# DEBATT | Nii palju vastamata kahtlusi ja võltsimisvõimalusi. Kuidas saaksime usaldada valimisteenist...

*Märt Põder*

10.04.2025, 13:00

(132)

Valimisteenistuse juht Arne Koitmäe lükkab turvalisuskahtlused ümber

Juba homme on oodata riigikohtust järjekordset lahendit kaebuses, mis seab kahtluse alla e-valimiste ning nende vaatlemise aususe.

**Märt Põder**

digiõiguste aktivist




*E-hääletuse vaatlemine*

*FOTO: Märt Põder| Delfi Meedia*

21 min

Demokraatliku legitimatsiooni ühemõttelisus ja vaidlustamatus on riikluse üks kõige olulisemaid

garantiisid ja seetõttu on eriti kahetsusväärne, kui valimiste korraldaja oma vigade tunnistamise asemel püüab neid peita vassivate väidete taha. Just seda paistab olevat teinud valimisteenistuse juht Arne Koitmäe, kui mõtles veebruaris välja käsitsi tehtavad pistelised kontrollid, mis pidanuks välistama temapoolse hüpoteetilise võltsimise näiteks 2023. aasta Riigikogu valimistel.



*Märt Põder*

*FOTO: erakogu*

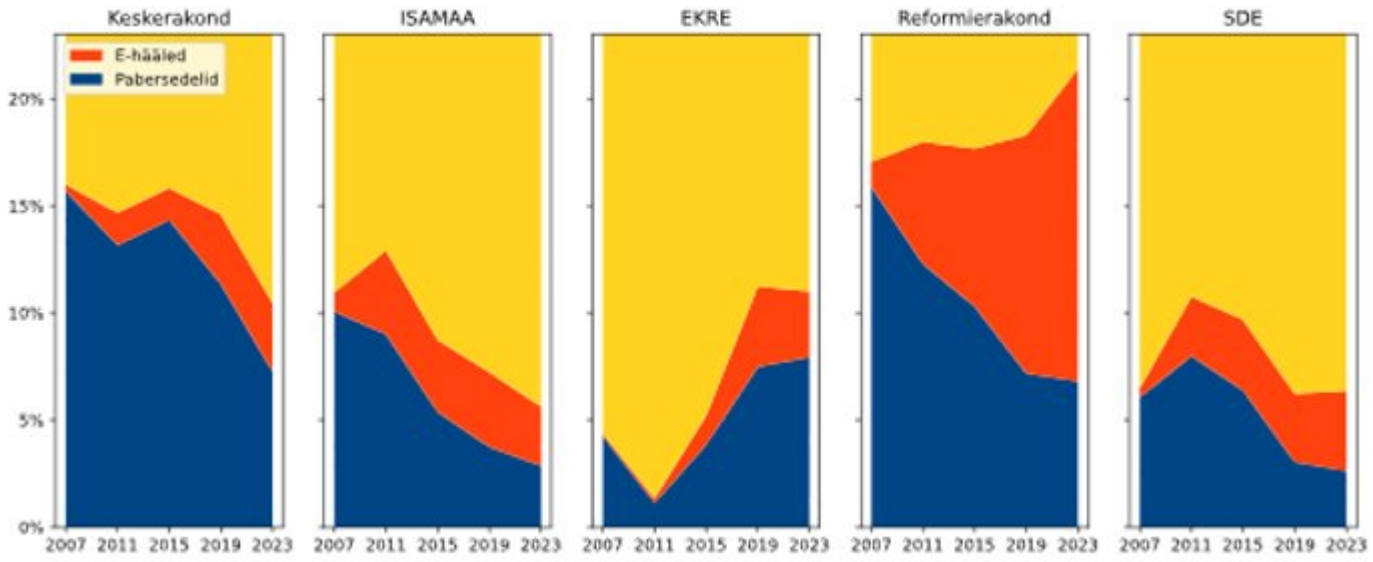
Seda tuleb järeldada Arne Koitmäe möödunud kuul ajakirjanduses antud vastustest (14.03, 20.03) osutustele, et tõendid selliste kontrollide läbiviimise kohta puuduvad ning sõltumatud osapooled pigem lükkavad nende läbiviimise ümber (7.03, 17.03). Kui valimisteenistuse juht on avalikkust valimiste protseduuride ja auditeerimisel läbitud sammude kohta sihilikult eksitanud, tuleb teda käsitleda ilmselt julgeolekuriski ja ohuna demokraatiale. Ent mis võiks üldse sundida meid valijatena usaldama valimisteenistust, mis sai kuni 2024. aastani vähemalt hüpoteetilise soovi korral täiesti märkamatult vahetada sedeleid digitaalses valimiskastis?

