

Miha Jesenšek [*miha.jesensek@sant.ox.ac.uk*]
St. Antony's College
Univerza v Oxfordu

Povzetek predstavitve – izroček

Zaupanje med politiko, stroko in javnostjo: odprtokodne in nekatere druge rešitve kot temelj zanesljivih, transparentnih in družbeno sprejetih e-volitev¹

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), ipd. Rešitev, ki se predvideva v Sloveniji – glasovanje preko 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.

Glasovanje na daljavo ni nova iznajdba. Pri nas in drugod po svetu ga poznamo v obliki oddaje glasovnic preko pošte. Tudi e-glasovanje na daljavo je že bilo izvedeno v praksi. Leta 1997 je ameriški astronom David Wolf svoj glas preko e-pošte oddal iz vesoljske postaje Mir, tri leta kasneje so preko interneta glasovali člani Demokratične stranke v Arizoni (ZDA), istega leta je 250 članov ameriškega vojaškega osebja poskusno oddalo svoj glas iz oddaljenih lokacij. Leta 2002 in 2003 je Anglija uvedla poskusna e-glasovanja na daljavo (internet in telefon) na lokalni ravni, istega leta so glasovali tudi v Kanadi in Franciji. Nekateri Nizozemci so leta 2004 e-oddaljeno glasovali v Evropski parlament, ipd. Podobnih primerov na lokalnih ravneh je po svetu mnogo, še bolj pa se uveljavlja elektronsko glasovanje na daljavo v primeru glasovanj v organizacijah in podjetjih. Letos so Estonci prvi na svetu oddajo glasovnice preko interneta ponudili kot alternativo na državnoborskih volitvah.

Kljub dejstvu, da tehnologija, ki omogoča oddaljeno e-glasovanje, obstaja že nekaj časa, in da je bila večkrat implementirana tudi v praksi, jo povprečni volivec sprejema z zadržki. Skrbijo ga **varnost, zanesljivost, anonimnost, zaupnost, neoporečnost, transparentnost in razumljivost** sistema oddaljenega e-glasovanja. Povprečni volivec v klasičnem „papirnatem“ glasovanju najde zadovoljive stopnje omenjenih lastnosti in zato sistemu in rezultatom volitev **zaupa**. E-glasovanje na daljavo tovrstnega zaupanja volivcev (še) nima, zato ga je potrebno vzpostaviti – le tako bo sicer tehnološko lahko dokaj dovršena rešitev zaživela tudi v praksi. Da bi ta cilj dosegli, mora sistem e-volitev na daljavo vsebovati tudi naslednje rešitve:

- dvotočkovni sistem preverjanja istovetnosti in varni prenos podatkov,
- možnost ponovne oddaje glasu po sistemu zadnji glas velja in anonimnost,
- odprtokodna programska infrastruktura
- jasen in pregleden uporabniški vmesnik in podporni sistem, ki temelji na dvosmerni komunikaciji.

Končna rešitev mora biti tehnološko dovršena ter hkrati sprejeta in podprta s strani politike, stroke in javnosti.

Dvotočkovni sistem preverjanja istovetnosti, varni prenos podatkov

Eden glavnih problemov oddaljenega e-glasovanja je vprašanje istovetnosti in anonimnosti oddanega glasu. Zagotoviti je potrebno, da je tisti, ki glas odda, dejansko oseba za katero se predstavlja, in da oddani glas doseže zbirni strežnik nespremenjen. To se lahko doseže z uporabo veljavnega elektronskega certifikata (digitalnega potrdila), ki služi kot podpis², dodatnega gesla (PIN), ki ga volivec dobi po pošti skupaj z vabilom na volitve, in uporabo kriptiranega prenosa podatkov³ med volivčevim računalnikom in zbirnim strežnikom.

1 Razširjena verzija predstavitve z razvitimi argumenti in viri bo v obliki strokovnega članka objavljena v naslednji številki revije Teorija in praksa.

2 Elektronski podpis, ki temelji na javni asimetrični kriptografiji, je v praksi edina tehnična rešitev za varne elektronske podpise. Zagotavlja avtentičnost podpisa, t.j. v primeru e-volitev zagotavlja, da je lastnik certifikata dejansko podpisan pod vsebino in da je vsebina do naslovnika prišla nespremenjena.

