverjena rešitev, ki jo uporabljajo tudi številna podjetja.

— Zaprtokodna metoda razvoja

Zaprtokodni sistem e-volitev kot medij volivcu omogoča prenos njegove volilne želje (oddanega glasu) od mesta glasovanja (osebni računalnik s povezavo v internet) do elektronske volilne skrinjice (zbirni strežnik). Glas se odda s pomočjo veljavnega elektronskega certifikata, PIN-kode, kriptirnega protokola in varne internetne povezave ter na osnovi zaprtokodne programske rešitve. Programsko rešitev pripravi izbrani izvajalec (gospodarska družba), ki v izvedbo (načrtovanje, kodiranje, testiranje) vključi določeno število strokovnjakov.

Postavitev računalniškega sistema med volivca in volilno glasovnico volivcu onemogoča preveriti, ali je bil njegov glas zabeležen pravilno. Potek dogodkov med trenutkom, ko je bil glas oddan in trenutkom, ko je bil preštet, je volivcu neznan. Programska oprema je zato posrednik in razsodnik, ki mu je potrebno zaupati. Volivčevo zaupanje v volitve pa v primeru uporabe zaprtokodne rešitve temelji na zaupanju v gospodarski subjekt, ki je kodo razvil, in revizijsko družbo, ki jo je pregledala. Prepustiti vedenje o postopku volitev zgolj gospodarski družbi je problematično, saj omogoča notranjo

[12] *Izpad glavnega in nadomestnih strežnikov zaradi okvare ali resni napadi tipa DoS in podobno.*

[13] *Lastniška (proprietary) programska oprema je tista, pri kateri njen lastnik omeji kopiranje, uporabo in spreminjanje, to pa tehnično ponavadi doseže tako, da uporabniku onemogoči vpogled v izvorno kodo. Pravno gledano jo lahko zaščiti tudi s patenti, pogodbami, avtorskimi pravicami in licencami.*

zlorabo sistema, povečuje možnost za zunanjo zlorabo, ogroža transparentnost in anonimnost sistema ter onemogoča vzpostavitev zaupanja med volivcem in sistemom: ne poznamo oz. ne moremo predvideti političnih in gospodarskih orientacij in interesov podjetja, ki bo kodo pisalo (prim. Phillips in von Spakovsky, 2001: 83)

Večino zlorab, ki se dogajajo v elektronskih volilnih sistemih, so zakrivili insajderji (gl. Lauer, 2004: 181–183), kar je še posebej problematično pri sistemih, ki jih pripravijo gospodarske družbe. Zlonamerni uslužbenec družbe, ki pripravlja programsko rešitev, lahko kodi doda dele, ki bodo na dan volitev omogočale manipuliranje z glasovi.[14] Ob uporabi tehnik prikrivanja kodnih dodatkov (zakrivalne tehnike – *obfuscation techniques*)[15] je take trojanske konje izredno težko odkriti, še posebej v primeru, ko končno rešitev nadzira zgolj majhno število ljudi (revizijska družba). Podjetje (izvajalec) oz. celo zgolj njegov uslužbenec brez vednosti vodstva tako pridobi nadzor nad oddanimi glasovi. Ena oseba lahko s sorazmerno malo truda na enem mestu priredi veliko število glasov (gl. Jefferson et al., 2004: 62).

Podjetje ima lahko vpogled v oddane glasove, hkrati pa dostopa tudi do vseh drugih (osebnih) podatkov volivca,[16] razkrije njegovo anonimnost in jo poveže s politično orientacijo volivca. S takimi podatki je mogoče trgovati. »Vedeti, kdo je volil koga, je neprecenljivega pomena za politične stranke, kandidate na volitvah, politične analitike, strokovnjake na področju političnega marketinga, določene medije (kako volijo znani ljudje), politične aktiviste in kogarkoli, ki ga zanima rezultat volitev. Zato je neetično zaupati osebne podatke, pridobljene v državno vodenem postopku, komercialnim dobaviteljem in na splošno katerikoli pridobitni organizaciji« (Xenakis in Macintosh, 2003: 282).