## Märkamatud manipulatsioonid valimiskastiga

Avastus ise polnud tegelikult uus, sest Kristjan Düüna oma magistritöös otsis tõendust OSCE

valimisvaatlejate 2023. aasta raporti väitele, et siseründaja oleks saanud valimiskastis hääli vahetada (lk 8, sh allmärkus 22) – ja leidis sellele eksperimentaalse kinnituse. Kuna OSCE raport avaldamise ajal valimisteenistuses reaktsiooni ei põhjustanud ja seda tuldi pool aastat hiljem meie ametnikele eraldi kohapeale seletama, siis võib arvata, et abivalmi tudengi sekkumiseta säilinuks Arne Koitmäel võimalus vahetada digitaalses valimiskastis märkamatult sedeleid veel sügisestel KOV valimistelgi.

Kontekstiks tuleks meenutada, et suur osa usaldamatusest e-hääletuse vastu tuleneb sellest, et uudse hääletusviisi poliitiline suurtoetaja Reformierakond on e-hääletusega alustamisest 2005. aastal võitnud kõik Riigikogu valimised ja seda kasvava e-häältesaagiga. See on ülekaalukas võit viitel järjestikustel valimistel ja heausksel valijal võib vähemalt tekkida täiesti põhjendatud kahtlus, et see võib olla saavutatud e-hääletuse manipuleerimise teel.




*Valimistulemused ja e-hääled*

*FOTO: Märt Põder| Delfi Meedia*

Ületamatu probleem on siin aga selles, et isegi kui me nüüd teame, et valimisteenistusel olidki kõik võimalused sellist võltsimist segamatult läbi viia, polnud meil riigikogu valimiste ajal ega ole ka praegu tagantjärele võimalik teada, kas valimisteenistus seda võimalust tegelikkuses kasutas või ei kasutanud – või kasutas ehk tagaust mõni välisründaja?

## Raportid käsitsikontrolle ei kinnita

Selle taustal mõjuvad valimisteenistuse kinnitused e-hääletuse jätkuvast „turvalisusest“ mõnitusena, sest eksperimentaalne hääletuskanal, mille puhul pole võimalik teha kindlaks, kas võltsimine toimus või mitte, ei saa sobida kasutamiseks demokraatlikel valimistel. Nüüdseks on aga tulnud välja, et magistritööd juhendanud doktorant Tarvo Treier oli vahetult enne uurimistöö tulemuste avalikkuse ette jõudmist Ago Samosonile kirja teel kinnitanud, et „audiitoritel oli teoreetiliselt võimalik teha käsitsi pistelist kontrolli, aga mida arvatavasti ei tehtud“.

Kuigi rohkem kui 300 000 e-hääle vaevarikkale käsitsi kontrollimisele osutab arveteõiendamises

juhtivteaduri Ago Samosoniga nii Postimees, ERR kui EPLi faktikontroll, ei leia märget selle kohta ei KPMG audiitorite Risto Jürissoni ja Taimo Toigeri 2023. aasta ametlikest auditiraportitest ega kinnita selle läbiviimist ka kohapeal protseduure jälginud vaatlejate, sh siinkirjutaja kogemus. Tegelikult rõhutab tõendite puudumist sellise kontrolli läbiviimise kohta nii Kristjan Düüna magistritöö (lk 33) kui ka juhendajaga kahasse avaldatud rahvusvaheline teaduspublikatsioon (lk 197771), mis lisaks pühendab eraldi peatüki arutamisele, et on ebaselge, mis metoodikaga selliseid kontrolle käsitsi teha saakski (lk 197772).

