Riigikohtu põhiseaduslikkuse järelevalve kolleegiumile

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

VALIMISKOMISJONI 13.06.2024 OTSUSE nr 5 VAIDLUSTAMINE

RESOLUTSIOON:

1. **Tühistada Vabariigi Valimiskomisjoni 13.06.2024 otsus nr 5.**

2. **Rahuldada kaebus ning tunnistada seadusevastaseks valimiste korraldaja toiming, millega säilitatakse kaebaja 03.06.2024 antud e-häält isikustatud elektroonilise häälena elektroonilise hääletamise süsteemis pärast elektroonilise hääle vastuvõtmist elektroonilise hääletamise süsteemi poolt.**

Menetluse käik

1) Kaebaja esitas 06.06.2024 kaebuse Riigi Valimisteenistuse (**RVT**) toimingu peale seoses sellega, et RVT töötleb kaebaja elektroonilist häält (**e-häält**) anonüümimata kujul. Kaebaja e-hääle talletamine viisil, mis võimaldab seostada kaebaja isikut ning tema poliitilist eelistust, ei ole õiguspärane.

2) Vabariigi Valimiskomisjon (**VVK**) tegi 13.06.2024 otsuse nr 5, millega jättis kaebuse rahuldamata. VVK leidis, et esineb õiguslik alus, mis võimaldab talletada valijate e-häält isikustatud kujul.

3) Kaebaja vaidlustab siinsega VVK 13.06.2024 otsuse nr 5. Kaebaja palub, et Riigikohus tühistaks vaidlustatud otsuse ning teeks asjas uue otsuse, millega tuvastaks toimingu seadusvastasuse. Kaebaja tugineb kõigile oma 06.06.2024 kaebuses toodud alustele ning täpsustab neid siinses kaebuses alljärgnevalt.

Faktiline alus ja vaidluse ulatus

4) Kaebaja andis Euroopa Parlamendi valimistel 03.06.2024 e-hääle. RVT säilitab kaebaja e-häält anonüümimata kujul ehk viisil, mis võimaldab antud häält kaebajaga seostada. RKVS § 48^6 lg 5 kohaselt säilitab RVT mh valija nime, isikukoodi, IP-aadressi, hääletamise kuupäeva. kellaaja, valimisringkonna ja asukohariigi. RKVS § 48^6 lg 6 kohaselt anonüümitakse e-hääletuse toimingute logid alles pärast elektroonilise hääletamise lõppemist. RKVS § 48^6 lg 7 kohaselt säilitatakse anonüümimata logisid

vähemalt kuu aega pärast valimiste lõppemist.

5) Asjas ei ole vaidlust faktilise asjaolu üle, et valimiste korraldaja säilitab kaebaja e-häält isikustatud kujul vähemalt e-hääletamise lõppemiseni ning sealt edasi vähemalt kuu aega pärast valimiste lõppemist, mil valimiste korraldajad selle koos toimingute käigus tehtud koopiatega RKVS §77[1] lg 2 kohaselt osaliselt hävitavad. Fakt, et valimiste korraldaja säilitab kaebaja e-häält niivõrd pika perioodi jooksul isikustatud kujul, on kaebuse aluseks.

6) Vaidlus on selle üle, kas eeltoodud tegevus on õiguslikult lubatav. Kaebaja on seisukohal, et tema poliitilise eelistuse isikustatud kujul säilitamine ei ole lubatav. VVK leidis, et see on lubatav. Kaebaja ei nõustu VVK otsuses tooduga ning põhjendab seda alljärgnevalt.

E-hääle säilitamine isikustatud kujul on vastuolus IKÜM-iga

7) Isikuandmete kaitse üldmääruse EL 2016/679 (IKÜM) § 4 p 1 kohaselt on isikuandmed igasugune teave tuvastatud või tuvastatava füüsilise isiku kohta. IKÜM artikkel 4 p 2 kohaselt on andmete säilitamine isikuandmete töötlemise toiming. Valimiste läbiviija on IKÜM artikkel 4 p 7 mõttes käsitatav vastutava töötlejana. IKÜM artikkel 9 lõike 1 kohaselt on isiku poliitiline veendumus isikuandmete eriliik, mille töötlemine on sama lõike kohaselt keelatud. E-hääles sisalduv valija tahe on käsitatav poliitilise veendumusena ja selle sidumine valija isikuga kvalifitseerib selle isikuandmete eriliigiks.

8) Riigikohus on selgitanud, et eraelu puutumatuse riivena käsitatakse muu hulgas isikuandmete kogumist, säilitamist, kasutamist ja avalikustamist (RKHKo 3-3-1-3-12 p 19). Riigikohus on leidnud, et riive on põhiõiguse kaitseala või sinna kuuluva õigusliku positsiooni igasugune ebasoodus mõjutamine (RKPJKo 3-4-1-1-02 p 12; RKÜKo 5-20-3/43, p 66). Kaebaja leiab, et isikustatud e-hääle edasine säilitamine pärast selle vastuvõtmist on õigusvastane andmetöötlustoiming. Andmete töötlemisahelas toimuv igasugune töötlustoiming nõuab eraldiseisvat õiguslikku alust. Valimiste läbiviijal puudub kehtivast õigusest tulenev alus andmete eriliikide töötlemiseks. Isikustatud e-hääle säilitamine pärast selle vastuvõtmist e-hääletamise süsteemi poolt on andmetöötlustoiminguna keelatud.

