

# Problem internetnih volitev

~ besedilo je v postopku objave v reviji *Teorija in praksa* ~

## Kazalo

Povzetek.....	1
Abstract.....	1
Uvod.....	2
Razlogi za internetno glasovanje.....	2
Razlogi proti internetnemu glasovanju.....	3
a) Elektronske storitve in internetno glasovanje – dva različna problema.....	4
b) Nižja stopnja transparentnosti in vprašanje odprte kode.....	5
c) Sistem internetnih volitev ne zagotavlja anonimnosti sam po sebi.....	6
d) Pri internetnih volitvah volivcu ni zagotovljeno varno volilno okolje.....	7
e) Kaj ne gre pri i-volitvah le za nadaljevanje ideje o glasovanju po pošti?.....	8
Primerjava i-volitev z glasovanjem s kroglicami.....	8
Ocena učinkovitosti in smiselnosti uvajanja i-volitev.....	10
Zaključek.....	11
Viri in literatura.....	12

## Povzetek

*V besedilu so analizirani nekateri pomisleki oz. razlogi, ki govorijo proti uvedbi internetnih volitev v Sloveniji. Tehnologija internetnih volitev namreč prinaša nove nevarnosti, povezane s tajnostjo in neposrednostjo glasovanja. Gre namreč za to, da sistem internetnih volitev sam po sebi ne zagotavlja tajnosti glasovanja, pač pa je tajnost glasovanja potrebno zagotoviti z dodatnim postopkom - anonimizacijo, kar pa odpira tudi vprašanje zaupanja. Poleg tega je informacijski sistem internetnih volitev kompleksen sistem, kompleksnost pa povečuje netransparentnost in zmanjšuje varnost. Prav tako pri internetnih volitvah ne gre za še eno e-storitev, saj se sistem internetnih volitev bistveno razlikuje od ostalih e-storitev v tem, da pri njem varnosti ne moremo zagotavljati z identifikacijo. V besedilu je na koncu predstavljena analiza učinkovitosti in smiselnosti uvajanja internetnih volitev - rezultati kažejo, da z uvajanjem internetnih volitev ne gre hiteti.*

## Abstract

*Paper analyses some doubts and arguments against the introduction of the internet elections in Slovenia. Introduction of the internet voting presents some new problems, especially in relation to voting by secret ballot and direct voting. One of the main problems with internet voting is that it does not guarantee voting by secret ballot by itself. A special procedure of anonymisation of votes must take place, but this opens a problem of trust in relation to the technology and procedure used. Another problem is that information and communications systems used to provide internet elections are highly complex systems. Greater complexity results in smaller degree of transparency and in lower level of security. Internet elections are not just another e-service or e-transaction, because security of the internet elections cannot be guaranteed using voter identification. Finally, paper presents analysis of efficiency and reasonableness of the introduction of the internet elections. Results show that the introduction of the internet elections should not be undertaken quickly and without proper debate and reflection.*

---

<sup>1</sup> dr. Matej Kovačič je asistent na Fakulteti za družbene vede, Univerza v Ljubljani, Jožko Škrablin je študent politologije na Fakulteti za družbene vede, Univerza v Ljubljani.

## Uvod

Redne in poštene volitve so eden izmed temeljnih pogojev sodobne demokracije, saj na njih prebivalci, ki imajo volilno pravico izbirajo politične zastopnike, ki jim bodo vladali v naslednjem mandatu. Postopki, po katerih se volitve izvedejo so jasno definirani, zakoni, ki opredeljujejo izpeljavo volitev natančni in nedvoumni, sam sistem volitev pa transparenten in zasnovan tako, da omogoča kar najmanj zlorab. Od legitimnosti volitev je namreč odvisna legitimnost oblasti, volitve pa so v sodobnih demokratičnih družbah tako rekoč osrednji politični dogodek, kateremu se namenja veliko pozornosti.

S pojavom informacijsko komunikacijske tehnologije in njenim prodiranjem v vse pore našega življenja, so se pojavile ideje, da bi bilo mogoče modernizirati tudi volilni postopek. Uporaba tehnologije naj bi izvedbo volitev pocenila, pospešila hitrost preštevanja glasov in zmanjšala možnost napak. Nekateri med elektronske volitve štejejo že uporabo elektronskih naprav za preštevanje glasovnic, vendar na splošno velja, da z izrazom elektronske volitve ali e-volitve označujemo volitve, kjer volivci lahko glasujejo s pomočjo elektronske naprave na klasičnem volišču. Praviloma gre za posebej prilagojen računalnik, ki volivcu omogoča oddajo glasu preko tipkovnice, s pomočjo miške ali s pomočjo zaslona občutljivega na dotik.

Naslednja stopnja v razvoju elektronskih volitev pa naj bi bile internetne volitve ali i-volitve, kjer volivec glasuje preko interneta. V tem primeru volivec obiše posebno volilno spletno stran, kjer se elektronsko identificira in odda svoj glas. Ideja je navidez preprosta, predvsem pa privlačna. Žal se ob pobudah za uvedbo i-volitev poraja kar nekaj tehtnih vprašanj, ki so tako tehnološke, kot tudi družbene narave, manjkajo pa tudi odgovori na vprašanja kaj skušamo izboljšati z uvedbo i-volitev, katere so težave z obstoječim načinom glasovanja, kako dobro uvedba i-volitev lajša te težave, katere nove težave povzroča uporaba i-volitev ter kakšne dileme in kakšno tehtanje predpostavlja uvedba i-volitev. Šele odgovori na ta vprašanja namreč pokažejo, ali je tim. dodana vrednost i-volitev tako velika, da je uvedba smiselna, oziroma je smiselna v kratkem času.