Eksperimentaalne hääletuskanal, mille puhul pole võimalik teha kindlaks, kas võltsimine toimus või mitte, ei saa sobida kasutamiseks demokraatlikel valimistel.

Valimisteenistus Kristjan Düüna magistritöö andmetel kõigest kinnitas, et audiitoritel „on võimalik“ teostada pistelist kontrolli (lk 33). Tööd juhendanud doktorandi Tarvo Treieri meediakampaania valgusvihus esitatud seisukohtades on *teoreetilisest võimalikkusest* aga saanud üleöö *praktiline tegelikkus* – ta väidab, et selliseid kontrolle tõepoolest tehti, lihtsalt mitte 100% ulatuses. Aga täpselt mitme protsendi ulatuses siis? Ja miks väitis ta veel loetud päevad enne ülesastumist ETV uudistes, et kontrolle „arvatavasti ei tehtud“?

Kui teadlane soovib ülikooli kommunikatsiooniosakonna ärgitusel või mõnel muul põhjusel tagasi võtta iseenda varem avaldatud seisukohad eelretsenseeritud teaduspublikatsioonis, mis on pealegi üle kinnitatud teadlaste omavahelises kollegiaalses suhtluses, siis ei piisa selleks äkilisest meelemuutusest telekaamera ees, vaid tuleks selgitada eksimise põhjusi ning tutvustada seisukohtade korrigeerimiseks kasutatud allikaid.

## Audiitor võltsimist ei avastakski

Kuigi magistrant Kristjan Düüna annetas valimisteenistusele oma uurimistöö tulemusena valminud mõnesaja realise programmijupi, mille see saab audiitorile täiendavateks kontrollideks edastada, ei lahenda see siiski probleemi. Nii magistritöös (lk 33) kui teaduspublikatsioonis (lk 197772) antakse mõista, et audiitor peaks õigupoolest kõik sellised programmid ise kirjutama, sest vastasel juhul saab valimisteenistus audiitorit jätkuvalt liiga hõlpsasti eksitada.

Tegelikkuses ongi üliõpilase avastatud turvanõrkus kurioosne hoopis selle poolest, et lubas valimisteenistusel valimiskastis sedeleid vahetada ka igasuguse pingutuseta audiitori petmiseks – audiitorile edastatud programm jättis osa valimiskastist lihtsalt auditeerimata. See tähendab, et elektroonsel valimiskastil oli sisuliselt sisseehitatud topeltpõhi, mis võimaldas seal mugavalt sedeleid vahetada. Välja tuli reetliku topeltpõhja olemasolu aga alles siis, kui valimistulemused olid juba välja kuulutatud ja elektroonsed asitõendid seaduse nõuete kohaselt hävitatud.

Siin peegeldub põhimõtteline probleem e-hääletuse passiivse vaatlemise või auditeerimisega, mis ei kõlba puuduste või manipulatsioonide avastamiseks. Küsimuse all olevatel Riigikogu valimistel ei märgi palgatud audiitorite raportid ei skandaalset topeltpõhja ega ühtegi teist olulistest puudustest digiallkirjade või puuduvate väljadega e-häälte krüptogrammides või korralagedusega

valimiste peavõtme genereerimisel, mida on vägikaikaveo tulemusel valimisteenistusega toonud välja *sõltumatud vaatlejad*. Nii võib ütelda, et auditeerimise peamine kasutegur avalikkuse jaoks on olnud pelk toimingute registreerimine, sest toimingute logisid ja videoid on valimisteenistus hoidnud salajas hoolimata vaatlejatele antud lubadustest neid jagada.

## Innovatiivne tähendus valimiste salajasusele

Avalikkuse kontroll e-hääletuse üle praegu sisuliselt puudub ja kuigi seaduse järgi on valimisteenistuse ja -komisjoni toimingud avalikud, on e-hääletusega seotud protseduure *ad hoc* põhjendustega järjepanu salajaseks kuulutatud. Nii kuulutas riigikohus 2024. aasta valimiskaebuste arutamisel valimiskomisjoni nõudel salajaseks (5-24-14, p 69) e-hääletuse turvadokumentatsiooni, sest see loovat „ohu e-hääletuse kahjustamiseks“ – ometi kaebasin valimisvaatlejana just sellesama dokumentatsiooni ja sellest lähtuvate protseduuride puudulikkuse üle.