3 Transport Layer Security in njegov predhodnik SSL je kriptografski protokol, ki omogoča varno prenašanje podatkov med dvema točkama v internetu.

S certifikatom zagotovimo istovetnost volivca. Dodatno geslo oz. PIN otežuje zlorabo kompromitirane e-identitete volivca iz oddaljenih lokacij in posledično oddajo lažnega glasu, kriptiran protokol, 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. administrator potencialno lahko posredno vpliva na volivca, ali pa neposredno (z namestitvijo posebne programske opreme) prestreže in prilagodi oddani glas. V domačih okoljih lahko sorodniki oz. prisotni vplivajo na glasovanje volivca. V najslabših primerih lahko pride tudi do trgovine z glasovi. Problem so uspešno rešili že Estonci, in sicer z možnostjo ponovne oddaje glasu. Volivec lahko kadarkoli v času, predvidenem za glasovanje, ponovno odda glas. Volivec se tako 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 zaključi pred pričetkom klasične izvedbe volitev). Zadnji oddani glas šteje.

Anonimnost glasu na zbirnem strežniku je zagotovljena z uporabo t.i. sistema dveh ovojnici. 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 zapakirana v novi ovojnici, ki ne vsebuje imena volivca. Le-ta se elektronsko odpre in glas se zabeleži.

Odprtokodna programska infrastruktura

Moč klasičnega „papirnatega“ glasovanja je v njegovi transparentnosti. Brez posebnega tehničnega znanja se lahko praktično vsak prepriča o načinu, poteku in rezultatih volitev. V primeru suma kršitev se lahko glasovi ponovno preštejejo. Postavitev računalniškega sistema med volivca in volilno glasovnico onemogoča volivcu 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 arbiter, ki mu je potrebno zaupati. V primeru suma kršitev se glasovi ne morejo ponovno prešteti. Tudi člani volilne komisije so (kljub dejstvu, da so tudi IT strokovnjaki) praktično le brezmočni opazovalci, saj ne poznajo izvorne kode in ne vedo, kaj se med procesom glasovanja dejansko dogaja. Volivčevo zaupanje v volitve pa v tem primeru 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 zlorabo sistema, ogroža transparentnost sistema in onemogoča vzpostavitev zaupanja med volivcem in sistemom: ne poznamo oz. ne moremo predvideti političnih orientacij in interesov podjetja, ki bo kodo pisalo. Ne gre zgolj za možnost manipuliranja z glasovi in vplivanja na rezultat volitev. Prepustiti nadzor nad podatki kot so „kdo in koga je volil“ komercialni družbi z minimalnim nadzorom je tvegano početje. Zbrani podatki so dragocen vir za politične stranke, tržne strokovnjake, analitike, aktiviste in podobne profile ljudi in organizacij, ki jih zanimajo vzorci volilnih odločitev.

Značilnost večine zlorab, ki se dogajajo v elektronskih volilnih sistemih je, da so izvedene s strani insajderjev. Zlonamerni uslužbenec družbe, ki pripravlja programsko rešitev, lahko kodi doda dele, ki bodo na dan volitev omogočale manipuliranje z glasovi. Ob uporabi tehnik prikrivanja kodnih dodatkov (zakrivalne tehnike – *obfuscation techniques*),⁴ je tovrstne trojanske konje izredno težko odkriti.

Rešitev problema je uporaba odprte kode. Javno dostopna koda pomeni, da poleg razvijalcev in revizorjev tudi javnost in politika nadzirata 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. Večje število ljudi, ki kodo pregleda, pomeni več odkritih napak, višjo stopnjo varnosti in zanesljivosti in manj možnosti za zasebne interese razvijalca. Dejstvo je, da sleherni 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. Poleg tega odprta koda omogoča trajno last in neodvisnost vlade od

4 Primerov iz prakse je mnogo, spomnimo se recimo zgolj Borlanda, nekoč enega največjih proizvajalcev podatkovnih baz in programske opreme. Podjetje je v izvorno kodo vgradilo del, ki je omogočal nepooblaščen oddaljene vstope v bazo in spreminjanje vnesenih podatkov. Danes obstajajo celo tekmovanja, v katerih se od pisca kode zahteva, da v navidez normalno delujoč program vgradi zlonamerno kodo, ki mora ob pregledu izgledati nesumljivo, program pa mora delovati po specifikacijah naročnika.

ponudnikov programskih rešitev in njegovih morebitnih izsiljevanj ter vplivanj na izvedbo volitev⁵; 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 možnost uporabe storitve širšemu krogu volivcev.