## Razlogi za internetno glasovanje

Za klasične volitve velja, da volivci svojo voljo izrazijo s pisalom, na papirnato glasovnico, ki jo vržejo v glasovalno skrinjico. Pri elektronskih oziroma internetnih volitvah gre po mnenju nekaterih zgolj za spremembo "medija", torej infrastrukture, ki podpira oddajo in preštevanje glasovnic. Namesto papirja in svinčnika, bi volivci uporabili računalnik in telekomunikacijsko omrežje, preko katerega bi oddali svoj glas. Kot bomo pokazali v nadaljevanju pa pri tem ne gre zgolj za spremembo medija, pač pa da sprememba medija za sabo potegne tudi spremembo samega koncepta glasovanja, kar ima za volitve lahko dolgoročnejše posledice. Poleg tega sprememba medija, oziroma uporaba informacijsko komunikacijske tehnologije odpira nova vprašanja glede varnosti in tajnosti glasovanja, tudi vprašanja, ki v primeru uporabe "klasičnega" medija (papirja in svinčnika) niso relevantna. Pri vprašanju e-volitev in i-volitev gre torej tako za načelno vprašanje menjave medija, kot za specifična vprašanja povezana z varnostjo in tajnostjo glasovanja na novem elektronskem mediju.

Poleg hitrejšega in bolj natančnega štetja glasovnic, na dolgi rok (če bi internetne volitve nadomestile klasično glasovanje) pa tudi nižje cene, zagovorniki elektronskega glasovanja v prid letemu navajajo različne razloge, ki jih lahko v grobem razdelimo v dva sklopa.

V prvi sklop bi lahko uvrstili argumente, da je elektronsko glasovanje bolj učinkovito in da je (predvsem med mladimi) dojeto kot modernizacija glasovalnega procesa, torej gre za lovljenje koraka s časom, uvedba elektronskega glasovanja (posebej internetnega) predstavlja zgolj logično nadaljevanje informatizacije vseh ostalih storitev (bančništva, elektronskega poslovanja, itd.). Skratka, gre za novo e-storitev, z uvedbo katere se vlade in politika skušajo predstaviti kot moderni, oziroma se države skozi projekte uvedbe elektronskih volitev celo želijo uveljaviti kot e-nacije. Povedano drugače, e-glasovanje je del procesa modernizacije, ki se ga lotevajo najbolj napredni. Elektronsko glasovanje je preprosto “in”.

V drugi sklop pa bi lahko uvrstili argumente, ki pravijo, da je elektronsko glasovanje pripomoček, ki lahko zaustavi trende upada zanimanja za volitve in za demokratični proces, saj omogoča dvig volilne udeležbe ter odpira možnosti za več neposredne demokracije (npr. pogostejše referendumne). Elektronske volitve, predvsem pa internetne bi tako po mnenju zagovornikov pomagale povečati volilno udeležbo, v prvi fazi predvsem med mladimi, kasneje pa še med ostalimi segmenti volivcev, saj olajšajo dostop do volišča. Internetno glasovanje, ki omogoča glasovanje “iz domačega naslonjača” oziroma omogoča lažji dostop do volišča bi torej po mnenju zagovornikov okrepilo in izboljšalo demokratični proces.

## Razlogi proti internetnemu glasovanju

Tiha predpostavka argumentov o i-volitvah kot načinu krepitev demokratičnega procesa je, da je pomemben, če ne celo bistven razlog za upad volilne udeležbe komoditeta oz. dejstvo, da se volivcem ne ljubi hoditi na volišče. Pri tem se žal pogosto pozablja ali zanemarja dejstvo, da so vzroki za upadanje volilne udeležbe večplastni in jih sama uvedba internetnega glasovanja zagotovo ne rešuje v celoti oziroma jih morda sploh ne rešuje.

Res je sicer, da v določenem segmentu volivcev lažji oz. internetni dostop do volišča dejansko lahko prinese povečano volilno udeležbo. Vprašanje pa je, v kolikšni meri. Žal empiričnih podatkov na to temo ni veliko. *Poročilo ženevskega kantona o elektronskih volitvah* iz julija 2007 na strani 2 navaja podatek, da je bil v Švici odstotek i-volivcev med leti od 2002 do 2006 na osmih volitvah redno okrog 20%, med temi dvajsetimi odstotki pa je bilo med 5 do 10% takšnih volivcev, ki prej niso volili (State Chancellery, 2007: 2). To v celotni populaciji sicer pomeni 1 do 2% povečano volilno udeležbo, kar je pravzaprav razmeroma malo. Podatki o volilni udeležbi za Estonijo sicer kažejo, da je elektronsko preko interneta svoj glas na volitvah 2007 oddalo 3,4% vseh, ki so volili, vendar podatka o tem koliko je bilo “novih” volivcev ni na voljo. Podatki o volilni udeležbi kažejo, da je se je volilna udeležba na estonskih parlamentarnih volitvah 2007 sicer povečala za 3,7 odstotne točke, vendar je volilna udeležba že pred uvedbo i-volitev nihala in to celo za več odstotnih točk:

leto	udeležba na volitvah
1992	67%
1995	68,9%
1999	57,4%
2003	58,2%
2007	61%

Vir: spletna stran estonske volilne komisije (Estonian National Electoral Committee, <http://www.vvk.ee>).

Ti podatki nam dajo misliti, da uvedba elektronskega glasovanja sicer verjetno res lahko vpliva na povečanje volilne udeležbe, vendar je povečanje le-te zgolj minimalno. Uvedba i-volitev torej problem upada volilne udeležbe in upada zanimanja za demokracijo rešuje le v zelo omejenem obsegu.

Tako zagovorniki, kot nasprotniki internetnega glasovanja pa se strinjajo, da takšno glasovanje odpira številne nove dileme in nevarnosti. Zagovorniki zato predlagajo številne tehnične, pravne in organizacijske ukrepe, ki naj bi zmanjšali ali celo onemogočili zlorabe, nasprotniki pa pri tem opozarjajo na problem tako imenovanega "človeškega faktorja". Prav tako nasprotniki opozarjajo, da je sistem klasičnih volitev "razpršen", kar pomeni, da do namernega ponarejanja volilnih rezultatov v večjem obsegu pride težje, saj bi bilo potrebno ponarejati rezultate na velikem številu volišč, kar bi vključevalo veliko ljudi. Podobno velja tudi za različne napake pri izvedbi volilnega procesa, katerih učinki so pri "razpršenem" sistemu lahko precej manjši kot pri centraliziranem. Sistem internetnih volitev pa bi bil "centraliziran", kar pomeni, da centralni del sistema (volilni strežniki) predstavlja eno samo možno "točko zloma", na kateri lahko pade celoten sistem internetnih volitev (tim. "single point of failure").

