Tietokonevaalit ja Tengvallin *credo*

HANNU NURMI JA ARTO SALOMAA

Johdanto

Arto Tengvallin artikkeli *Politiikan* numerossa 3—4/1991 on mielenkiintoista luettavaa kaikille tietokonevaaleista kiinnostuneille. Se täydentää ja pyrkii parantamaan sitä äänestysprotokollaa, jota esittelimme *Politiikan* numerossa 1/1991. Pidämme arvokkaana sitä, että Tengvall on huolellisesti perehtynyt artikkeliimme ja tehnyt useita huomionarvoisia korjausehdotuksia kuvailemaamme protokollaan. On hyvin tärkeää, että vaihtoehtoisia järjestelmiä tutkitaan, sillä näyttää väistämättömältä, että tietokonevaaleihin tullaan ennemmin tai myöhemmin joka tapauksessa siirtymään. Siksi olisi erinomaista, jos valinta voitaisiin tehdä mahdollisimman monipuolisesta ja ominaisuuksiltaan tunnetusta järjestelmävalikoimasta. Seuraavassa esitämme joukon omasta mielestämme tärkeitä näkökohtia Tengvallin artikkelin johdosta.

Luottamus tietokoneeseen

Vaikka Tengvallin järjestelmä on esitetty huolellisesti, emme voi yhtyä hänen peruslähtökohtaansa. Meidänkin kaavailemassamme järjestelmässä tietokoneet näyttelevät toki keskeistä osaa, mutta meillä on Tengvallia oleellisesti epäluuloisempi asenne niihin henkilöihin, jotka huolehtivat äänestysjärjestelmän rakentamisesta, käyttöönotosta ja toiminnasta. Tietokonevaalien aikakaudellakin oletamme ihmismielen pysyvän perusominaisuuksiltaan jokseenkin samanlaisena kuin nykyään. Tähän oletukseen sisältyy valitettavasti se mahdollisuus, että ihminen saattaa turvautua vilpillisiin menettelyihin tavoitteisiinsa pyrkiessään, jos katsoo sen »kannattavan». Siksi vaalijärjestelmien tulee pyrkiä eliminoimaan mahdollisuudet vilpintekoon.

Tengvall toteaa aivan oikein, ettei ole tärkeää salata ääniä sähköisiltä muistipiireiltä tai paperilapuilta, vaan toisilta ihmisiltä. Ongelmana on kuitenkin äänestystiedon — siis sellaisen tiedon, joka mahdollistaa äänen antaneen äänestäjän henkilöllisyyden paljastumisen — salassapito silloin, kun se on tallennettu ihmisten ylläpitämiin sähköisiin tai muihin tietojärjestelmiin. Kokemukset tietokoneviruksista eivät rohkaise ylenpalttiseen luottamukseen tässä asiassa. Esittelemämme järjestelmä pyrkii ja uskoaksemme myös kykenee eliminoimaan tietokonejärjestelmää ylläpitävien, äänioikeuden tarkistavien ja vaalitulosten laskennasta vastaavien vaaliviranomaisten vaalivilpin.

Tietokonejärjestelmää(kään) ei pidä ostaa kuin sikaa säkissä. Tengvallin *credo* on, että kun tietokoneen sisältävä pakkaus avataan suorassa televisiolähetyksessä, niin kone on kaikenlaista vilppiä ajatellen *tabula rasa*: juuri sitä, mitä opaskirjoissa kerrotaan. Mutta onko mahdollista taata, ettei käyttöjärjestelmään ole ohjelmoitu tietoja, jotka sopivalla hetkellä aktivoituvat muuttamaan vaalitulosta? Voisi ehkä ajatella, että suorassa televisiolähetyksessä konetta testataan mahdollisen vilpin löytämiseksi. On kuitenkin matemaattinen tosiseikka, ettei tällainen testiohjelma ole edes periaatteessa mahdollinen. Meidän esittelemässämme systeemissä ei *tabula rasa* -oletusta tehdä.

Tengvallin systeemissä ohjelmointiasemat ovat tarkoin vartioituja ja vain harvoin käytössä. Ideaalitapauksessa ylläpito tuskin vaatiikaan jatkuvaa

päivystystä. Toimintahäiriöt ja järjestelmän tietoiset sabotointiyritykset on kuitenkin otettava huomioon alusta pitäen. Ne eivät toivomalla poistu. Kriittinen lukija voisi kyllä kysyä, että jos ohjelmointiasemia tarvitaan paljon ja jos ne vaativat jatkuvaa valvontaa, niin eikö niitä sitten voisi jo käyttää äänestyspaikkoinakin. Tällöin järjestelmä olisi olennaisesti sellainen kuin esim. Yhdysvaltojen tietyissä osavaltioissa käytössä olevat äänestyskoneet. Itse asiassa jälkimmäiset olisivat Tengvallin esittelemää systeemiä parempia siinä, että äänestäjien henkilöllisyys voitaisiin tarkistaa.