9) VVK asus vaidlustatud otsuses seisukohale, et „Isikustatud e-häälte töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks ja vastab seetõttu IKÜM art 6 lg 1 punktile e“. VVK on jätnud arvestamata, et IKÜM artikkel 6 on üldnorm, mille suhtes kehtib erinormina artikkel 9. Artiklist 6 tulenevaid õiguslikke aluseid ei ole võimalik kohaldada artikkel 9 lg-s 1 toodud andmete eriliikide suhtes, sest vastasel juhul muutuks erinorm sisutühjaks. Lähtuda tuleb põhimõttest *lex specialis derogat legi generali*. Kaebaja e-hääle isikustatud kujul töötlemise aluseks ei saa seega olla IKÜM artikkel 6 lg 1 punkt e.

10) VVK asus täiendavalt järgmisele seisukohale:

„IKÜM art 9 lg 1 ei keela siiski elektroonilisi hääli koos isikuandmetega talletada. See säte kajastab üldpõhimõtet, millest on lubatud erandid. IKÜM art 9 lg 2 punkt g näeb ette, et lõiget 1 ei kohaldata, kui töötlemine on vajalik olulise avaliku huviga seotud põhjustel

liidu või liikmesriigi õiguse alusel ning on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ja tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks. Valimiseelistust sisaldavate isikuandmete töötlemine on vajalik seadusega ette nähtud elektroonilise hääletamise läbiviimiseks Euroopa Parlamendi valimistel. Toimingu seadusevastasust ei saa järeldada ainult sellest, et teistsuguste hääletamisviiside korral oleks võimalik hoiduda olukorrast, kus hääli kogutakse isikustatud kujul.“

11) Kaebaja nõustub, et IKÜM artikkel 9 lg 2 punkt g võiks teoreetiliselt anda aluse tema e-hääle isikustatud kujul töötlemiseks. Selleks peaksid aga olema täidetud artikkel 9 lg 2 punktis g toodud eeldused. Neid eelduseid ei ole täidetud.

12) IKÜM art 9 lg 2 punkt g eriliiki isikuandmeid juhul, kui:

- töötlemine on vajalik olulise avaliku huviga seotud põhjustel
- liidu või liikmesriigi õiguse alusel ning
- on proportsionaalne saavutatava eesmärgiga,
- austab isikuandmete kaitse õiguse olemust ja
- tagatud on sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks

13) Selleks, et kaebaja e-hääle töötlemisel saaks tugineda IKÜM art 9 lg 2 punktile g, peavad kõik eeltoodud nõuded täidetud olema. Praegusel juhul ei esine sellist olukorda.

14) Puudub õiguslik alus. IKÜM art 9 lg 2 punkti g kohaselt on lubatud eriliiki isikuandmeid töödelda üksnes juhul, kui selleks esineb eraldiseisev alus liidu või liikmesriigi õiguses. See tähendab, et seaduses peab olema sätestatud eraldiseisev õiguslik alus, mis võimaldaks valimiste läbiviijal säilitada kaebaja häält isikustatud kujul.

15) Valimiste läbiviija säilitab kaebaja e-häält kuni valimiste lõppemiseni ning sealt edasi veel vähemalt kuu aega isikustatud kujul ehk viisil, kus kaebaja isik ja tema antud hääl on seostatavad. EL-i ega Eesti õiguses ei ole sätet, mis võimaldaks neid andmeid taoliselt säilitada. RKVS § 48^6 lg-s 5 on toodud andmed, mida logitakse. Selles sättes ei ole toodud, et valimiste läbiviija võiks salvestada isikustatud kujul andmeid selle kohta, kelle poolt kaebaja hääletas. See on välja toodud ka vaidlustatud otsuses (punkt 18: „Vabariigi Valimiskomisjon märgib, et logides ei sisaldu ka valija valimiseelistus“). VVK ei ole samas välja toonud, millisest sättest tuleneb õiguslik alus valimiseelistuse säilitamiseks isikustatud kujul.

16) Kaebaja rõhutab, et IKÜM põhjenduspunktis 41 on toodud, et kui IKÜM-s osutatakse õiguslikule alusele või seadusandlikule meetmele peab liikmesriigi õiguslik alus või seadusandlik meede, mille alusel andmetöötlus toimub, olema selge ja täpne. Sellest tulenevalt ei ole vajalikku õiguslik alust võimalik ka kaudselt tuletada mõnest muust sättest. Õiguslik alus valija e-hääle, sh poliitilise eelistuse, isikustatud kujul säilitamiseks peaks olema otsesõnu seaduses sätestatud. Seaduses ei ole taolist alust toodud. Seaduses ei ole e-häält isegi üheselt defineeritud, mistõttu ei ole õiguslikku alust selliste eriliiki isikuandmete säilitamiseks.