V nadaljevanju si bomo ogledali in podrobneje analizirali nekaj argumentov, ki se pojavljajo v razpravi okrog uvedbe internetnih volitev v Sloveniji.

### **a) Elektronske storitve in internetno glasovanje – dva različna problema**

Prvi argument, ki se pojavlja je, da gre pri uvedbi i-glasovanja zgolj za zamenjavo medija. Če smo prej glasovali s papirjem in svinčnikom, bomo sedaj glasovali s pomočjo računalnika in interneta. Šlo naj bi torej za uvedbo nove e-storitve. Zagovorniki argument pogosto podkrepijo z dejstvom, da so ostale e-storitve, kot npr. e-bančništvo, e-poslovanje, vodenje sistema izpitov na fakultetah, ipd. že splošno uveljavljene in sprejete storitve in torej ni razloga, da ne bi enake oz. nekoliko prilagojene tehnologije uporabili tudi pri i-volitvah.

A pri tem se pozablja, da gre pri elektronskem poslovanju in volitvah preko interneta za dva povsem različna problema, predvsem iz stališča zagotavljanja varnosti. Pri uporabi informacijsko komunikacijske tehnologije za namene i-volitev gre namreč za netipično uporabo te tehnologije. Ena izmed bistvenih zahtev demokratičnega glasovanja je tajnost glasovnice. V povezavi s tehnologijo internetnega glasovanja pri tem nastopi predvsem problem anonimnosti, varnega prenosa podatkov in obnove informacij.

Znani ameriški strokovnjak za kriptografijo in informacijsko varnost Bruce Schneier je v eseju "*Internet Voting vs. Large-Value e-Commerce*" izpostavil dejstvo, da elektronski finančni sistemi praviloma temeljijo na zagotavljanju identitete kot bistvenem elementu zagotavljanja varnosti (transakcij), česar pa zaradi zahteve po tajnosti glasovanja ni mogoče implementirati pri sistemu internetnih volitev: "*Finančnim transakcijam so priložena imena: kdo dobi denar, kdo ga izgubi. Glasovnice nosijo le informacijo o prejemniku: celoten smisel tajne glasovnice je v tem, da se odstrani ime volivca. Zaradi tega je sistem veliko težje zaščititi pred zlorabo, veliko težje je ugotoviti zlorabo, če do nje pride in veliko težje je identificirati napadalca in ga zapreti*" (Schneier, 2001).

Povedano drugače: gre za drugačen tip varnostnega problema. Varnost elektronskih finančnih transakcij je zagotovljena z zmožnostjo revizije izvedenih transakcij, ki je mogoča zaradi prometnih oz. identifikacijskih podatkov. Ti podatki omogočajo odkrivanje napačnih ali zlonamernih transakcij

in njihovo popravljanje, če pa to ni mogoče pa vsaj uveljavitev finančnega zavarovanja transakcije (npr. v primeru vdora v banko vračilo denarja). Tak način zagotavljanja varnosti v primeru volitev ne more biti mogoč. Poleg tega je pomembna lastnost sodobnih informacijsko komunikacijskih tehnologij, predvsem interneta, da zagotavljajo možnost beleženja in hrambe prometnih podatkov, oz. podatkov o "transakcijah". Tehnologija je že v osnovi zasnovana za tovrsten nadzor, oz. že v sami osnovi otežuje ali celo popolnoma onemogoča anonimnost.<sup>2</sup> Dodatne težave pri zagotavljanju anonimnosti pa povzročata tudi zakonodaja o obvezni hrambi prometnih podatkov, ki je od leta 2006 v veljavi v EU,<sup>3</sup> Slovenija pa jo je v svojo zakonodajo implementirala decembra 2006, ko je bila sprejeta novela *Zakona o elektronskih komunikacijah*,<sup>4</sup> ki v členih 107 do 107. e določa obvezno hrambo prometnih podatkov na področju elektronskih komunikacij.

Dodatno težavo pri zagotavljanju varnosti pa povzročata tudi različna pogostost uporabe tehnologije za izvajanje finančnih transakcij ter elektronskih volitev. Bruce Schneier je v eseju "*Getting Out the Vote: Why is it so hard to run an honest election?*" to dejstvo izpostavil takole: "*Volilni sistemi so v uporabi redko, največ nekajkrat na leto. Sistemi, ki so v uporabi vsak dan se izboljšujejo, ker ljudje nanje postanejo navajeni, odkrijejo napake in se spomnijo izboljšav.*" (Schneier, 2004). Iz zapsanega torej sledi, da je problem zagotavljanja varnosti i-volitev bistveno drugačen od problema zagotavljanja običajnih e-storitev, zato ga tudi ne moremo reševati na enake načine, kot rešujemo varnostne probleme uveljavljenih e-storitev.

## **b) Nižja stopnja transparentnosti in vprašanje odprte kode**

Pomembno novost, ki jo prinese uporaba novega "medija" je nižja stopnja transparentnosti samega sistema. Za razumevanje "delovanja" klasične volilne skrinjice ni potrebno praktično nikakršno predznanje. Sistem volitev na papirju deluje tako, da volivci v skrinjico oddajo svoje glasovnice, po koncu glasovanja pa člani volilnega odbora volilno skrinjico odprejo in glasovnice preštejejo. Poudariti je morda potrebno še, da sta identifikacija volivca in oddaja glasovnice fizično ločena procesa. Pred začetkom glasovanja se preveri ali je volilna skrinjica prazna, volilni odbor pa skrbi, da vsak volivec v skrinjico odda le eno glasovnico. Postopek lahko nadzorujejo tudi zaupniki strank oz. kandidatov.