Iluzorno je pričakovati, da bo sistem brez napak. NASA kritične aplikacije zelo strogo preverja, veliko strožje, kot se to dogaja v povprečnem komer-

[14] Kocher in Schneier (2004: 104) ugotavljata, da je v ZDA pri volitvah v Predstavniški dom en glas »vreden« 400 dolarjev.

[15] Primerov iz prakse je veliko, spomnimo se recimo npr. Borlanda, nekoč enega največjih proizvajalcev podatkovnih baz in programske opreme. Podjetje je v izvorno kodo vgradilo del, ki je omogočal nepooblaščene oddaljene vstope v bazo in spreminjanje vnesenih podatkov (gl. US-CERT, 2001). Danes obstajajo celo univerzitetna tekmovanja, v katerih se od pisca kode zahteva, da v navidez normalno delujoč program vgradi zlonamerno kodo, ki ob pregledu ne sme biti sumljiva, program pa mora delovati po specifikacijah naročnika (gl. The Underhanded C Contest, 2006).

[16] To lahko stori brez zamudnega in najbrž neizvedljivega »vdora« v kriptirane podatke. Podatke lahko enostavno zbere, še preden se zakriptirajo (e-volilni vmesnik, s pomočjo katerega volivec odda glas, kopijo glasovnice in podatke o volivcu pošlje podjetju), šele nato jih varno prenese na uradni zbirni strežnik. V primeru zgolj prilagajanja oddanih glasov pa lahko poseže v že odkriptirane podatke na uradnem zbirnem strežniku. To se načeloma lahko zgodi tudi volivcu, če njegov operacijski sistem ni posodobljen oz. vsebuje »luknje«. Pomembno je ozaveščanje volivcev o pomembnosti posodobitev, priporočljiva je uporaba odprtokodnih operacijskih sistemov. Vedeti pa moramo, da je volivec sam odgovoren za varnost svojega operacijskega sistema.

cialnem sektorju, kljub temu pa pričakujejo napake v programski kodi. V obsegu kode, potrebne za izvedbo e-volitev, se kljub obsežnemu testiranju in preverjanju pričakuje vsaj 60 neodkritih napak (gl. McGaley in McCarthy, 2004: 159). Za testiranje sistema e-volitev, ugotavljanje napak in popravljanje le-teh ima podjetje na voljo omejeno število strokovnjakov, zato veliko napak ostane neodkritih. Še več, odkrite napake podjetja prikrivajo (to si lahko privoščijo zaradi zaprte kode), da bi s tem ohranila svoj tržni delež oz. upravičila svojo vlogo primernega izvajalca projekta. Zato je nevarnost zunanjih zlorab (napadov na sistem z željo vdora v sistem ali onemogočanjem delovanja sistema) visoka.

Zaprtokodna rešitev v projektih, kot so e-volitve, postavlja naročnika v podrejen položaj, saj postane odvisen od dobavitelja (gl. Kitcat, 2004: 66). Xenakis in Macintosh analizirata e-volitvene projekte na lokalni ravni v Veliki Britaniji in ugotavljata, da so državne organizacije odvisne od znanja strokovnjakov zaposlenih v podjetjih, ki pripravljajo programske rešitve e-volitev. Poudarjata, da je za ustrezno izpeljane e-volitve vendarle odgovorna oblast (Xenakis in Macintosh, 2003: 281). Toda kako naj državni uradnik odgovarja za rezultate sistema, ki ga ne pozna in ga zaradi zaprte kode niti ne more (s)poznati? »Sodelovanje s ponudniki tehnologije na osnovi enakopravnega sodelovanja je ena stvar, biti popolnoma odvisen od njih – takšen je bil primer večine lokalnih oblasti v opazovanih projektih – pa nekaj popolnoma drugega« (Xenakis in Macintosh, 2003: 281). Odvisnost se lahko razvije v izsiljevanje (izvajalec pogojuje naročniku vsebino projekta, zavrača zahtevane nadgradnje ipd.), saj se izvajalec zaveda svoje superiornosti in ne nazadnje tudi monopolnega položaja, v katerem podjetje usmerja potek volitev. Na Irskem je po uvedbi možnosti elektronskega glasovanja leta 2001 in po dogovorih med vlado in izvajalskim podjetjem prišlo do zanimive, a za državo nezavidljive situacije. »Pravila o štetju glasov ne pripadajo več Ircem, niso več javna in se lahko spremenijo brez pravnih postopkov« (McGaley in McCarthy, 2004: 156). Vprašanje je tudi, kaj se zgodi z e-volilnim sistemom v primeru, ko podjetje odide v stečaj.

