

*Vabariigi valimiskomisjonile*

Märt Pöder  
sündinud 11.09.1979  
elukohaga Jakobi 13-2, Tartu 51006  
kontaktitav gafgaf@infoaed.ee

## **VALIMISKAEBUS EUROOPA PARLAMENDI VALIMISTEL 2024**

Sain vaatejana 9.06 ja 10.06 protseduuride käigus toimunud küsimuste-vastuste voorus teada, et valimistel käitatava häältekogumise süsteemi päritolu on sama ebaselge ja dokumenteerimata nagu 20.05.2024 võtmeloomeks kasutatud süsteemi oma, mis oli dokumenteerimata juba 2023. aasta Riigikogu valimistel ning leidis käsitlemist 17.02.2023 valimiskaebuses ja lõpuks Riigikohtu asjas 5-23-40, mille punktis 15 valimiskomisjon kinnitab:

“Operatsioonisüsteemi ja tarkvara räside protokollimine ei ole dokumentatsiooni kohaselt nõutav.”

RKVS §48<sup>7</sup> “Valimiste turvalisuse tagamine” lg 1-2 järgi vastab e-hääletuse süsteem küberturvalisuse seaduse nõuetele ja valimisteenistus võtab vastu infoturbe poliitika, mida RVT 3.04.2024 korraldusega nr 5 on ka teinud.

Selle 7.8 ütleb, et “EHS arvutitele baassüsteemide paigaldamisel, operatsioonisüsteemide turvapaikade laadimisel ja muude teenindusprotseduuride käigus tagatakse, et teave pärineb usaldusväärsest ja kontrollitud allikast”, lisaks kinnitab 7.6, et “RVT säilitab tõendid EHS rakenduste lähtekoodi tervikluse kohta”.

Sellest tuleb järeldada, et operatsioonisüsteemi ja tarkvara päritolu peab olema dokumenteeritud, kuid RVT e-hääletuse eksperdi Indrek Leesi sõnul pole häältekogumise süsteemi päritolu ei dokumenteeritud ega isegi teada selle loomise täpne aeg või missugusest lähtekoodi versioonist see lähtub, mh polnud e-hääletuse süsteemi lähtekoodi avaldatud enne kui 30.05.2024, mistõttu pole selge, kas see oli häältekogumise või võtmeloomesüsteemi ettevalmistamise ajaks üldse saanud lõpliku kuju.

Imselt on ekslik ka valimiskomisjoni 2023. aasta hinnang, et opsüsteemi ja tarkvara räside protokollimine pole dokumentatsiooni kohaselt nõutav, sest see või mõni muu meede peab aitama ka valimiste korraldajal enesel veenduda, et bassüsteem ja

e-hääletuseks kasutatav tarkvara pärineb usaldusväärsetest allikatest – selline veendumus ei saa tuleneda lihtsalt igapäevastest dokumenteerimata tööprotsessidest, vaid see peab olema tõendatult tagatud.

Olen kirjeldanud probleeme 2023. aasta võtmelooma arvuti dokumenteerimata päritoluga blogipostituses ja kuigi pärast seda on infoturbe poliitikat uuendatud ja enam ei kehti blogipostituses osutatud ISKE, pole ilmselt tegelike praktikate vastuolu infoturbe nõuetega vähenenud:

- <https://gafgaf.infoaed.ee/posts/esoteeriline-turvamudel/>

Kuigi ma ise vaatlejana 2024. aasta võtmelooma protseduuride juures ei viibinud, siis tunnistajate hinnangul oli süsteemi päritolu endiselt dokumenteerimata, sj on valimisteenistus 2015. aastast alates järk-järgult loobunud arvutisüsteemide seadistamise vaatlemisest ning auditeerimisest sellele võrdväärseid infoturbe meetmeid asemele pakkumata.

Infoturbe poliitika 5.3-5.6 järgi on e-hääletuse süsteem määratletud kui “väga suure kaitsetarbega infosüsteem”, sj häältekogumise süsteem “luuakse igaks hääletamisperioodiks lähtudes asjakohastest E-ITS kõrge turvaastme meetmetest ja riskianalüüsisist tulenenud individuaalsetest turvameetmetest” ning “RVT koostab igaks hääletamisperioodiks EHS testimise ajakava ja ulatuse ning testimise tulemused ja avalikustab tulemuste raporti”, sj “RVT korraldab EHS auditeerimise, mille käigus infosüsteemide audiitor kontrollib EHS testimise, EHS terviklikkuse ja RVT toimingute vastavust seadustele, Vabariigi Valimiskomisjoni otsustele ning elektroonilise hääletamise dokumentatsioonile”.

RVT dokumendiregistris puudub Euroopa Parlamendi valimisteks 2024 selline testimise ajakava ja ulatuse määratlus ning avalikustatud testimise raport.

Arvestades, et “valimiste turvalisuse tagamine” on VVK 9.02.2024 otsuses nr 95 toodud eraldi eesmärgina ja RKVS §48<sup>2</sup> nõuab, et kasutataks “ajakohast elektroonilise hääletamise süsteemi”, pole see valijatele tegelikult tagatud, kui baassüsteemide turvanõudeid praktikas ei järgita, kuid vaatleja tegevuse muudab see samuti tähendusetuks, sest kui süsteemid kompromiteerimine on toimunud nende auditeerimata, vaatlemata ja dokumenteerimata ettevalmistamise raames, siis äärmiselt alamääratletud ja juhuslikult korraldatud vaatlemise abil pole võimalik vaatlejatel veenduda süsteemide korrektsetes toimimises.

Seega on siin riivatud minu õigusi vaatlejana teha oma tööd

sisuliselt ja valijana riivatud õigust ajakohasele ja tuvalisele e-hääletuse süsteemile.

Sisuliselt ekslikud on seejuures ka VVK osutused Riigikohtu asjas 5-23-40:

“Hääletamistulemusi pahavaraga kompromiteerida ei saa, sest hääletamistulemuste kindlakstegemisel väljastatud lugemistõendi abil selguks kompromiteerimine kohe. Lugemistõendi alusel on matemaatiliselt võimalik tõestada, et hääletamistulemust ei ole võltsitud ega kompromiteeritud.”

Miksimis- ja lugemistõend on väga spetsiifilised tõendid, mis katavad süsteemis toimuvat ainult viimastes faasides ega taga üldiselt e-hääletuse sisendi ja väljundi vastavust, vaid peamiselt teostatud krüptograafiliste protseduuride endi sisendi ja väljundi korrektsust.

**Taotlen kaebusega, et Euroopa Parlamendi valimistel kasutusel olnud e-hääletuse süsteem tunnistataks vastuolus olevaks või puudulikult vastavaks e-hääletuse infoturbe nõuetele, mida väljendab RKVS §48<sup>7</sup> ja mida peab tagama RVT 3.04.2024 korraldus nr 5.**

Raske on üheselt ütelda, mis on vaidlustatav toiming, kuid see paistab olevat e-hääletuse süsteemi ettevalmistamine, mille toimumise aeg ei olnud ega ole ka praegu mulle teada ja mille toimumisest ja toimumise aja määratlematusest sain teada 9.06 ja 10.06 protseduuride käigus.

Kui kaebetähtaeg oletatava toimingu suhtes on ületatud, siis palun ajakavade ja ulatuste määratlematuse ning hilinevad dokumentatsiooni tõttu see ennistada, sest sain puudusest teada häälte kokkulugemise vaatlusprotseduuride käigus.