Preprost postopek, ki pa pri izvedbi e-volitev, ali celo i-volitev postane bistveno bolj zapleten. Povprečen državljan, pa naj gre za volivca, člana volilnega odbora ali zaupnika na volišču nima ustreznega znanja za podrobno razumevanje delovanja sodobnih informacijsko informacijskih sistemov (tako strojnega, kot programskega nivoja, vključno z razumevanjem in poznavanjem operacijskega sistema ter volilne aplikacije). Ti sistemi so kompleksni, kar jim zmanjšuje transparentnost pa tudi samo varnost. Stranski pojav tega je lahko tudi manjše zaupanje v celoten sistem.

---

<sup>2</sup> Študija izvedljivosti e-volitev s predlogi implementacije navaja podatek, da so "v ZDA z raziskavo *Secure Electronic Registration and Voting Experiment (SERVE)* prišli do spoznanja, da so oddaljene e-volitve preko interneta varnostno tako ranljive, da lahko ogrozijo zasebnost volivca in omogočijo ponarejanje glasov. Ugotovili so, da so nekatere problematične lastnosti *inherentne internetu* in, da se jim na današnji tehnološki stopnji razvoja ne da izogniti." (Turk, 2004: 19).

<sup>3</sup> Direktiva 2006/24/ES Evropskega parlamenta in Sveta z dne 15. marca 2006 o hrambi podatkov, pridobljenih ali obdelanih v zvezi z zagotavljanjem javno dostopnih elektronskih komunikacijskih storitev ali javnih komunikacijskih omrežij, in spremembi Direktive 2002/58/ES (Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC), sprejeta 14. 12. 2005. Official Journal L 105, 13/04/2006, p. 0054 - 0063.

<sup>4</sup> Zakon o spremembah in dopolnitvah Zakona o elektronskih komunikacijah (ZEKom-A), Uradni list RS, št. 129/06.

Pri tem se seveda takoj zastavi vprašanje ali bi moral biti sistem elektronskih oziroma internetnih volitev odprtokoden, ali ne. Leta 1883 je flamski lingvist in kriptolog Auguste Kerchoffs objavil članek *La cryptographie militaire*, v katerem je izpostavil šest načel, ki jih morajo upoštevati dobri šifrirni sistemi. Eno izmed teh se imenuje Kerchoffsov zakon, ki pravi, da je dober šifrirni sistem varen, tudi če je o njem znano vse, razen šifrirnega ključa (Schneier, 2002). Kerchoffsov zakon tako zavrača načelo, da je mogoče varnost zagotoviti s skrivanjem (t. i. 'security through obscurity'), ter poudarja načelo varnosti skozi transparentnost (ang. *security through transparency*). Kerchoffsov zakon opozarja na dejstvo, da skrivnost ne zagotavlja varnosti, pač pa da vsaka skrivnost celo predstavlja možno točko zloma varnosti, saj je pri sistemih, ki niso odprti, veliko večja verjetnost, da je v njih kakšna napaka, ki bi jo javni pregled verjetno odkril, avtorji pa bi s tem dobili možnost, da jo odpravijo. Bruce Schneier, ki je med drugim tudi avtor številnih člankov in knjig o kriptografiji, je zapisal: "Ne spominjam se nobenega kriptografskega sistema, razvitega na skrivaj, v katerem ne bi, potem ko je bil razkrit javnosti, kriptografska skupnost našla napake" (Schneier, 2002). Kerchoffsovo načelo je mogoče prenesti tudi na programsko opremo. Eric S. Raymond tako pravi: "Vsaka varnostna programska oprema, ki ne predpostavlja, da sovražnik poseduje izvorno kodo, je nevredna zaupanja; zatoorej: nikoli ne zaupaj zaprti kodi" (Raymond, 2004).

Odprtost je torej predpogoj za transparentnost in nadzor nad delovanjem informacijsko komunikacijskih sistemov, posledično pa odprtost omogoča kvaliteten varnostni pregled sistema, odkrivanje napak in pomanjkljivosti, ter povečuje zaupanje v sistem. Že samo dejstvo, da so sodobni informacijsko komunikacijski sistemi kompleksne naprave, uporabnikom in javnosti onemogoča vpogled v njihovo delovanje. Onemogočen dostop do programske kode, kar v praksi pomeni, da je tak elektronski volilni sistem v bistvu "črna škatla" v delovanje katere nimamo pravega vpogleda, pa transparentnost teh sistemov le še zmanjšuje.

Odgovor na vprašanje odprta koda da ali ne je torej jasen: odprta koda je nujen predpogoj za zagotovitev zanesljivosti in varnosti sistema e- ali i-volitev. Potrebna je tako zunanja (plačana) revizija, kot dostop do kode splošni (in ne zgolj zainteresirani) javnosti. Seveda je za res temeljito revizijo takega potreben tudi ustrezen čas, zato hitenje z uvedbo i-volitev že iz stališča zagotavljanja varnosti ni na mestu. Pri uporabi odprte kode sicer lahko nastopi vprašanje odgovornosti za zanesljivost delovanja, zato je potrebno natančno razlikovati med avtorjem in skrbnikom, prav tako pa dejstvo, da je koda odprta ne pomeni nujno, da mora biti koda dostopna pod kakšno izmed prostih licenc (npr. GNU GPL). Pomeni le, da mora imeti javnost, oz. katerikoli posameznik, prost dostop do kode za namene pregleda in testiranja.

Klub vsemu je smiselno še enkrat poudariti, da je odprtost sistema zgolj predpogoj za njegovo transparentnost, bistveni problem pa ostaja znanje in sposobnosti za razumevanja sistema tako s strani članov volilnih odborov, zaupnikov ter konec koncev tudi volivcev.

