*Riigikohtu põhiseaduslikkuse järelevalve kolleegiumile*

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

# VVK 23.02.2023 OTSUSE nr 54 VAIDLUSTAMINE

Vaidlustan VVK 23. veebruaril 2023 tehtud otsuse sellega ette nähtud protseduuri käigus ilmnenud asjaolude tõttu, millest lähtuvalt ei saa pidada asjakohaseks VVK hinnanguid võtmegeneerimise, selle ettevalmistamise, aga ka samas arvutisüsteemis läbiviidud häältelugemise protseduuride korrektsuse või laiemalt vastavuse osas demokraatlike valimiste põhimõtetele.

Kettatõmmise vaatlemise protseduuri käigus 28. novembril selgus, et tegelikkusele ei vasta VVK otsuses kirjeldatu:

> "Võtmete loomisel kasutatud kõvakettale on installeeritud Microsofti repositooriumist alla laaditud Windows 10 operatsioonisüsteem. Seejärel käivitati arvuti Riigikogu Kantselei arvutivõrgus ning installeeriti saada olevad uuendused, kaasa arvatud aktiivse viirusetõrje tarkvara Windows Defender. Arvuti valmistas ette e-hääletamise süsteemi operaator, Riigikogu Kantselei töötaja."

Protseduurile eelnenud selgituses andis RVT esindaja sellega üldiselt kooskõlas oleva ülevaate võtmete loomisel kasutatud kõvaketta kohta, täpsustades, et tegu on MSDN portaalist alla laaditud autentse kettatõmmisega, mille räsisid allalaadimisel vastavalt parimatele praktikatele kontrolliti, ning mis seejärel paigaldati füüsilisele kettale.

Ketta arvuti külge ühendamisel ja käivitamisel ilmnes aga (vt lisatud `kettavaatlus_2023.jpg`), et kettale oli paigaldatud ka kasutajatarkvara, nende hulgas näiteks Digidoc klient ja Notepad++ rakendus. Ketta allalaadimise kohta ja räside kontrollimise kohta polnud protokolli, lisaks sellele, et RVT esindaja ei mäletanud, et ta oli kettale paigaldanud ka Digidoc kliendi ja Notepad++ rakendused, polnud protokolle ka kasutajatarkvara allalaadimise, räside või nende kontrollimise kohta.

Seetõttu tuleb tõdeda, et ilma adekvaatse dokumentatsiooni, protokollimise, veel vähem auditeerimise või vaatlemiseta lihtsalt ilmus kuskilt elektroonilise hääletuse turvalisuse aspektist kõige olulisem arvutisüsteem, milles a) viidi läbi valimiste peamiseks krüptograafiliseks turvagarantiiks oleva RTV/VVK avaliku ja privaatvõtme genereerimine ja b) viidi läbi pärast töötlemist valimisurni jäänud ja segatud krüptogrammide lahtikrüptimine ja elektroonilistel valimissedelitel tuvastavate häälte kokkulugemine.

Arvestades, et ketas loodi e-hääletamise süsteemi operaatori rollis olnud RVT töötaja poolt igapäevaste tööülesannete käigus, siis kaasnevad sellega laialdased võimalused

süsteemi kompromiteerimiseks viisil, mille tulemuseks saab olla valimistulemuse manipuleerimine ilma, et see oleks protseduuride käigus või tagantjärele tuvastatav audiitori või vaatlejate poolt. Kompromiteerimiseks piisab, kui valimistulemuse manipuleerimise sooviga siseründaja või RVT igapäevaselt kasutatavatele arvutisüsteemidele ja arvutivõrkudele või ka füüsilisele töökohale ligipääsu omav osapool saavutab, et kettale paigaldatakse muu tarkvara seas ka tema poolt modifitseeritud tarkvara, mis sekkub võtmegenereerimisse ja/või häälte kokkulugemisse.

Kuna tõmmiste ja paigaldatud tarkvara räsisid ei registreeritud ega protokollitud, kuigi see võiks olla selliste protseduuride puhul elementaarne, siis ei saa ka RVT ega VVK üldsusele tõendatavalt, st mistahes arvestatava tõsikindlusega väita, et võtmegenereerimise ja häältelugemise arvutis polnud valimistulemust modifitseeriv pahavara.

Pahavara jaoks, mis on paigaldatud valimiste turvalisuse vaatenurgast kriitiliste protseduuride nagu võtmegenereerimise ja häältelugemise eest vastutavasse arvutisüstemi, avanevad manipulatsiooniks ja rünneteks laialdased võimalused elektroonilise hääletuse eri etappides – alates hajutatud rünnetest valimissaladuse vastu kuni rünneteni, mis modifitseerivad e-hääletuse eri etappides häälteurni või valimistulemust.