Zaprta koda je zaradi svojih tehničnih lastnosti primernejša za komercialno usmerjene projekte – programska rešitev v binarni obliki deluje samo na eni vrsti oz. na omejenem številu operacijskih sistemov.

– Odprtokodna metoda razvoja[17]

Odprtokodni sistem e-volitev je zelo podoben zaprtokodnemu: kot medij volivcu omogoča prenos njegove volilne želje (oddanega glasu) od mesta glasovanja (osebni računalnik s povezavo v internet) do elektronske

[17] *Yoneji Masuda je že leta 1980 v knjigi The Information Society as Post-industrial Society (ponatisnjeno kot Managing in the Information Society) govoril o konceptu, ki se je kasneje uresničil skozi idejo prostega oz. odprtokodnega programja. Sam ga je imenoval computopia (gl. Masuda, 1980/1990: 130).*

volilne skrinjice (zbirni strežnik). Glasovanje se izvede s pomočjo veljavnega elektronskega certifikata, PIN-kode, kriptirnega protokola in varne internetne povezave ter na osnovi odprtokodne programske rešitve. Programsko rešitev pripravi izbrani izvajalec (gospodarska družba), ki v izvedbo (načrtovanje, kodiranje, testiranje) vključi določeno število strokovnjakov. Razlika med zaprto- in odprtokodno rešitvijo je v tem, da se napisane kode ne skriva, temveč se objavijo že testne različice: omogoči se vpogled v kodo ter njeno uporabo, testiranje, spreminjanje.[18] Javnost tako aktivno sodeluje pri nastajanju sistema e-volitev, vedno pa ji je na voljo tudi končna različica kode, ki je uporabljena na volitvah. Bistveno je, da celoten sistem e-volitev, ne le njegov del, temelji na odprti kodi.

Javno dostopna koda pomeni, da poleg razvijalcev in revizorjev tudi javnost, stroka in politika nadzirajo sistem e-glasovanja. S tem pisca kode prisilimo v dodatno previdnost ter v pisanje čiste in dokumentirane kode, saj se zaveda dejstva, da bo njegovo delo javno dostopno in pregledano (Kitcat, 2004: 66). Večje število ljudi, ki kodo pregleda, zagotavlja več odkritih napak, višjo stopnjo varnosti in zanesljivosti[19] in manj možnosti za zasebne interese razvijalca.[20] »Varnostna shema, katere izvorna koda in načrt sta znana, a kljub temu omogoča zadovoljivo stopnjo varnosti, je dobra shema« (Kitcat, 2004: 65). Dejstvo je, da vsak posameznik ne bo pregledoval kode, a že samo zavedanje, da je koda dostopna in da jo lahko nekdo, ki mu zaupamo in ima ustrezno znanje, pregleda, dviguje stopnjo zaupanja posameznika v sistem (Hall, 2006: 4). Odprtokodna rešitev ne implicira ukinitve notranjega in zunanjega (revizijska hiša) nadzora izvedbe projekta e-volitev, temveč ju dopolnjuje.

Odprta koda omogoča trajno uporabo sistema in neodvisnost države od ponudnikov programskih rešitev in njegovih morebitnih izsiljevanj ter vplivanj na izvedbo volitev; odprtokodne rešitve so lahko nadgradljive in prilagodljive (zniževanje stroškov); javno testiranje pomeni tudi testiranje na različnih možnih kombinacijah volivčeve strojne in programske opreme in tako omogoča, da storitev uporablja širši krog volivcev.

[18] Obstaja razlika med sistemi, ki so bili razviti po principu odprte kode (t. i. ljubiteljsko programiranje, ki ni honorirano), in sistemi, ki so bili razviti komercialno, a je bila končna različica objavljena pod GPL ali katero drugo licenco. Tretja možnost so sistemi, ki imajo izvorno kodo sicer priloženo, a je dovoljen le vpogled, uporaba, spreminjanje in testiranje pa niso dovoljeni. Primeren pristop k e-volitvam je profesionalen razvoj kode (skupina strokovnjakov pripravi rešitev in koordinira razvoj), vendar po odprtokodnih principih OSI in v tesnem sodelovanju z javnostjo.