### **c) Sistem internetnih volitev ne zagotavlja anonimnosti sam po sebi**

Kot je bilo že večkrat poudarjeno, je problem zagotavljanja tajnosti glasovanja oz. anonimnosti volivca eden ključnih problemov i-volitev. Ko govorimo o anonimnosti gre lahko za tajnost glasovanja (tim. anonimnost glasovnice), lahko pa tudi za neobstoje informacije o tem, da se je posamezen volivec sploh udeležil volitev. Res je sicer, da v obstoječem klasičnem sistemu volilni odbor na volilnem imeniku s svinčnikom označi kateri volivci so se pojavili na volišču, vendar je ta evidenca ročna. Pri internetnih volitvah bi bila taka evidenca računalniško vodena, kar seveda odpira nove vidike vprašanja anonimnosti, med drugim tudi vprašanje zbiranja in zavarovanja

osebnih podatkov, kar ureja *Zakon o varstvu osebnih podatkov*.<sup>5</sup>

Tajnost glasovanja (glasovnic) naj bi po estonskem zgledu tudi v Sloveniji zagotovili s sistemom tim. dvojnih "elektronskih ovojnici". Sama glasovnica bi se nahajala v prvi, šifrirani "elektronski ovojnici", ta pa bi se "vstavila" v drugo, ki bi bila digitalno podpisana in bi vsebovala ime volivca in ustrezen časovni žig (s čimer je omogočeno, da se upošteva zadnji glas volivca, ki elektronsko voli večkrat). Za samo ugotavljanje volilnega rezultata bi nato imeli dva strežnika. Na prvem bi preverili digitalne podpise volivcev, ki so oddali glasovnico (in preverili ali imajo volilno pravico ter izločili morebitne prejšnje glasovnice istega volivca, oziroma v primeru volivca, ki se je udeležil tudi klasičnih volitev izločili vse elektronske glasovnice), nato pa bi šifrirane glasovnice prenesli na ločen strežnik, kjer bi jih dešifrirali in ugotovili volilni rezultat. S tem bi se zabilasala informacija o tem kako je posamezen volivec volil, s čimer bi se zagotovila tajnost glasovanja.

V čem je torej problem? Problem je v tem, da nam sistem *sam po sebi ne zagotavlja* anonimnosti. Če bi bilo namreč preverjanje prve "digitalne ovojnice" in dešifriranje druge izvedeno na istem strežniku oziroma izvedeno na povezan način, bi sistem omogočal ugotavljanje kako je glasoval konkreten volivec. S pravilno izvedbo anonimizacije glasovnic pa to ni mogoče. Gre torej za to, da tehnologija sama po sebi ne zagotavlja tajnosti glasovanja, pač pa je potrebno tajnost glasovanja doseči z anonimizacijo. To pa preprosto pomeni, da problema tajnosti glasovanja ne rešujemo s tehnologijo, pač pa z ustreznimi pravnimi pravili. Tajnost glasovanja nam torej ne zagotavlja več sistem kot tak, temveč jo zagotavlja zaupanje v posestnika šifrirnega ključa oziroma upravitelja informacijsko komunikacijskega sistema. S tem problem ni več tehničen, pač pa družben - gre za vprašanje zaupanja.

Povedano drugače: uporaba nove tehnologije odpira nove probleme, ki pa jih ne rešujemo s tehnologijo, pač pa z dodatnimi pravnimi in organizacijskimi pravili.

#### **d) Pri internetnih volitvah volivcu ni zagotovljeno varno volilno okolje**

Naslednji problem i-volitev je v tem, da država volivcu ne zagotovi varnega volilnega okolja. Pri tem sta pomembna dva vidika. Prvi vidik zadeva problem varnosti terminalne opreme uporabnika. Ker bi bil sistem i-volitev odprt (v smislu, da se nanj lahko povezujejo tudi varnostno nepreverjene naprave - računalniki volilnih upravičencev), to pomeni, da vseh delov sistema ni mogoče nadzorovati in na njem zagotoviti tehnično-informacijske varnosti. Med nevarovane dele sistema gotovo sodi javno telekomunikacijsko omrežje in terminalna oprema na strani uporabnikov (računalnik, modemi, usmerjevalniki, brezžične povezave). Če se da problem varnosti javnega telekomunikacijskega omrežja (oziroma celotnega prenosnega omrežja) rešiti z uporabo šifriranja, pa problem varnosti terminalne opreme na strani uporabnika ni rešljiv na enostaven način. Za zagotovitev varnosti bi bila namreč potrebna ustrezna zunanja naprava (npr. čitalnik pametnih kartic), ki zagotavlja varen vmesnik med krmilnikom v mediju in računalnikom, kar omogoča varno podpisovanje in/ali šifriranje dokumentov. Pri tem se seveda postavljajo vprašanja kdo bo zagotovil take čitalnike in ustrezne pametne kartice. Znano je, da je v primeru Estonije pametne kartice s certifikati državljanom zagotovila država. Tako je med estonskimi volivci okrog 90% takih, ki imajo pametno kartico, poleg tega - in to ni nepomembno - imajo država in državljani že pet let izkušenj z uporabo pametnih kartic (Martens, 2007). Poročilo *Internet in slovenska država* iz leta 2006 pa za Slovenijo ugotavlja, da ima digitalne certifikate le dobrih 36% uporabnikov interneta (govorimo o aktivnih mesečnih uporabnikih interneta v starosti med 12 in 65 let, ne o celotni populaciji volilnih upravičencev!), večinoma imajo bančne certifikate, certifikat SIGEN-CA pa ima

<sup>5</sup> Zakon o varstvu osebnih podatkov (ZVOP-1), Uradni list RS, št. 86/04.

manj kot 10% uporabnikov (Vehovar in Zupanič, 2006: 69).

Drugi problem pa predstavlja dejstvo, da imajo pri i-glasovanju volivci možnost glasovati od doma (lahko pa tudi iz službe ali drugega nenadzorovanega prostora). S tem se odpirajo možnosti za različne pritiske na volivce, možnosti za preprodajo glasov, saj volivec lahko dokaže kako je volil, lahko pa pride tudi do kršitev tajnosti glasovanja, ko nekdo z bolj ali manj prikritim opazovanjem preprosto ugotovi kako je kdo volil. S tem izgubimo tim. "posvečeni prostor", kjer je zagotovljena ustrezna zasebnost za volivca, ni pa tudi več volilnega odbora in zaupnikov, ki bi skrbeli, da volivec svobodno izrazi svojo voljo. Z drugimi besedami, ko smo volišče "preselili" v dnevno sobo, je odgovornost za zagotovitev varnega volilnega okolja država preložila na volivca.