Selle loogilise jätkuna eemaldati siinkirjutaja 6. märtsil 2025 valimisvaatlejana seaduse järgi avalikult valimiskomisjoni koosolekult päevakorrapunkti ajaks, mille teemadeks olid „e-hääletamise riskikäsitlusplaan“ ja „e-hääletamise toiminguid“. Valimiskaebus selle kohta jõudis riigikohtusse juba 11. märtsil ja riigikohus on lubanud nüüd teha lahendi teatavaks 11. aprillil. Kuigi menetlejatena on toodud valimiskaebuste puhul enneolematud viis kohtunikku riigikohtu esimehe Villu Kõve juhtimisel, on veel vara hinnata, kas kõrge kohus on valmis e-hääletuse vaadeldavuse küsimusi ka sisuliselt arutama.

Paradoksaalselt ei paista riigikohus märkavat, et ohuallikas valimistele ei saa demokraatias olla mitte avalik debatt valimiste korralduse üle, vaid hääletussüsteem, mis hoolimata seaduse järgi ette nähtud avalikkusest siiski erapooletut kõrvalpilku ja avalikku küsitlemist ei talu. Juba oma esimestest sammudest põhineb meie e-hääletus kui mitte otsesel pettusel, siis vähemasti enesepettusel, et suudetakse panna arvutid iseseisvalt viima ellu demokraatlike valimiste põhimõtteid – neist põhimõtetest on aga järgnenud 20 aastaga kukesammudega kaugenetud.

## Põhiseadus garanteerib julgeolekut

E-hääletusega 2005. aastal alustades tuli riigikohtul tunnistada, et selle läbiviimiseks oletatavasti vajalik ülehääletamine riivab *valimiste ühetaolisust*, mille võimaldamiseks lahjendati küsitava õigusliku innovatsiooniga omakorda *hääle salajasuse* põhimõtet (3-4-1-13-05, p 23-32). Praeguseks on selgunud, et ülehääletamisel pole häältemüügi ärahoidmisel määravat rolli ja lahjendatud salajasuse tingimustes on valimisteenistus loonud võimaluse vaadata valijate hääli – nt 2023. aasta valimiste kurioosumina koguni president Alar Karise oma.

Hääletusviisi nõrkus põhiseaduslikkuse mõttes pole abstraktne juriidiline küsimus, vaid iga allahindlus vabade, üldiste, ühetaoliste, otseste ja salajaste valimiste põhimõtete tagamisel muudab valimised rünnatavaks ka tegelikkuses. Demokraatlike valimiste põhiseaduslike nõuete tagamist ei saa asendada „turvalisusega“ – innovatiivse valimispõhimõttega, mida põhiseadus isegi

ei nimeta ja mille asjaolud on avalikkuse eest salastatud.

Kui me pole valmis usaldama põhiseaduse tarkust, siis riskime arutult demokraatiaga.

**Riigi valimisteenistusel ega ühelgi teisel valimiste korraldajal ei ole kunagi olnud võimalust valimiskastis e-hääli märkamatult välja vahetada. Hääletamistulemuse tervikluse tagamiseks näeb seadus ette kontrollmehhanismid, mida järgitakse ja mille järgimist kontrollitakse.**

E-hääletamine on kasutusel olnud 20 aastat, selle aja jooksul on üksipulgi läbi arutatud nii süsteemi turvalisus kui ka põhiseaduspärasus. Kokku on kutsutud erinevad e-hääletamise turvalisust uurivad komisjonid ja tellitud eriraportid ning sellist kohta süsteemis, kus oleks toimunud või saaks päriselt toimuda e-häältega manipulatsioon, ei ole leitud. Teoreetilised riskid, millele skeptikud ja osa vaatlejaid rõhub, saaksid toimuda olukorras, kui puuduksid süsteemi kontrollmehhanismid. Aga kontrollmehhanismid on ja need on seaduse tasandil ette nähtud.