17) Puudub proportsionaalsuse hinnang. VVK on väitnud, et „Toimingu seadusevastasust ei saa järeldada ainult sellest, et teistsuguste hääletamisviiside korral oleks võimalik hoiduda olukorrast, kus hääli kogutakse isikustatud kujul“. VVK väide on vastuolus IKÜM-iga – IKÜM art 9 lg 2 punktis g toodud proportsionaalsuse nõue tähendabki täpselt seda, et juhul, kui hääletamist on võimalik läbi viia nii, et hääli ei koguta isikustatud kujul, siis tuleks seda üldjuhul eelistada. Erandi saab teha üksnes juhul, kui privaatsuse riive on vajalik, et suuremal määral edendada mõnda muud õiguspärast huvi.

18) Antud juhul esineb eelkõige kaks võimalikku alternatiivi, mis võimaldaks hääletada niimoodi, et kaebaja e-häält ei ole vaja isikustatud kujul säilitada:

* E-hääletamine niimoodi, et valija anonüümitakse juba enne või vahetult pärast hääle andmist;

* Hääletamine üksnes pabersedelitega, kus valija anonüümib oma hääle sedeli laskmisega valimiskasti.

19) Kaebajale ei ole teada, et oleks läbi viidud proportsionaalsuskontroll, mis oleks jõudnud järeldusele, et e-hääletamine praegusel viisil (e-häälte säilitamine isikustatud kujul) tagab põhiõigusi paremini kui mõni eeltoodud alternatiividest. Näiteks Šveitsis ei ole e-häält võimalik uue e-häälega ega paberhäälega n-ö üle hääletada.[1]

20) OSCE/ODIHR viimase kahe Eesti vaatlusmissiooni, st 2019. ja 2023. aasta e-hääletuse ekspert Carsten Schürmann on TA konverentsil toonud välja järgmist: „Taani ei kasuta ühtegi elektroonilise hääletuse viisi, sest nad leiavad, et hääletamise salajasust pole võimalik tagada määral, mida nõuab konstitutsioon ja punkt -- kogu lugu. Ilmselgelt Eestis on Interneti-hääletus ja selgelt teistusugune tõlgendus, mida hääletamise salajasus tegelikult tähendab“[2]

21) Puuduvad vajalikud kaitsemeetmed. VVK samastab ekslikult salajasust ja valimisvabadust (salajasuse riivet ja valimissundi), mida tuleb käsitleda ja tagada eraldi, st valimissaladuse riive pole ainult vahetu individuaalse valimissunni vahend, vaid ka valijate tahte kaudse mõjutamise vahend (valija ei julge oma soovitud kandidaati valida, kui on oht, et hääle salajasus pole piisavalt kaitstud RVT või kellegi teise eest, sj ka siis, kui hääl saab soovimatule osapoolele teatavaks pärast hääletusperioodi lõppu ja vahetu valimissund tahteavalduse mõjutamisena valimistel pole enam võimalik);

22) VVK eksitab süsteemi infotehnoloogiliste omaduste osas (“ajakohane hääle salastamise krüptograafiline lahendus, mis on süsteemi toimimise eelduseks”) ja esitab olemasolevat süsteemi kui hääle salajasuse jt põhiseaduslike põhimõtete tagamiseks ainuõiget või

1 Šveitsi e-hääletamise kohta (https://www.ch.ch/en/votes-and-elections/e-voting/#how-does-e-voting-work):

“Sinu hääl krüpteeritakse. Valimiste läbiviija ei saa tuvastada, kuidas sa hääletasid. Kui sa oled hääle elektrooniliselt andnud, siis salvestatakse sinu valijakaart ning muul viisil valimine on blokeeritud (posti teel või valimisjaoskonnas)”.

originaal: “Your vote will encrypted. The authorities cannot trace how you voted. Once you have cast your vote electronically, your voter identification card will be recorded and blocked for other forms of voting (by post or at a polling station).”

2 Eesti Teaduste Akadeemia küberturvalisuse komisjoni konverents "Usaldusest ja usaldatavusest" 17. oktoober 2023 https://youtu.be/7RtVVAv4qFE?t=1871)

paratamatult piisavat, kuigi on võimalikud süsteemid, millel puuduvad olemasoleva süsteemi ebasoovitavad omadused (varases faasis anonüümivad süsteemid) – arusaadavalt on kaebuse sisu, et olemasolev süsteem ei taga salajasust piisavalt, et olla kooskõlas IKÜM ja PS, aga ka CM/Rec (2017)5 ja RKVS §48[6] nõuetega.

23) Puudub IKÜM nõutud mõjuhinnang ja PS salajasuse nõude põhiseaduspära ajakohane ning terviklik tõlgendus, mis põhineb 2005. aasta lahendi väga esialgsetel väidetel ega ole süsteemi tegelikus teostuses kooskõlas RKVS §48[6] nõuetega (sj VVK ei paista oma seisukoha punktis 15 isegi teadlik RVT praktikast RKVS §23 lg 1 ja eeldatavasti EPVS §22 lg 1 alusel anda valijale tõend hääletamisviisi kohta).

E-häälte isikustatud kujul töötlemine rikub valimiste salajasust

24) RVT on vaidlustatud otsuses väitnud, et „valimiste korraldajal (riigi valimisteenistus) **pole võimalik** tuvastada e-hääletanute valikut, kuna hääletamissedelid on salastatud kujul ning nende avamine ilma juurdepääsuta privaatvõtmele ei ole võimalik. Privaatvõti on jaotatud Vabariigi Valimiskomisjoni ja riigi valimisteenistuse teenistujate vahel (RKVS § 48[3] lg 3).”