## E-hääletuse vaatlemise põhimõtted

Iseenesest on korrektne väide, et kaebuse aluseks olnud lause e-hääletuse käsiraamatus ei väljenda selgelt, millisel viisil võimaldatakse tuvastada pahavara puudumist võtmegenereerimise süsteemis:

> "Süsteemi võtmepaari genereerimine on auditeeritav protseduur. Süsteemi võtmepaar genereeritakse eraldi võrgust lahti ühendatud arvutis, millel on eemaldatud sisemised salvestusvahendid (v.a. andmete välisele andmekandjale kirjutamist võimaldav seade) ning mis alglaaditakse väliselt kõvakettalt. Sellisel moel on võimalik audiitoritel ja vaatlejatel veenduda, et süsteemis ei sisaldu pahavara, mis häälte avamise võtit salvestab või kasutab."

Pelgalt võtmete genereerimine võrgust lahti ühendatud arvutis seda kindlasti ei garanteeri, mida näitlikustab ka 28. novembril läbitud protseduur, mille käigus ilmnes, et tsitaadis osutatud välise kõvaketta sisu oli n-ö ametlike protseduuride aspektist isetekkeline. Võib arvata, et see lause on käsiraamatus ajast, mil ka kettatõmmiste loomine ja sinna tarkvara paigaldamine oli veel vaadeldav protseduur ning selle käigus sai ilmselt vaadelda neid arvutsüsteemide ettevalmistamisi, mida praegu RVT teeb oma igapäevatoimetuste käigus – arvutisüsteemide seadistamise protseduuride vaatlemisest paistab pärast 2015. aastat olevat järk-järgult loobutud.

Seejuures ilmneb, et RVT ei oma pädevust nende protseduuride korrektseks läbiviimiseks, sest vaatlejana võideldes endale tehniliste ja juriidiliste vahenditega kätte ligipääsu eri e-hääletuse läbiviimise eteppidele ilmneb, et avalikkusele antud selgitused ei vasta olulise tähendusega detailides sugugi mitte alati tõele ja lahknevustele

seadusega ettenähtud protseduuridest pole võimalik kaebemenetluse raames saada õiguslikku selgitust.

Seejuures on RVT eksitanud ka Riigikohust, nt kaasuse 5-23-11 lahendi punktides 31-34 polnud kolleegium informeeritud asjaolust, et elektroonilise valimissedeli EHAK-koodi väli sisaldas kõikide ametiku valijarakendusega antud häälte puhul erinevalt VVK 10.10.2022 otsusega nr 47 ettenähtud vormist märgijada `0000`. Kaebused selliste seadustest lahknevuste kohta, sh kehtetute digiallkirjade kohta e-häälte konteineritel jäid Riigikohtus arutamata ning VVK sisuliselt otsustas oma äranägemise järgi, missugust seadust või otsust tuleb e-hääletuse läbiviimisel järgida ja missugust võib eirata.

Seejuures VVK 30.03.2023 koosoleku nr 64 protokollis on VVK viitega Riigikohtu kaasuse 5-21-31 lahendi punktile 21 püüdnud õigustada valimistulemuse väljakuulutamist hoolimata kaebusest, mis puudutas kõigi loetud e-häälte hälbimist seadusest ja oleks võinud mõjutada valimistulemust. Kaasuse punktis 21 on seevastu selgelt välja toodud, et valimistulemuse väljakuulutamine hoolimata kaebuste jätkuvast olemasolust võib olla õigustatud juhul, kui see ei või mõjutada valimistulemust:

> "Selle sätte eesmärgiks on vältida olukorda, kus pärast valimistulemuste väljakuulutamist ja uute volikogude töö alustamist selgub valimiskaebemenetluses mõni selline õigusrikkumine, mis võis mõjutada hääletamis- ja valimistulemust."

Riigikohus ei pidanud põhjendatuks kaasuses 5-23-26 kaebetähtaja ennistamist, et seda küsimust arutada. Selle tulemusel loeti kokku e-hääled, mis ei vastanud vähemalt kahes punktis seaduse nõuetele ja arvutuste kohaselt on seetõttu Riigikogu mandaatidest 22 omandatud kehtetute sedelite lugemise teel.

Tundub, et olemasolev kaebemenetlus ja vaatlemise protseduurid ei võimalda selliste probleemide lahendamist ja seetõttu peab valijaskond lihtsalt leppima sellega, et valimised viidi läbi seadust eirates.

**Kuna selliste probleemide tuumaks tundub olevat, et vaatlemise tähendus e-hääletuse jaoks on läbimõtlemata ning puuduvad garantiid, et tagada e-hääletuse seadust järgiv läbiviimine, siis taotlen Riigikohtult e-hääletuse vaadeldavuse põhimõtete läbiarutamist ja seadusandjale vastava suunise andmist.**