Problem, ki je zopet nastal zaradi uporabe nove tehnologije – tako imenovanega "novega medija" - pa spet rešujemo s pravnimi in organizacijskimi pravili. Tako ima po predlogih volivec možnost elektronsko glasovati večkrat (šteje se zadnji elektronsko oddani glas) ali celo glasovati na klasičen način (v tem primeru se šteje klasično oddan glas, elektronske glasovnice pa se zavržejo), vendar to ne rešuje osnovnega problema. To pa je: uvedba nove tehnologije je odprla nove možnosti zlorab (katerih prejšnji sistem ni dopuščal), te nove probleme pa ne rešujemo s tehnologijo, pač pa s pravnimi in organizacijskimi pravili. Poleg tega tak sistem že v osnovi skuša reševati zgolj problem odkritih pritiskov na volivca, ne pa tudi problema prikrite kršitve volilne tajnosti.

Prenašanje odgovornosti za pošteno in varno izvedbo volitev na volivca je problematično predvsem zato, ker se na njej zamaje načelo tajnosti glasovanja. Ker je tajnost glasovanja pomembna zaradi zagotavljanja same legitimnosti glasovanja, je tajnost in z njo povezana neposrednost glasovanja po najinem mnenju bistvena za sodobno demokracijo.

### **e) Kaj ne gre pri i-volitvah le za nadaljevanje ideje o glasovanju po pošti?**

Med zagovorniki uvedbe i-volitev se pojavlja tudi argument, da gre pri volitvah preko interneta le za tehnološko nekoliko drugačen način glasovanja po pošti. Oba načina glasovanja je na neki ravni gotovo mogoče vzporejati. Vendar pa slovenska zakonodaja določa, da po pošti lahko glasujejo osebe, ki so na zdravljenju v bolnišnicah oziroma oskrbovanci domov za starejše, ki nimajo stalnega prebivališča v domu ter volivci, ki so na dan glasovanja v tujini.<sup>6</sup>

To pomeni, da se volitev po pošti udeležuje le omejen krog ljudi, poleg tega gre v slovenskem volilnem sistemu za izjemo, ki glasovanje omogoča posebnim, deprivilegiranim skupinam ljudi, ki sicer ne bi mogle voliti, pri i-volitvah pa bi princip glasovanja in nekontroliranega volilnega okolja potencialno prenesli na celotno populacijo volivcev. Hkrati je smiselno ponovno poudariti, da za razumevanje in nadzorovanje sistema glasovanja po pošti (predvsem odpiranja dvojnih kuvert z identifikacijo volivca in ločene kuverte glasovnico) ni potrebno kakšno posebno tehnično predznanje, kar za digitalno odpiranje dvojnih elektronskih glasovnic ne velja.

## **Primerjava i-volitev z glasovanjem s kroglicami**

Ker pri internetnih volitvah sistem sam po sebi ne omogoča izpolnjevanja določenih zahtev za poštene in demokratične volitve, pač pa je treba te zahteve doseči z uvedbo dodatnih pravnih in

<sup>6</sup> Zakon glasovanje po pošti omogoča tudi osebam, ki so na služenju vojaškega roka, vendar to zaradi ukinitve naborniškega sistema ni več aktualno.

organizacijskih pravil ter zaupanja (pri tem se tudi odpira vprašanje tim. "človeškega faktorja"), v nadaljevanju avtorja postavlja tezo, da so internetne volitve bolj primerljive glasovanju s kroglicami, kot klasičnemu glasovanju.

V kontekstu tajnosti glasovanja je zanimiva primerjava sistema i-volitev z volitvami s kroglicami, ki se je uporabljal v kraljevini SHS in v povojni Jugoslaviji. Pri volitvah s kroglicami je volivec dobil glasovalno kroglico. Glasoval je tako, da je kroglico spustil v glasovalno skrinjico liste, za katero je želel glasovati (imena list so bila napisana na skrinjicah oz. so jih nepismenemu volivcu prebrali). Glasovalnih skrinjic je bilo namreč toliko kot kandidatnih list, volivec pa je izbral skrinjico svoje liste. Pred in po končanem glasovanju je moral volilnemu odboru pokazati prazne roke, s čimer se je preprečila zloraba načela en volivec - en glas. Tajnost glasovanja je bila zagotovljena s tem, da je volivec potisnil roko v vsako skrinjico, glasovalno kroglico pa spustil v tisto skrinjico, ki je pripadala listi za katero je hotel oddati svoj glas. Volilne skrinjice so bile od znotraj ustrezno obložene tako, da so zadušile zvok kroglice ob padcu (Grad, Lukšič in Zagorc, 2004: 34). Na volitvah takoj po drugi svetovni vojni je sicer prišlo do zlorabe, saj je kroglica, ki jo je volivec vrgel v "napačno" skrinjico zacingljala in s tem razkrila izbiro volivca, o čemer poje tudi znana pesem Frana Miličinskega Ježka "*Cinca marinca*",<sup>7</sup> dejstvo pa je, da je bilo pri takem sistemu povsem verjetno, da je pozoren član volilnega odbora lahko slišal (zadušen) zvok kroglice, ko je ta padla v skrinjico. Tajnost glasovanja je bila torej povezana z zaupanjem članom volilnega odbora, da ne bodo izrabili možnosti za kršitev volilne tajnosti.

Splošne javne volitve v sodobnih demokracijah morajo zagotoviti naslednjim pogojem: morajo biti splošne, svobodne, enakopravne, tajne in neposredne. Primerjava med volitvami s kroglicami z i-volitvami kaže, da oboje zadostijo pogoju *splošnosti* (vsak volivec lahko sodeluje v volilnem procesu), *enakopravnosti* (vsak volivec ima en glas) in *neposrednosti* (vsak volivec glasuje sam).