25) E-häälte isikutatud säilitamine ja anonüümimata dekrüptimine on hääletuse süsteemi arhitektuuris ettenähtud võimalus, mille realiseerumist püütakse vähendada e-hääletuse organisatsiooni ja protseduuridega. See on süsteemi tehniline aluspõhimõte, et salastatud hääled dekrüptitakse privaatvõtmega, st dekrüptimine privaatvõtmega on olemasoleva e-hääletuse vältimatu osa. Sellest tulenevalt on tagatised hääle salajasuse kaitseks nõrgad, sest on organisatsioonilised ega tulene süsteemi arhitektuurist (organisatsioonilised nii vastutavate isikute ja nende rollide mõttes nagu VVK ja RVT privaatvõtme osakuid omavad inimesed, kelle koostöös on võimalik hääle salajasust murda, aga ka tehnilised, st privaatvõtme loomisel ja säilitamisel kasutatavate arvutisüsteemide omadustest ja ettevalmistamise viisist tulenevad).

26) Väide, et valimiste läbiviijal „pole võimalik“ tuvastada e-hääletanute valikut, põhineb üksnes asjaolul, et valimiste läbiviija ei tohiks seda teha ning see on teatud määral protseduuridega tagatud, et seda ei juhtuks. Väide, et seda ei ole üldse võimalik teha, ei ole aga tõene.

27) **Valimiste läbiviijal on faktiliselt võimalik tuvastada e-hääletanute valikut.** See on krüptograafiline paratamatus – e-hääled säilitatakse krüpteerituna isikustatud kujul ning valimiste läbiviijal on olemas privaatvõti, millega on võimalik e-hääli dekrüpteerida. RVT ise loob vastava võtme, mistõttu on RVT võimeline ise krüpteeringut avama – eriti pidades silmas võtmeloomise süsteemi turvanõuete puudulikku täitmist, mida on kaebaja dokumenteerinud mh Riigikohtu menetluses (RKPJKo 5-23-40 p 9).

28) VVK on vaidlustatud otsuses toonud, et “RKVS § 48[6] lõige 3 sätestab, et enne elektrooniliste häälte lugemist eraldatakse isikuandmed elektroonilisest häälest selliselt, et **ei ole võimalik** tuvastada valija tahteavaldust. Kuni selle toiminguni on e-hääletamise lugemise protsessis hääled isikustatud, kuid krüpteeritud.“

29) See pole praktikas tõene, sest kontrollrakendus dekrüpteerib hääle valijale QR-koodis

sisalduva juhuslikkuse abil ning isikustatult. QR-koodile ligipääsev isik, mis võib olla ka RVT, saab teha sedasama – seega ei ole tagatud, et isikustatud e-hääled ei saa avalikuks. RVT levitab ja vahendab nii valimisrakendust kui kontrollrakendust, millel on mõlemal ligipääs nii QR-koodile kui valija isikustatud tahteavaldusele viisil, mis võimaldab selle dekrüpteerida.

30) VVK on vaidlustatud otsuses väitnud, et "Tegemist on vajalike toimingutega topelthääletamise välistamiseks, samuti hääletamise salajasuse ja valimiste vabaduse tagamiseks."

31) Tegu on vajalike toimingutega üksnes lähtuvalt eeldusest, et RVT-l ja audiitoril ei ole valija tahteavalduse kindlakstegemiseks alternatiivset viisi, mis ei ohusta hääle salajasuse põhimõtet nii tugevalt nagu seda teeb oma tehnilisest arhitektuurist lähtuvalt praegune e-hääletus. Seejuures ei taga kasutatav arhitektuur mitte hääletamise salajasust, sest võimaldab seda otseselt riivata nii kontrollrakendusega (vt RVT seisukohas välja toodud „erijuht", lisaks kontrollrakenduse tehnilised edasiarendused, mis tühistavad 15 min piiri ja võimaldavad dekrüpteerida ja tõendada e-häält digiallkirja tõsikindlusega) kui RVT ja VVK poolt privaatvõtme kaudu, vaid tagab ainuüksi valimiste vabadust ning sedagi postuleerides küsitava eelduse, et seda tuleb tagada oma tehniliselt arhitektuurilt salajasust ohustava hääle muutmisega (sisuliselt uue hääle edastamisega, millest peaks lugemisele minema "valija viimasena antud hääl").

32) VVK on vaidlustatud otsuses väitnud, et "Seejärel hävitatakse sama lõike alusel nii elektroonilised hääled, kui ka süsteemis sisalduvad valijate isikuandmed."

33) Pakutavad garantiid isikuandmete hävitamiseks ei ole piisavad, sest hävitatakse see osa isikuandmetest, mis on RVT valduses ja mida RIA jt partnerid valimiste korraldamisel suudavad hävitada, sj ei hävitata füüsiliselt kõiki andmekandjaid, mida kasutati RIAs või muudeks toiminguteks (nt RVT e-hääletamise eksperdi Indrek Leesi sülearvutit 2023. aasta valimiste järel, millega ta töötles 10.03.2023 toimingu raames kaebaja isikustatud hääli kaebaja juuresolekul).