[19] Čeprav se večji del stroke strinja, da so odprtokodni sistemi zanesljivejši in varnejši od zaprtokodnih, saj večje število testiranj odkrije več napak, in s tem se v kodo vnese tudi več popravkov (gl. npr. Paulson et al., 2004; Hall, 2006), zgolj dejstvo, da je izvorna koda odprta, še ne zagotavlja najvišje stopnje varnosti in zanesljivosti. Hall za doseganje le-te predlaga kombinacijo različnih tehnik: metodo preverjanja kode »adversial penetration testing«, vzporedno nadzorovanje, test zanesljivosti in odziv razvijalcev in uporabnikov (Hall, 2006: 4).

[20] Tudi temelje participatornemu modelu je postavil Masuda (1980/1990).

Uporabo odprte kode podpira tudi dokument *Politika vlade pri razvijanju, uvajanju in uporabi programske opreme in rešitev temelječih na odprti kodi*, s katerim vlada spodbuja uporabo odprtokodnih rešitev in zastavlja smernice za njihovo uporabo: »Posebej v primerih, kjer je zaupanje uporabnikov pomembno za uporabo posamezne storitve (npr. obdelava in izmenjava osebnih podatkov, volitve ...), moramo odprtokodne rešitve jemati kot zaželeno obliko načina izvedbe projekta« (2003: 6).

— Varnost skozi skrivanje: argument proti odprti kodi?

Protiargument možnih izvajalcev implementacije rešitve e-volitev – gospodarskih subjektov – temelji na skrivanju izvorne kode, saj naj bi vpogled vanjo morebitnim napadalcem olajšal delo. Gre za princip varnosti skozi skrivanje (*security through obscurity*), ki ga je, čeprav se nekateri nanj zanašajo še danes, že leta 1883 ovrgel Auguste Kerckhoffs. Po Kerckhoffsu mora biti sistem varen, četudi napadalec pozna vse dele sistema, razen ključa (Kerckhoffs, 1883). Skrivanje se je izkazalo za nesmiselno v mnogih primerih – npr. programi in operacijski sistemi, ki so skrivali svojo kodo, so kljub temu postali tarča napadov virusov, črvov in trojanskih konjev, ki so izkoriščali varnostne luknje. Najbolj znani primeri so Microsoftovi. Tudi na področju e-volitev se skrivanje kode ni obneslo. Ko je bila izvorna koda Dieboldovih sistemov (nenamerno) objavljena, se je izkazalo, da gre za rešitev, ki ne ustreza varnostnim standardom (gl. Hursti, 2006).

Primeri kažejo, da zaradi zagotavljanja varnosti kode ni smiselno skrivati, saj »/.../ računalniškega programa ne moremo nikoli dovolj testirati, da bi lahko bili absolutno prepričani o njegovem delovanju« (McGaley in McCarthy, 2004: 159). Zaprtokodne rešitve testira zgolj omejena skupina strokovnjakov, medtem ko javno dostopna koda ta krog močno razširi. Napake v kodi formalno zaključenega izdelka so pričakovane, odprtokodni programi pa so se izkazali za uspešen način, ki omogoča večje odkrivaje le-teh. Ko napako v sistemu e-volitev odkrije javnost, je v njenem interesu tudi, da se jo odpravi. Če pa je potrebno izvorno kodo v primeru programskih projektov tipa e-volitve skrivati, to pomeni, da je stopnja njene zanesljivost vprašljiva oz. da se predvideva ali celo ve, da koda vsebuje napake, ki se jih želi zaradi ekonomskega interesa skriti. Programska koda razkriva način delovanja sistema, ki mora biti preverjen in jasno pokazati, da koda dejansko izvaja to, kar naročnik od nje zahteva.