V prid uporabi odprte kode govori tudi leta 2003 prejeti dokument *Politika vlade pri razvijanju, uvajanju in uporabi programske opreme in rešitev temelječih na odprti kodi*, s katerim vlada vzpodbuja uporabo odprtokodnih rešitev. „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,“ zastavlja smernice uporabe odprte kode vladna politika.

Kljub temu in kljub pozitivnim vidikom odprtokodnih rešitev gre pri vpeljavi odprte kode v sistem e-volitev za enega izmed bolj kontroverznih predlogov. Hkrati je ta predlog tudi najbolj pomemben. Uraden protiargument potencialnih izvajalcev implementacije rešitve e-volitev – gospodarskih subjektov – temelji na skrivanju izvorne kode, saj naj bi vpogled v njo morebitnim napadalcem olajšal delo. Gre za t.i. princip *security through obscurity*, ki morda lahko velja na nekaterih drugih področjih, računalniška znanost pa ga je ovrгла. Računalniškega programa ne moremo nikoli dovolj testirati, da bi lahko bili absolutno prepričani o njegovem delovanju⁶. Zaprtokodne rešitve testira zgolj omejena skupina strokovnjakov, med tem 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 odkrivanje le-teh. Če 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.

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. Še več, že spisano kodo lahko konkurenčno podjetje uporabi, izboljša in z njo konkurira prvotnemu piscu. Toda če v primeru volitev komercialni interesi prihajajo v konflikt z demokratičnimi, morajo slednji prevladati. Posel se lahko preseli na druge trge, demokracijo pa imamo zgolj eno in 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 privatno, ki ni bil javno pregledan in za katerega varnost odgovarja nekdo, katerega interesi niso vedno jasni, 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 potrebno poskrbeti, da so predstavitve novega sistema, osveščanje uporabnikov in komunikacija med volivcem in izvajalcem volitev pravočasni, kvalitetni in dvosmerni. Osrednje spletno mesto z vsemi relevantnimi podatki o e-volitvah in brezplačna uporabniška telefonska linija sta nujna servisa. Pomembno je, da je omogočena dvosmerna komunikacija, se pravi da izvajalec volitev informacij ne komunicira zgolj volivcu, temveč da hkrati tudi odpre kanale po katerih lahko informacije po sistemu web 2.0 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 – najpomembnejši gradniki sodobne demokracije.

Končna rešitev: tehnološko dovršena ter hkrati sprejeta in podprta s strani politike, stroke in javnosti

Le s pomočjo interakcije in participacije bodo e-volitve uspešno zaživele v praksi. Bistveno za vsak uspešen e-volilni sistem ni zgolj to, da je vreden zaupanja, ampak da mu volivci, politiki, stroka in mediji tudi dejansko zaupajo. E-volitve namreč niso zgolj vprašanje tehnoloških rešitev ali zgolj skupek socioloških, politoloških ali pravnih vprašanj. E-volitve so sociotehnološki problem, ki predstavlja izziv in priložnost za oba pola, da si podata roke.

5 Irska je leta 2001 sprejela zakonodajo o elektronskem glasovanju in podpisala dogovore z gospodarsko družbo, ki je pripravila zaprtokodne programske rešitve. Posledica zakonodaje in dogovorov med podjetjem in vlado je bila, da je programska oprema postala zadnji arbiter volitev, predpisi o štetju glasov pa ne pripadajo več irskemu ljudstvu, niso javni in se lahko spremenijo brez pravnih procedur. Vlada je tako postala odvisna od izvajalca volitev – gospodarske družbe.

6 NASA kritične aplikacije podvrže mnogo rigoroznejšim preverjanjem kot v povprečnem komercialnem sektorju, a se kljub temu pričakujejo napake v programski kodi. V obsegu kode, potrebne za izvedbo e-volitev, se kljub obsežnem testiranju in preverjanju pričakuje vsaj 60 neodkritih napak.