34) Ennatlik ja sisuliselt ekslik on ka Riigikohtu 3-4-1-13-05 punktis 31 toodud väide: "Valija, keda on elektroonilise hääletamise käigus ebaseaduslikult mõjutatud või jälgitud, saab taastada valimiste vabaduse ja hääletamise salajasuse, hääletades mõjutustest vabanenult uuesti elektrooniliselt või valimissedeliga."

35) Valija, keda on jälgitud, ei saa hääletamise salajasust taastada uuesti hääletamisega, välja arvatud erandlikul juhul, kus valija muudab pärast ebaseaduslikult jälgimist vabatahtlikult oma valikut. On ebatõenäoline, et isik sooviks muuta oma poliitilist eelistust üksnes seetõttu, et teda on e-hääle andmisel jälgitud.

36) Seetõttu on on põhimõtteliselt ekslikud Riigikohtu väited uuesti hääletamisega tagatavast hääletamise salajasusest, aga ka RVT pole toonud ühtegi põhjendust, kuidas aitab valija isikustatud tahteavalduse töötlemine tagada hääletamise salajasust – ülaloleva valguses tuleb pidada ka RVT sellekohaseid väiteid ekslikuks.

37) Kasutatud tõlgendus hääletuse salajasusest ei vasta Euroopa tavadele: "Pole veel selge, kas see uuenduslik tõlgendus salajasuse põhimõttest Eestis elab üle integratsiooni Euroopa Kogukonda. Euroopa Ülemkohtu viimatised otsused ei anna põhjust arvata, et

nad järgiksid Interneti-hääletuse kaitsjate **teleoloogilist argumendiliini**."[4] (Originaal: "*It is not yet clear whether this innovative interpretation of the principle of secrecy in Estonia will survive the integration of the country into the European Community. Recent decisions of the European High Court give no hint that they will follow the* ***teleological line of argument*** *given by the defenders of online voting.*")

"Mis puudutab hääletamise salajasust, on [Eesti] riik kasutanud üsna uuenduslikku lähenemisviisi sellest põhimõttest tulenevate piirangute käsitamiseks. Algusest peale on see riik kaitsnud hääletamise salajasuse **teleoloogilist tõlgendust**, kuid seejuures aru saamata, et valimisasutustel ei ole mingit funktsiooni selle tagamisel, et hääletajad saaksid anda oma hääle salaja ka siis, kui nad hääletavad järelevalveta keskkonnas."[5] (Originaal: „*When it comes to secret suffrage, the country has adopted quite an innovative approach to understand the constraints imposed by this principle. From the outset, the country has advocated for a* ***teleological interpretation*** *of secret suffrage, but without understanding that the electoral administration has no role in ensuring that votes can cast their votes secretly even when voting from unsupervised environments.*")

38) Seejuures on võimalik tagada nii hääletamise salajasust, valimiste vabadust kui valimiste ühetaolisust "üks valija, üks hääl" põhimõtte tähenduses ilma valijate isikustatud tahteavaldusi töötlemata, nt anonüümides valijad veel enne tahteavalduste esitamist – lahendus, mida kasutavad mitmete teiste riikide e-hääletuse pilootprojektid.

E-hääletuse süsteem on vastuolus RKVS salajasuse paragrahviga

39) Varem RKVS §48[6] "Valimiste salajasuse tagamine" (edaspidi: salajasuse paragrahv) üldse puudus, mistõttu olid samad põhimõtted tagatud madalama VVK otsuste vm madalama taseme regulatsiooniga. Valimiste ajal 3.06.2024 kehtima hakanud salajasuse pargarahvi sätted sõnastavad küll õigeid põhimõtted, kuid tegelik e-hääletuse süsteem neid varem implitsiitsena kehtinud nõudeid praktikas ei taga.

40) Implitsiitne on ka nõuete seos CM/Rec (2017)5 e-hääletuse standardite soovitusega (edaspidi: standardite soovitused), mida need suuresti kopeerivad, kuid nende kooskõla soovitustega ei ole analüüsitud ega teinud seda ka paragrahvi seadusse toonud 344SE seletuskirjad. Seetõttu on praktikas ka vastavus standardite soovituste IV jaotisega "salajane hääletus" (*secret suffrage*) osaline ja põhistamata.

41) Salajasuse paragrahvi lõike 1 järgi **peab** olema e-hääletamine korraldatud selliselt, et "igas hääletamisetapis, sealhulgas pärast elektroonilise hääle tühistamist, järgitakse hääle salajasuse põhimõtet". Seadus ei täpsusta, kas salajasuse põhimõtet peab järgima valimiste korraldaja või valija, vaid sätestab üldise salajasuse põhimõtte tagamise, mis implitseerib mõlemat. Ka sätestatakse kohustus, et salajasuse põhimõtet järgitakse ka tühistatud häälte puhul, mis tähendab, et salajaseks peavad jääma ka hääled, mis on muudetud uuesti hääletamisega või hääletamisega jaoskonnas, mis tühistab varasemad e-hääled.