Pravi problem odprte kode za gospodarsko družbo pa je seveda v tem, da odprtokodna rešitev ne omogoča patentiranja pravic in ne prinaša dovolj velikih dobičkov. Že spisano kodo lahko konkurenčno podjetje uporabi, izboljša in z njo konkurira celo proti prvotnemu piscu (Hall, 2006: 8). Toda McGaley in McCarthy v primeru e-volitev zavračata argument trga. »Kjer komercialni interesi prihajajo v konflikt z demokratičnimi – kot v primerih,

kjer bi objava tehničnih podrobnosti lahko ogrozila pravice intelektualna lastnina – morajo demokratični interesi prevladati. Ne nazadnje se posel lahko preseli na druge trge, demokracijo pa imamo zgolj eno« (McGaley in McCarthy, 2004: 162). Demokracija je preveč pomembna, da bi jo prepustili gospodarskim družbam. Koda aplikacije za izvedbo e-volitev je del državnega volilnega sistema, ki mora biti pravičen in transparenten. Sistem, sicer pod nadzorom vladne komisije, a napisan zasebno, ki ni bil javno pregledan in za njegovo varnost odgovarja nekdo, za katerega ne vemo natančno, kakšne interese ima, ni transparenten sistem.

Jasen in pregleden uporabniški vmesnik in podporni sistem, ki temelji na dvosmerni komunikaciji

Da bo proces izvedbe e-volitev potekal tekoče, mora biti uporabniški vmesnik jasen in pregleden. Pri uvajanju novih tehnologij v ustaljene volilne procese je treba poskrbeti, da so predstavitev novega sistema, ozaveščanje uporabnikov in komunikacija med volivcem in izvajalcem volitev pravočasni, kakovostni in dvosmerni. Osrednje spletno mesto z vsemi relevantnimi podatki o e-volitvah in brezplačna telefonska linija za pomoč uporabnikom sta nujna servisa. Pomembno je, da je omogočena dvosmerna komunikacija, se pravi da izvajalec volitev informacij ne sporoča zgolj volivcu, temveč da hkrati tudi odpre kanale, po katerih lahko informacije od volivca tudi sprejema (t. i. *citizen* oz. *netizen* participacija). Še posebej pa je pomembno, da se že v sam proces izgradnje oz. razvoja sistema vključijo politika, stroka in javnost – trije poli, ki so najpomembnejši gradniki sodobne demokracije.

Sodelovanje vseh akterjev

Mahrer v svojem SMP-modelu opisuje komunikacijo/interakcijo med različnimi igralci v sferi *družbe* (državljani, lobiji, mnenjski voditelji), *medijev* (mediji, agencije, raziskovalci trga) in *politike* (administracija – vlada in sodstvo, zakonodaja – parlament, svetovalci), ki se dogaja na štirih ravneh: (1) javna razprava o političnih idejah in vprašanjih, (2) formalno odločanje, (3) implementacije in izvedba odločitev in (4) javne volitve. Interakcije med igralci razume kot informiranje, odzivanje/konzultiranje in participiranje, in jih poveže v e-vladno raziskovalno portfolijo. Skoznjo ugotavlja, da pri e-demokraciji ne gre zgolj za vprašanje tehnologije, temveč projekt zajema vse aspekte organizacij, ki v ta odnos vstopajo. Žal pa ugotovi tudi, da e-vladna raziskovalna portfolija ne izkorišča vseh svojih zmožnosti, predvsem ker vlade večino IT-sredstev namenijo za administrativne procese. Pristop k e-vladanju po principu »najprej storitev, nato demokracija« predstavlja veliko oviro pri uspešni izvedbi e-vladnega programa (Mahrer in Krimmer, 2005: 29–31).

Xenakis in Macintosh kot rešitev ponujata zasuk in postavitev državljana kot osrednje točke sistema. Državljana »dosežeta« s pomočjo tehnik menedžmenta znanja. Ena od ključnih idej te teorije je želja, da se izboljšajo odnosi z zunanjim svetom (v poslovnem svetu gre za stranke in strateške partnerje, v primeru e-volitev za državljane – volivce). Pretok znanja mora biti omogočen na razmerju proti in od volivcev, proti in od administrativnega osebja ter proti in od oblasti (države) (Xenakis in Macintosh, 2003: 275–278). Nujni elementi uspeha e-volitev so izobraževanje volivcev in ozaveščanje o novem sistemu, promocija novega sistema, navodila o uporabi in spremljanje odziva volivcev – vse to pomaga vzpostavljati zaupanje in posledično zagotavlja uporabo novih rešitev. Enako velja za administrativne delavce na terenu, ki so vez med državo in volivcem – sami morajo sistem najprej razumeti in poznati, da ga lahko uspešno predstavijo volivcu. Pretok znanja med izvajalcem e-volitev in administrativnim osebjem je zato nujen. Celotna politika (poslanci, stranke) mora razumeti, kako sistem e-volitev deluje, da bi mu lahko zaupali.