Käytännön hankaluudet

Tengvall toteaa perustellusti, että äänestäjän on vaikea muistaa suuria lukuja. Todellakin, 200-numeroisten lukujen muistaminen on varmasti mahdotonta. On kuitenkin syytä korostaa, että tietoyhteiskuntaa ajatellen nykyinen infrastruktuuri on kovin primitiivinen; sitä voisi verrata liikenneverkkoon 100 vuotta sitten nykyliikenteen vaatimusten näkökulmasta. Jo 10—20 vuoden tähtäimellä Tengvallin mainitsemat ylipääsemättömät esteet lienevät poistuneet. Vilppi ja kieroilu sitä vastoin kukoistanee vielä paljon pitempään. Viittaamme tässä yhteydessä *Scientific American* -lehden syyskuun 1991 numeroon.

On syytä todeta, että eräitten kryptosysteemien vaatimien raskaiden laskutoimitusten suorittamiseen on jo nyt tarjolla tietokonesiruja, joiden ansiosta äänestäjään kohdistuvat vaatimukset pysyvät kohtuullisina. Hänen ei suinkaan tarvitse muistaa suuria lukuja, vaan ne on tallennettu laskentavälineen muistiin. Tuotekehittely tällä rintamalla etenee nykyään sangen ripeästi salaisen viestinnän yleistyessä. Näin ollen tulemme varmasti jo lähitulevaisuudessa näkemään korttien tai sirujen tapaisia apuvälineitä, joiden avulla on mahdollista yhdistää Tengvallin (ja myös meidän) kaipaama käyttäjäystävällisyys ehdottomaksi vaatimukseksi asettamaamme vaalisalaisuuteen.

Epäolennaisia eroja

Tengvall mainitsee järjestelmänsä etuna mm. sen, että äänioikeutettujen luettelot pysyvät jatkuvasti ajan tasalla, jolloin esim. kuolleet henkilöt pyyhitään pois äänioikeutettujen joukosta. Meidän esittelemässämme systeemissä kullakin äänestäjällä on julkinen kryptausfunktio ja yksityinen dekryptausfunktio. Kuolleen henkilön äänioikeus eliminoituu meidän järjestelmässämme siten, että kuollut henkilö poistetaan äänioikeutettujen luettelosta, joten jos joku pyrkii äänestämään vainajan jälkeensä jättämillä kryptaus- ja dekryptausfunktioilla, niin äänioikeuden tarkistava systeemi pystyy torjumaan yrityksen.

Julkisen avaimen kryptosysteemeissä avaimia voidaan toki vaihtaa vaikka joka vaaleissa. Ehkä näin on jopa suositeltavaa menetellä. Vaihtaminen tapahtuu yksinkertaisesti siten, että ilmoitetaan julkisesti, että uusi kryptausfunktio on otettu käyttöön. Tietenkään ei nytkään paljasteta salaista dekryptausfunktiota. Mistään jatkuvasta äänioikeuden menetyksestä ei siis kuvaamassamme systeemissä voi olla kyse.

Tengvallin järjestelmässä äänestyskorttinsa ja salasanansa hukannut äänestäjä voi tilata lokeronsa tuhoamisen. Jokin konsti Tengvallin pitäisi kyllä keksiä sitä vastaan, että äänestäjä pyytää tuhottavaksi muidenkin äänestäjien lokeroita ja äänestää sitten »heidän puolestaan».

Ajatus lokeron avaamisesta äänestäjän pyynnöstä on mielestämme epäilyttävä. Tengvallin järjestelmässähän lokerot sisältävät äänestäjän koko äänestyshistorian. Vääriin käsiin joutuessaan tällaisella tiedolla voisi olla hyvin ikäviä seurauksia äänestäjälle. Jo epäily äänestyshistorian avautumisesta viranomaisille voisi nakertaa äänestäjän halua paljastaa todelliset mieltymyksensä äänestyksissä.

Siirtyminen jatkuviin vaaleihin tuntuu olevan Tengvallille hyvin tärkeää. Emme ole tähän puoleen puuttuneet artikkelissamme, sillä äänestysjärjestelmämme arvioinnin kannalta vaalien pitämisfrekvenssillä ei ole merkitystä. Saatamme toki ymmärtää kiinnostuksen tietokonevaaleihin jatkuvien vaalien näkökulmasta, mutta haluamme korostaa, että tietokonevaalit ja jatkuvat vaalit ovat erillisiä asioita.

Lopuksi

Arto Tengvallin esittelemä äänestysjärjestelmä on mielestämme tutkimisen arvoinen erityisesti käyttäjäystävällisyytensä johdosta. Suhtaudumme kuitenkin varauksin sen tiettyihin yksityiskohtiin ja erityisesti lähtökohdaksi otettuun oletukseen, jonka mukaan esitellyt järjestelyt riittävät sulkemaan pois vaaliviranomaisten vilpin. Lisäselvityksiä kaipaavat myös eräät äänestäjien ulottuvilla olevat sabotointimahdollisuudet, erityisesti mahdollisuus muiden äänestäjien lokeroiden tuhoamiseen. On todennäköistä ja ainakin toivottavaa, että joihinkin ongelmiin löytyy tyydyttävä ratkaisu. Toi-

vomme, että huomautuksistamme on hyötyä Tengvallin järjestelmän kehittelyssä. Kuten aluksi totesimme, on pelkästään myönteistä, että tietokoneäänestyksen erilaisia malleja kehitellään ja analysoidaan. Vain siten voimme olla kohtalaisen varmoja siitä, että kun aika on kypsä tietokoneäänestyksen käyttöönotolle, meillä on tarjota hyviä järjestelmiä.