4 Buchstein, H. (2004). Online Democracy, Is it Viable? Is it Desirable? Internet Voting and Normative Democratic Theory. lk 52-53 In: Kersting, N., Baldersheim, H. (eds) Electronic Voting and Democracy. Palgrave Macmillan, London. https://doi.org/10.1057/9780230523531_3

5 Adrià Rodríguez-Pérez, „Secret texts and cipherballots: secret suffrage and remote electronic voting', PhD Thesis, Universitat Rovira i Virgili, Dept of Public Law, Juhendaja: dr Jordi Barrat i Esteve, lk 35−36 ja üksikasjalikumalt lk 111jj. Veebis https://www.tdx.cat/bitstream/handle/10803/675606/TESI%20Adri%C3%A1n%20Rodr%C3%ADguez%20P%C3%A9rez.pdf

42) Arvestades, et soovija saab kontrollrakendusega valija antud e-hääle alla laadida ja selle QR-koodis oleva võtmega avada, pole salajasuse põhimõtte järgimine selles faasis tagatud, eriti kui vaadata seda kooskõlas lõikega 10, mille kohaselt tuleb korraldada e-hääletus ja häälte lugemine selliselt, et "ei ole võimalik luua seost valija ning avatud hääle vahel". Isegi kui "avatud hääle" puhul peetakse rangelt silmas lugemisele läinud, RVT/VVK jagatud privaatvõtmega avatud või kokku loetud häält, siis lõike 1 järgi peab olema salajasuse põhimõte tagatud ka tühistatud e-hääle puhul, st nende e-häälte puhul, mis lugemisele ei läinud, aga lõike 10 järgi ka "elektroonilise hääletamise" enda ja mitte ainult häälte lugemise etapis. Nii tühistatud kui ka lugemisele läinud hääli saab avada lisaks RVT/VVK jagatud privaatvõtmele ka QR-koodi efemeerse võtme ehk juhuarvuga, mistõttu ei ole tagatud hääle salajasuse põhimõtte järgimine igas hääletamisetapis.

43) Samamoodi on lõikes 2 nõutud, et valijarakendus **peab** "salastama valija hääle selliselt, et hääle edastamisel ei ole võimalik näha, kelle poolt valija hääletas", milles salastamise all peetakse silmas hääle krüptimist RVT/VVK avaliku võtmega. Kuna kasutusel olev ElGamal krüptosüsteem eeldab lisaks efemeerse võtme ehk juhuarvu kasutamist, mille abil saab hääle dekrüpteerida RVT/VVK jagatud privaatvõtit omamata ja millel põhineb kontrollrakendus, mis kasutab krüptosüsteemis rangelt *efemeersena* määratletud võtit mitte-sihtotstarbekohaselt ehk mitte seda pärast krüptimist ära visates[6], vaid säilitades ja edastades eeldatavasti kasutaja teisele seadmele, siis pole tagatud ka valija hääle salastamine selliselt, et edastamisel pole valija tahteavaldust näha **võimalik**.

44) Lõike 9 järgi **peab** elektroonilise hääletamise süsteem lisaks tagama, et "kui valija on hääletanud mitu korda, ei ole võimalik valijal kellelegi tõendada, milline tema antud elektrooniline hääl läks arvesse". See pole tagatud üksiku e-hääle puhul, sest korrektselt vastuvõetud hääl läheb eelduslikult arvesse ja krüptitud hääles sisalduv tahteavaldus on dekrüpteeritav QR-koodis oleva efemeerse võtmega, kuid see pole tagatud ka muudetud e-häälte puuhul, sest valija saab oma SK ID Solutions poolt registreeritud ID-toimingute ehk OCSP päringute logi alusel tõendada, missugune oli tema viimane hääl, kui logis on ID-kaardi sertifikaatide kehtivuskinnituste ajatemplid seatavad vastavusse kontrollprotokolli alusel alla laaditud häälekonteinerites toodud kehtivuskinnituste ajatemplitega. Jättes lahtiseks, kas valija tahab häält tõendada ise või sunnitakse teda selleks, on lõikes 9 nimetatud "ei ole võimalik kellelegi tõendada" igal juhul tagamata.

45) VVK seisukoha punkti 15 järgi ei oma RKVS §48[6] lg 9 kaebuse vaatenurgast tähtsust, kuid arvestades kaebuses toodud väidet, et hääletamise salajasus pole piisavalt tagatud, on tähtsad kõik salajasuse puuduliku tagamise detailid, sj on tähelepanuväärne, et punktis 15 kinnitab VVK, et elektroonilise hääletamise süsteem "ei anna valijale teavet selle kohta, mitu korda valija elektrooniliselt hääletas või kas ta hääletas ka valimisjaoskonnas", kuid jätab tähelepanuta selle, et selle info saab valija isikuandmete päringuga SK ID Solutionsilt ja lisaks sellele on saanud valija RKVS §23 lõike 1 alusel isikuandmete päringu esitamise käigus RVT käest ka väljavõtte oma andmetest valijate nimekirjas, kus on toodud välja, kas valija hääletas ka jaoskonnas.