Gre torej za dvosmerno povezavo politike, stroke in javnosti. Konceptu pa je potrebno dodati še nekaj – klasično ločenost izvajalca od uporabnika (države od volivca) po sistemu, v katerem izvajalec za zaprtimi vrati pripravi novo rešitev in jo nato s pomočjo PR-metode ponudi uporabnikom, je treba nadomestiti z vključenostjo akterjev v načrtovanje in izvedbo projekta. Javnost, politiko in stroko je potrebno povezati že med načrtovanjem in pripravami na sistem.[21] Namesto od zgoraj navzdol se sistem gradi od spodaj navzgor.

Odprtokodni pristop omogoča prav to – celostno sodelovanje vseh udeležencev pri pripravi in implementaciji sistema e-volitev. Le s pomočjo interakcije *in* participacije bodo e-volitve uspešno zaživele v praksi.

Sklep

Stroka, javnost in politika navajajo različne argumente za uvedbo e-volitev in proti. Članek z njimi ne polemizira in e-volitve raje predstavlja kot storitev, ki jo bomo volivci lahko kot dodatno možnost uporabljali v bližnji prihodnosti. E-volitve moramo razumeti kot neke vrste poživitev volilnega načina, korak s časom, sledenje razvoju, ki ga ponuja 21. stoletje. Tehnologija je navzoča, le pametno jo je potrebno uporabiti. Obstaja nekaj manjših negotovosti (npr. kako zaščititi identiteto volivca v času, ko so nerazdružene

[21] *»Dobro je poznan, a malokdo ta princip uporablja v praksi – vključiti različne kategorije uporabnikov v začetne faze načrtovanja in implementacije tehnologij je ključno za inovacijo« (Oostveen in Besselaar, 2004: 62). E-volitve namreč niso zgolj vprašanje tehnoloških rešitev ali zgolj skupek sociooloških, politoloških ali pravnih vprašanj. E-volitve so sociotehnološki vprašanje, ki predstavlja izziv in priložnost za povezovanje sociooloških in tehnoloških rešitev.*

ovojnice z glasovi shranjene na strežniku), za katere je treba poiskati ustrezne rešitve. Varnost ob primerno zasnovanem odprtokodnem sistemu ni več vprašanje, ki bi onemogočilo implementacijo e-volitev. V projekt je ustrezno in pravočasno potrebno vključiti tudi vse udeležence, da spoznajo prednosti in priložnosti ter slabosti in nevarnosti – zavedati se je potrebno, da noben sistem, niti klasično papirnato glasovanje, ni popoln. Takrat se bodo volivci lahko odločili, ali so slabosti zanemarljive in je prednosti toliko več, da lahko e-volitvam zaupajo in jih uporabljajo.

LITERATURA

GPL (2007): GNU General Public License. Dostopno prek http://www.gnu.org/licenses/gpl.html, 15. 11. 2007.

Grad, Franci; Lukšič, Andrej; Zagorc, Saša (2004). Ustavno-pravni in politološki vidiki uvajanja e-volitev v RS, študija izvedljivosti, Center Vlade RS za informatiko. Dostopno prek http://e-uprava.gov.si/eud/e-uprava/evolitve-priloga1.doc, 15. 11. 2007.

Hall, Joseph Lorenzo (2006): Transparency and Access to Source Code in E-Voting. USENIX/ACCURATE Electronic Voting Technology Workshop Working Paper. Dostopno prek http://ssrn.com/abstract=909582, 15. 11. 2007.

Hursti, Harri (2006): Diebold TSx Evaluation. Dostopno prek http://www.blackboxvoting.org/BBVtsxstudy.pdf, 15. 11. 2007.