Kako pa je s kriterijema *svobodnosti* in *tajnosti*? Študija *izvedljivosti e-volitev s predlogi implementacije* iz leta 2004 o svobodnosti pravi, da je za načelo svobodnosti volitev najpomembnejše, da je celoten volilni proces voden "brez manipulacij, nasilja, vplivanja in pritiskov na volivce, s strani države ali posameznikov" (Turk, 2004: 9). V zvezi z i-volitvami je zapisano: "Nasprotno lahko pri e-volitvah, ko volivec izpolnjuje in oddaja svojo glasovnico v nenadzorovanem okolju, nanj vplivajo člani družine, tretje osebe, delodajalci ali politiki. Tveganje ni specifično le za on-line volitve, ampak je inherentno tudi predčasnim volitvam po pošti ali drugim oddaljenim načinom volitev. E-volitve pa poleg teh tveganj s seboj prinašajo nove grožnje za svobodo in integriteto odločitev volivca. Tudi če ni opisanih poskusov vplivanja na volivca, obstaja tveganje, da IT strokovnjaki v določenih primerih in okoljih spremljajo ali beležijo aktivnosti na računalniški in telekomunikacijski opremi ter tako pridobijo kopijo izpolnjene elektronske glasovnice. Še več, porazdeljena narava interneta lahko pospeši množično trgovanje in prodajo volilnih glasov. Odprava preprodaje volilnih glasov, izsiljevanja in pritiskov je možna s takim sistemom e-volitev, ki nobenemu volivcu **ne bi omogočal dokazati njegove izbire na volilni glasovnici**. V vsakem primeru velja, da je razne oblike vplivanja na volivca težko preprečiti samo s tehnologijami. Možna rešitev je razvoj javno dostopne infrastrukture in javnih ter nadzorovanih volišč." (Turk, 2004: 9). Študija tudi poudarja, da bi moral biti portal i-volitev brez volilnih reklam. Temu pogoju sicer ni težko zadostiti, odpirajo pa se vprašanja volilnega oglaševanja po spletu in elektronski pošti, ko spletna stran z volilnimi reklamami volivca usmerja na spletno volišče ter vprašanje volilnega molka, saj naj bi internetne volitve potekale v času predčasnega glasovanja.

Morda najbolj zanimiva vzporednica med volitvami s kroglicami in i-volitvami pa se kaže v primeru *tajnosti* volitev. Kot že rečeno, tajnost i-volitev ne zagotavlja sistem sam, pač pa jo

<sup>7</sup> Cinca marinca, ta je zoper nas / u črna skrinca / vrgu je svoj glas (avtor: Fran Milčinski Ježek).

zagotavljamo z anonimizacijo in zaupanjem v imetnika šifrnega ključa oz. upravitelja informacijskega sistema. Na podoben način pa je pravzaprav tajnost glasovanja zagotovljena tudi pri volitvah s kroglicami, saj sistem predpostavlja, da člani volilnega odbora ne bodo poslušali v katero skrinjico je padla kroglica (kar razkrije kako je volivec glasoval), oziroma bodo - v kolikor bodo to slišali - to dejstvo obdržali v tajnosti. Skratka, podobno kot pri sistemu i-volitev, tudi pri glasovanju s kroglicami tajnosti glasovanja ne zagotavlja sistem kot tak, pač pa je le-ta zagotovljena s pravnimi (prepoved poslušanja ali razkritja ugotovljene volivčeve izbire) in organizacijskimi (oblazinjenje skrinjic) pravili. V luči te primerjave se zdi uvedba internetnega glasovanja prej korak nazaj, kot pa modernizacija volilnega procesa.

## Ocena učinkovitosti in smiselnosti uvajanja i-volitev

Za konec si oglejmo še analizo i-volitev po prilagojeni Schneierjevi metodologiji za analizo varnostnih ukrepov. Bruce Schneier v knjigi *Beyond Fear* (2003) predlaga analizo varnostnih ukrepov v petih točkah oz. z zastavitvijo petih vprašanj, ki smo jih za potrebe učinkovitosti i-volitev prilagodili takole:

1. Kaj skušamo zaščititi oz. izboljšati z uvedbo i-volitev?
2. Katere so težave z obstoječim načinom glasovanja?
3. Kako dobro uvedba i-volitev lajša te težave?
4. Katere težave *povzroč*a uporaba i-volitev?
5. Kakšne dileme in kakšno tehtanje (ang. *trade-off*) predpostavlja uvedba i-volitev?

### **1. Kaj skušamo doseči oz. izboljšati z uvedbo i-volitev?**

Z uvedbo i-volitev skušamo izboljšati sistem glasovanja, povečati volilno udeležbo in posledično izboljšati demokracijo. Skušamo se tudi predstaviti kot moderna država.

### **2. Katere so težave z obstoječim načinom glasovanja?**

Zagovorniki uvedbe i-volitev navajajo dva sklopa težav: padanje volilne udeležbe in zanimanja za demokracijo ter dejstvo, da so klasične volitve staromodne (da je potrebno volilni proces modernizirati, itd.).

### **3. Kako dobro uvedba i-volitev lajša te težave?**

Uvedba i-volitev po eni strani omogoča, da volivec glasuje od doma in se mu ni treba sprehoditi do volišča, kar v teoriji lahko dvigne volilno udeležbo. Konkretnih študij o dvigu volilne udeležbe sicer ni, a nekateri prikazani podatki kažejo, da v praksi ne prihaja do drastičnega dviganja volilne udeležbe zgolj zaradi uvedbe i-volitev.

Projekt i-volitev pomeni tudi dobro promocijo tako za državo, kot za njeno politiko.

### **4. Katere težave povzroč**a uporaba i-volitev?

Uvedba i-volitev med drugim povzroč

a naslednje glavne grožnje: anonimnost ni več vgrajena v sistem, pač pa jo je potrebno zagotoviti z anonimizacijo. Država volivcu ne zagotavlja več varnega volilnega okolja, temveč povečuje možnost preprodaje glasov. Uvedba povzroči tudi manjšo transparentnost sistema, pojavijo se možnosti onemogočanja delovanja i-volilnega sistema z DOS in DDOS napadi, konec koncev pa uvedba i-volitev predstavlja tudi dodaten strošek, saj je poleg i-volitev potrebno izpeljati še klasične volitve.