46) Seega annab e-hääletuse süsteem või selle korraldusega olemuslikult seotud taristu välja tõendid, mis võimaldavad valijal tõendada oma e-häält tõendusjõuga, mis on samaväärne valimiste korraldaja poolt kasutatavate tõenditega, mille alusel ta hääli kokku loeb (erinevusega, et valija saab enda käes olevaid tõendeid kontrollida, lasta teistel

6 https://en.wikipedia.org/wiki/Ephemeral_key

kontrollida ja veenduda nende kehtivuses). Seda näitlikustab ning selgitab kaebaja poolt 2023. aasta Riigikohtu asja 5-23-20 lisana esitatud asjatundja hinnang[7].

47) Salajasuse paragrahvi lõigetes 3 ja 4 tuuakse välja samaväärselt tugevaid nõudeid e-hääletuse süsteemi osas, mis pole samuti tagatud, sest lõike 3 nõue, et süsteem **peab** tagama, et "enne elektrooniliste häälte lugemist eraldatakse valija isikuandmed elektroonilisest häälest selliselt, et **ei oleks võimalik** tuvastada valija tahteavaldust" on tagatud üksnes protseduuriliselt, st mitte **võimatuse** tähenduses, vaid ainult tähenduses, mille järgi ametliku protseduuri järgimisel ei tohiks seda juhtuda. Seejuures toob e-hääletuse süsteemi arendaja oma VVK otsuse seisukoha punktis 1 välja, et see eeldab pahatahtlikke valimiste korraldajaid, kes "kasutavad häälte dekrüpteerimise võtmeid kooskõlastatult selleks mitte ettenähtud ajal", kuid jätab kõrvale võimaluse, et valimiste korraldaja või tema arvutisüsteemid on kompromiteeritud juba võtmete loomise ajal, mis oleks võtmeloome baasüsteemi ettevalmistamise ja võtmeloome enda protseduuride dokumenteeritult kehva kvaliteeti silmas pidades märksa tõenäolisem stsenaarium.

48) Lugemisele eelneva töötlemise hääle salajasuse nõuded pole läbi mõeldud ka ses osas, et VVK oma seisukoha punktis 12 väidab, et "valija isikuandmed ei sisaldu samas krüptogrammis e-häälega", kuid tegelikkuses on ElGamali krüptosüsteemi kasutamisel iga krüptogramm unikaalne efemeerse võtme kasutamise tõttu ja eesmärgiga tagada valija tahteavalduse sisu tuvastamatus pelgalt krüptogrammide võrdlemise teel. Krüptogrammide prakilise unikaalsuse tõttu on need vähemalt enne segamist/rekrüptimist otseselt seotud hääle edastanud valijatega. See tähendab, et krüptogramm sisaldab oma krüptograafiliste omaduste tõttu valija isikuandmeid, sest on krüptograafiliselt kokku viidav valija edastatud ja digiallkirjastatud häälekonteineriga, milles tagab seost täiendavalt krüptogrammi räsi, mille äratoomine on digiallkirjastatud konteineris kohustuslik.

49) Salajasuse paragrahvi lõikes 4 väljendatud andmete minimalismi nõue on tagatud ainult eeldusel, et pole mõeldavad e-hääletuse süsteemid, mis tagaks valimiste salajasust ja valija hääle salastatust paremini või paremas proportsioonis valimisõiguse põhimõtetega. See eeldus pole aga põhjendatud ja teiste riikide e-hääletuse pilootprojektid väldivad e-häälte isikustatud töötlemist ülemäärases ulatuses ega säilita neid digitallkirjastatud vormis, mis loob väga tugeva seoses salvestatud hääle ja selle andnud isiku vahele. Selline valik võib olla e-hääletuse süsteemi planeerimisel 2002-2005 tehtud ekslik eeldus, et ID-kaardi abil digiallkirjastamine on olemuslik ja vajalik e-hääletamise osa, kuigi praktikas see hoopis välistab valimiste vaadeldavuse ja kompromiteerib hääletamise salajasuse põhimõtet.

50) VVK oma seisukohtade punktis 6 osutab Euroopa Nõukogu soovitusi CM/Rec (2017)5 e-hääletuse standardite kohta, mille punktist 25 tuleneb implitsiitselt salajasuse paragrahvi lõikes 1 nõutud salajasuse põhimõtte järgimine ka tühistatud ja lugemisele mitte läinud häälte osas, mida ülal kirjeldatust lähtudes Eesti e-hääletuse süsteem praktikas ei taga. Samamoodi annab raami salajasuse paragrahvi lõigete 1 ja 9 tõlgendamiseks standardite punkt 23, mille kohaselt ei tohi olla valijale olla kättesaadavad kolmandatele pooltele edastatavaid tõendeid antud hääle kohta ja valijad peavad olema riskidest informeeritud (negatiivseks eeskujuks sobib Alar Karis 2023. aasta Riigikogu valimistel QR-koodi

7 https://infoaed.ee/salajasus/eksperthinnang.asice

ERRi uudistes avaldamisega potentsiaalslet tõendamas oma valimistel antud häält[8]).