Varem sai ka avalikult

Igal valimistel kontrollib audiitor e-häälte lugemise sisendi ja väljundi omavahelist vastavust ning krüptogrammide pistelised käsitsi kontrollid on digiallkirjade, kontrollsummade, valija nimekirja ja muude arvuliste andmete kontrollimise kõrval olnud aastaid tavapärane praktika. Enne Euroopa Liidu isikuandmete kaitse üldmääruse kehtima hakkamist on krüptogrammide kontrolle tehtud ka avalikult ehk vaatlejate juuresolekul.



*Riigi valimisteenistuse juht ARNE KOITMÄE*

*FOTO: Martin Ahven| Õhtuleht*

Sisuliselt tähendab krüptogrammide kontroll seda, et e-häälte töötlemisetapis kontrollitakse, kas lugemisele minevad hääled on samad, mis pärinevad e-valimiskastist. Selleks võetakse pisteliselt ette töötlemisel olevad krüptogrammid ja kontrollitakse, kas need samad krüptogrammid on ka valimiskastis. Kuivõrd valimiskastis on krüptogrammid koos isikuandmetega (hääletaja nimi ja isikukood), tohivad taoliste andmetega tutvuda ainult valimiste korraldajad ja audiitorid, kelle

ülesanne on andmeaudit seaduse kohaselt läbi viia. Seetõttu ei saa ka vaatleja enda kogemusele viidates väita, et sellist kontrolli 2023. aasta valimistel ei tehtud – seaduse kohaselt ei ole vaatlejatel õigust tutvuda hääletanute isikuandmetega ja seega ka viibida selle kontrolli juures.

Alates 2024. aastast on tänu TTÜ teaduritele tehtud krüptogrammide kontroll audiitorile mugavamaks – see toimub tänu vastavale programmile automaatselt ja hõlmates kõiki krüptogramme. Sellest ei saa mitte kuidagi järeldada, et varasemalt ei oleks pistelisi kontrolle üldse tehtud.

Veelgi meelevaldsemad on vaatleja järeldused, et varasemate valimiste tulemused võivad olla seetõttu võltsitud ja e-valimiskastil oli topeltpõhi. Ka Kristjan Düüna viitab oma magistritöö annotatsioonis, et seni puudus **lihtne viis seda teha** ja et tema pakutav lahendus lisab **täiendavad kontrollmehhanismid** veendumaks, et kõik hääled, mis olid olemas esialgses valimiskastis, oleks olemas kas tühistatud häälte hulgas või lugemisele minevate häälte hulgas. Etteruttavalt võib öelda, et valimisteenistus plaanib koos TTÜ teadlastega teisigi täiendusi, mis muudavad auditeerimisprotsessi paremini jälgitavaks ja audiitoritele mugavamaks.

Auditeerimise puhul ei tohiks unustada, et tegemist on sõltumatu kontrolliga. Auditeerimise ulatus on kirjeldatud seaduses ning auditi peab läbi viima infosüsteemide audiitor. Audiitor selgub hanke käigus ja valimisteenistus on seaduse kohaselt kohustatud jagama audiitoriga kõiki andmeid, mida audiitor valimistulemuse tervikluse kontrolliks vajab ja küsib. Raporti detailsuse on otsustanud iga audiitor ise.

Vaatleja heidab ka ette, et audiitorid kasutavad auditeerimisel valimisteenistuse etteantud programme ja teeb sellest järjekordsed meelevaldsed järeldused, et see võimaldab audiitoreid lihtsasti petta, jätta osa valimiskastist auditeerimata ja seeläbi luua valimiskastile topeltpõhi. Valimisteenistus avalikustab auditirakenduse lähtekoodi, sellest kompileerib audiitor ise auditirakenduse ja kontrollib sellega andmete terviklust.

Audiitori valik

Taaskord – selle kas ja kui suures mahus audiitor kasutab lähtekoodi, otsustab audiitor. Auditirakenduse lähtekood on avalikus koodihoidlas – sellega saavad kõik huvilised tutvuda ja veenduda, et selles ei peitu mingeid audiitoreid eksitavaid programmijuppe, nagu vaatleja väidab.