### **5. Kakšne dileme in kakšno tehtanje (ang. trade-off) predpostavlja uvedba i-volitev?**

Po eni strani z uvedbo i-volitev pridobimo možnost večje udobnosti pri glasovanju, (malenkostno)

se poveča volilna udeležba, projekt pa je dobra promocija za državo in njeno politiko. Po drugi strani pridobimo več potencialnih varnostnih ranljivosti in sistem, ki v osnovi ne zagotavlja tajnosti glasovanja, pač pa so za le-to potrebna dodatna pravna in organizacijska pravila.

## Zaključek

Glede na to, da je celo tehnologija "klasičnih" elektronskih volitev oziroma uporaba elektronskih volilnih naprav na nekaterih voliščih po svetu privedla do številnih težav (naj omenimo le varnostno analizo volilne naprave AccuVote-TS podjetja Diebold, v okviru katere so raziskovalci Princetonske univerze dokazali, da je na omenjene volilne naprave mogoče namestiti tim. volilni virus, poseben računalniški program, ki omogoča neopazno ponarejanje elektronskih glasovnic (več o tem v Feldman, Halderman in Felten, 2006)), se smiselno zastavlja vprašanje ali uvedba internetnega glasovanja ne pomeni vsaj enakega ali celo večjega varnostnega tveganja.

Dejstvo namreč je, da ideja internetnih volitev že v osnovi prinaša nekatere nove nevarnosti in pasti. Glede na zapisano se torej zastavlja vprašanje, ali je hitra uvedba i-volitev v Sloveniji res samoumevna? Elektronske oz. internetne volitve volilnemu procesu sicer prinašajo neko dodano vrednost, vprašanje pa je, če je le-ta zares tako velika, da je z uvedbo takega načina glasovanja smiselno hiteti brez resnih raziskav, pilotnih študij, predvsem pa široke javne razprave.

## Viri in literatura

1. Estonian National Electoral Committee: Elections And Referendums In Estonia 1989-1999, A Brief Overview. <<http://www.vvk.ee/english/overview.html>>. (Datum dostopa: 10. november 2007).
2. Estonian National Electoral Committee (2003): Parliamentary Elections 2003 – Turn-out. (Datum dostopa: 10. november 2007). <<http://www.vvk.ee/r03/paeveng.stm>>. (Datum dostopa: 10. november 2007).
3. Estonian National Electoral Committee (2007): Parliamentary Elections 2007 – Turn-out. (Datum dostopa: 10. november 2007). <<http://www.vvk.ee/r07/paeveng.stm>>.
4. Feldman, J. Ariel, Halderman, J. Alex in Felten, W. Edward (2006): Security Analysis of the Diebold AccuVote-TS Voting Machine. <<http://itpolicy.princeton.edu/voting/ts-paper.pdf>>. (Datum dostopa: 10. november 2007).
5. Grad, Franci, Lukšič Andrej in Zagorc, Saša (2004): Študija izvedljivosti ustavno-pravni in politološki vidiki uvajanja e-volitev v RS. <[http://mid.gov.si/mid/mid.nsf/V/K2633A9BFD03509F2C1256E52005D938F/\\$file/Evolitve\\_ustavnopravni\\_in\\_politoloski\\_vidiki.pdf](http://mid.gov.si/mid/mid.nsf/V/K2633A9BFD03509F2C1256E52005D938F/$file/Evolitve_ustavnopravni_in_politoloski_vidiki.pdf)>. (Datum dostopa: 18. oktober 2007).
6. Martens, Tarvi (2007): Internet Voting in Practice. <<http://www.vvk.ee/english/tarvi0303.ppt>>. (Datum dostopa: 18. oktober 2007).
7. Raymond, S. Eric (2004): If Cisco Ignored Kerchoff s's Law, Users Will Pay the Price – elektronsko pismo Erica S. Raymonda, poslano 17. maja 2004. Lwn.net, <<http://lwn.net/Articles/85958/>>. (Datum dostopa: 20. december 2006).
8. Schneier, Bruce (2001): Internet Voting vs. Large-Value e-Commerce. V *Crypto-Gram*, 15. februar 2001. <<http://www.schneier.com/crypto-gram-0102.html#10>>. (Datum dostopa: 18. oktober 2007).
9. Schneier, Bruce (2002): Secrecy, Security, and Obscurity. V *Crypto-Gram*, 15. maj 2002.
10. Schneier, Bruce (2001): Getting Out the Vote: Why is it so hard to run an honest election? V *Schneier on Security*, 31. oktober 2004. <[http://www.schneier.com/blog/archives/2004/10/getting\\_out\\_the.html](http://www.schneier.com/blog/archives/2004/10/getting_out_the.html)>. (Datum dostopa: 18. oktober 2007). <<http://www.schneier.com/crypto-gram-0205.html>>. (Datum dostopa: 3. maj 2005).
11. State Chancellery, Republic and Canton of Geneva (2007): State Council's Report to the Grand Council on the Geneva electronic voting project. <[http://www.geneve.ch/evoting/english/doc/rapports/EN\\_RD\\_639\\_and\\_Annex.pdf](http://www.geneve.ch/evoting/english/doc/rapports/EN_RD_639_and_Annex.pdf)>. (Datum dostopa: 18. oktober 2007).
12. Turk, Marjan (2004): Študija izvedljivosti e-volitev s predlogi implementacije. <<http://e-uprava.gov.si/eud/e-uprava/evolitve-priloga2.doc>>. (Datum dostopa: 18. oktober 2007).
13. Vehovar, Vasja in Zupanič, Tina (2006): Internet in slovenska država. Ljubljana: Fakulteta za družbene vede. <<http://www.ris.org/uploadi/editor/1180437049InternetInSlovenskaDrzava2006.pdf>>. (Datum dostopa: 18. oktober 2007).