Jefferson, Davif; Rubin, Aviel D.; Simons, Barbara; Wagner, David (2004): Analyzing Internet Voting Security. Communications of the ACM 47(10): 59–64.

Kerckhoffs, Auguste (1883): La cryptographie militaire. Journal des sciences militaires (9): 5–38, 161–191.

Kitcat, Jason (2004): Source Availability and E-Voting: An Advocate Recants. Communications of the ACM 47(10): 65–67.

Kocker, Paul, in Schneier, Bruce (2004): Insider Risk in Elections. Communications of the ACM 47(7): 104.

Lauer, Thomas W. (2004): The Risk of e-Voting. Electronic Journal of e-Government 2(3): 177–186.

Lukšič, Andrej (2007). O politiki e-volitev in e-referendumov v Sloveniji. Teorija in praksa 44(1/2): 85–102.

Mahrer, Herald, in Krimmer, Robert (2005): Towards the Enhancement of E-democracy: Identifying the Notion of the 'Middleman Paradox. Information Systems Journal 15(1): 27–42.

Masuda, Yoneji (1980/1990): The Information Society as Post-industrial Society/Managing in the Information Society: Releasing Synergy Japanese Style. Oxford: Basil Blackwell.

McGaley, Margaret, in McCarthy, Joe (2004): Transparency and e-voting: Democratic vs. commercial interests. V The International Workshop on Electronic Voting in Europe.

Mercuri, Rebeca T., in Camp, L. Jean (2004): The Code of Elections. Communications of the ACM 47(10): 52–58.

Oostveen, Anne-Marie, in van den Besselaar, Peter (2004): Internet Voting Technologies and Civic Participation: The Users' Perspective. Javnost / The Public Vol. 11(1), 61–78.

OSI: Open Source Initiative. Dostopno prek http://www.opensource.org, 15. 11. 2007.

Paulson, James W.; Succi, Giancarlo; Eberlein, Armin (2004): An Empirical Study of Open-Source and Closed-Source Software Products. IEEE Transactions on Software Engineering (30)4: 246–256.

Phillips, Deborah. M., in von Spakovsky, Hans. A. (2001): Gauging the Risks of Internet Elections. Communications of the ACM 44(1): 73–85.

Pičman Štefančič, Polona (2006): E-volitve – oddaljena vizija ali prihajajoča realnost. Javna uprava (42)2: 903–920.

Pieters, Wolter (2006): Acceptance of Voting Technology: between Confidence and Trust. V Ketil StŅlen (ur.), Trust Management: 4th International Conference, ITrust 2006, 283–297. Berlin: Springer.

Pieters, Wolter, in Becker M. J. (2006): Ethics of evoting An essay on requirements and values in Internet elections. Dostopno prek http://kind.cs.kun.nl/~wolterp /Ethics_of_e-voting_CEPE.pdf, 15. 11. 2007.

Politika Vlade RS pri razvijanju, uvajanju in uporabi programske opreme in rešitev temelječih na odprti kodi (2003). Dostopno prek http://www.camtp.uni-mb.si/opensource/Slovenia/Politika_OSS_Koncna.pdf, 15. 11. 2007.

Randell, Brian in Ryan, Peter Y. A. (2006): Voting Technologies and Trust. IEEE Security and Privacy, 4(5): 50–56.

The Underhanded C Contest (2006). Dostopno prek http://brainhz.com/underhanded, 15. 11. 2007.

Turk, Marjan (2004). Študija izvedljivosti e-volitev s predlogi implementacije. Dostopno prek http://e-uprava.gov.si/eud/e-uprava/evolitve-priloga2.doc, 15. 11. 2007.

US-CERT (2001): Vulnerability Note VU#247371. Dostopno prek http://www.kb.cert.org/vuls/id/247371, 15. 11. 2007.

Ustava republike Slovenije, Ur. l- RS, št. 33/1991.

Xenakis, Alexandros, in Macintosh, Ann (2003): Using Knowledge Management to Improve Transparency in E-voting. In Proceedings of KMGOV 2003, 274–284. Berlin: Springer.

ZVDZ-UPB1(2006): Zakon o volitvah v državni zbor (uradno prečiščeno besedilo), Ur.l. RS, št. 109/2006.