Avalik on ka e-valimiskasti lähtekood, mis võimaldab kõigil huvilistel selle toimimisega tutvuda ja veenduda, et seal ei ole mingeid musti kaste ega pimedaid nurgataguseid. Süsteemi vaatlejate välja toodud oht häälte välja vahetamisest siseründaja poolt on hüpoteetiline – see ei ole päriselus saavutatav, sest häälte lugemise protsess on seaduses kirjeldatud, selle järgimist kontrollitakse ning kõik sellised katsed on tuvastatavad.

Mistahes väited, et valimisteenistus piirab omavoliliselt vaatlejate ligipääsu infole ja salastab järjepanu e-hääletamise protseduure, ei vasta tõele. Logid, millele vaatleja viitab, sisaldavad hääletanute isikuandmeid ja seaduse järgi ei tohi selliseid andmeid kõrvaliste isikutega jagada. See

on kujuteldamatu, et valimisteenistus jagab vaatlejatega, kelleks võib olla iga inimene tänavalt, sellist infot, mis võimaldab tuvastada, millal konkreetne inimene on valimas käinud. See läheb otseselt vastuollu valimiste salajasuse põhimõttega ja on seaduse vastane.

Vabariigi valimiskomisjoni koosoleku päevakorra punkt, mida vaatlejal ei võimaldatud kuulata, käsitles e-hääletamise riskikäsitlusplaani ehk teavet, mille asutusesiseseks kasutamiseks seadus kohustab ning mida ei saa seetõttu arutada asutusevälistе isikute juuresolekul. Avaliku teabe seaduse § 35 lg 1 p 9 kohustab tunnistama asutusesiseseks kasutamiseks teabe turvasüsteemide, turvaorganisatsiooni või turvameetmete kirjelduse kohta. Samamoodi on piiratud kõrvalistele isikutele näiteks pabersedelite turvaelementide arutelu.

Vaatleja nimetab turvalisust etteheitvalt innovatiivseks valimispõhimõtteks, mida põhiseadus isegi ei nimeta. Aga kuidas saab ilma turvalisuseta üldse olla vabasid ja salajasi valimisi? Valijate andmed, hääletamise fakt, hääletaja valik ja turvasüsteemide kirjeldused ongi seaduse järgi kaitstavad selleks, et igal hääleõiguslikul kodanikul oleks kindlus, et ta saab valimistel osaleda ilma, et teda tema eelistuse tõttu taga kiusama hakataks.

Käib pidev ajakohastamine

Sama arusaamatuks jääb seisukoht, et e-hääletus on eskperimentaalne, sest süsteemi ajakohastatakse enne iga valimist. Eesti elektroonilise hääletamise süsteemi, protseduure ja seadusandlust on 20 kasutusaasta jooksul pidevalt arendatud ja ajakohastatud, et tagada valimiste turvalisus ja läbipaistvus. See ei ole märk mitte süsteemi eksperimentaalsusest, vaid süsteemi ajakohasena hoidmisest.

Seadus paneb riigi valimisteenistusele kohustuse kasutada ajakohast elektroonilise hääletamise süsteemi ning tagada selle turvalisus ja usaldusväärsus. Seetõttu on süsteemi pidev uuendamine ja arendamine mitte üksnes parim praktika, vaid ka seadusest tulenev nõue.

Ka on vabade ja demokraatlike valimiste loomulikuks osaks välisvaatlejate, sh OSCE demokraatlike institutsioonide ja inimõiguste büroo missioonid. ODIHR on vaadelnud ja analüüsinud Eestis e-hääletust regulaarselt ning on teinud soovitusi selle kohta, mida saaks paremini teha, et veelgi suurendada ja säilitada usaldust e-hääletamise vastu.

Näiteks üheks OSCE soovitusest sündinud uuendus on 2015. aastal loodud kontrollrakendus, mis võimaldab hääletanul oma silmaga veenduda, et tema e-hääl jõudis korrektselt valimiskasti kohale. Kummalisel kombel on skeptikud ja vaatlejad seda viimastel nädalatel hakanud esitlema, kui „võimalust vaadata valijate hääli“, mida see kindlasti ei ole. Ainult valija ise saab vaadata, kas tema hääl jõudis kohale. Tegemist on hädavajaliku kontrollmehhanismiga valijale kindluse andmiseks ja e-hääletuse läbipaistvuse tagamiseks.

Kuidas see lugu Sind end tundma pani?

Rõõmsana