51) Seejuures standardite soovituste punkt 26 eeldab valijate anonüümimist häältelugemise ajal, kuid kuna häältelugemine algab töötlemisega, kus eemaldatakse korduv- ja topelthääli, aga mõnikord ka parandatakse oletatavaid lugemisvigu mitte-ametlike tühistusnimekirjadega[9], sh eemaldatakse hääli, mis ei vasta oletatavatele krüptograafilistele nõuetele, digiallkirja standardile, mis kõik mõjutavad valimistulemust, siis pole täidetud ka eeldus, et häältelugemise ajal on valijad anonüümsed ja tagatud on anonüümsus ka auditeerimisel RVT palgatud audiitori poolt.

52) Riigikohtu hinnangul põhiseaduse tõlgendamisel kohaseks abivahendiks oleva Euroopa Nõukogu soovituse CM/Rec (2017)5 e-hääletuse standardite kohta rakendusjuhiste IV peatükis toodud nõuetest hääletamise salajasuse tagamiseks ei täida kaebaja hinnangul e-hääletuse süsteem punktidest 19-26 täielikult ühtegi ning on otseses vastuolus nõudmistega 23, 25 ja 26.

53) Tõlgendades valimiste ajaks lisandunud salajasuse paragrahvi iseeseisvalt kui VVK eeskujul võttes šnitti Euroopa Nõukogu standardite soovitusest ei ole RKVS §48[6] nõutud salajasus tagatud, mistõttu kaebaja nõudmine oma e-häält isikustatud kujul säilitada on sisuliselt motiveeritud. Arvestades, et kaebaja olnud Riigikohtu menetluses olnud kaebuses asjatundjana arvamust avaldama, tuleb pidada teda ka piisavalt informeerituks selliste otsuste tegemisel, kui küsimuse all on tema isiklik hääl valimistel.

Elektroonilise hääletamise süsteemi arendaja seisukoht

54) Elektroonilise hääletamise süsteemi (EHS) arendaja osutab stsenaariumile, kus „valimiste korraldajad on pahatahtlikud ning kasutavad häälte dekrüpteerimise võtmeid kooskõlastatult selleks mitte ettenähtud ajal" ning väidab: „Selle ohu maandamiseks on elektroonilise hääletamise süsteemis võti osadeks jagatud ja selle taastamine eeldab rohkem kui poolte võtmehaldurite pahatahtlikku tegutsemist. Võtmeosakud on jaotatud Vabariigi Valimiskomisjoni liikmete ja riigi valimisteenistuse teenistujate vahel."

55) EHS arendaja jätab tähelepanuta, et võti ei pea lekkima RVT/VVK liikmetele väljajagatud kaartidelt, vaid võib lekkida ka genereerimise või juba sellele eelneva arvutisüsteemide ettevalmistamise käigus. See teeb e-häälte salajasuse murdmise krüpteeritud valimiskasti tervikuna dekrüpteerimise teel tunduvalt lihtsamaks ja varjatumaks. Ka pole privaatvõtme olemasolul selline dekrüpteerimine tehniliselt keerukas, nt arendaja avaldatud lähtekoodis tegeleb sellega napilt paarisaja realine Java-lähtekood, mis on hästi kommenteeritud ning suurema vaevata kasutatav dekrüpteerimiseks ka võtmeosakuteta.[10]

8 https://digi.geenius.ee/rubriik/uudis/ajakirjanikel-oli-teoreetiline-voimalus-president-alar-karise-e-haale-salajasuse-murdmiseks/

9 https://digi.geenius.ee/rubriik/uudis/valimiskomisjon-langetas-e-valimiste-osas-otsuse-mis-riigikohtu-hinnangul-ei-olnudki-otsus/

10 Vahetult dekrüptimisega tegelev osa koosneb 14 Java-lähtekoodi reast: https://github.com/valimised/ivxv/blob/published/common/java/src/main/java/ee/ivxv/common/crypto/elgamal/ElGamalPrivateKey.java#L171-L185

56) EHS arendaja on vaidlustatud otsuses toonud võimalike rünnetena hääletamise salajasuse vastu välja järgmist: “Valimiste korraldajad on pahatahtlikud ning kasutavad häälte dekrüpteerimise võtmeid kooskõlastatult selleks mitte ettenähtud ajal.” Lisaks: “Hääle salajasuse rikkumine QR-koodi kaudu on **võimalik** ainult valija enda tegevuse tulemusel.”

57) Mõlemad on lihtsustused, sest valimiste korraldaja ja valija **võimalus** salajasust rikkuda tähendab, et seda on võimalik rikkuda ka mõni samas rollis olev ründajal (esimesel puhul RVT, RIA, Riigikogu kantselei vmt töötaja, tema üle mõju saavutanud või tehniliste vahendite abil samaväärsesse rolli sisenenud välisründaja, teisel puhul RVT kui valijarakenduse ja kontrollrakenduse levitaja, aga ka brauserite tootja ja kontrollrakenduste levitaja Apple/Google, kuid kõige lihtsamini kliendiarvutile ligi pääsev isik, nt pereliige või ka väline ründaja).

58) EHS arendaja on vaidlustatud otsuses toonud, et “Riigi valimisteenistus peaks selleks tegema kõvasti lisatööd – jälgima valijaid, muutma rakendusi.”

59) Küsimus pole küberturbe ründevektorite analüüsis, st kui palju ja missugust lisatööd peaks selleks tegema, vaid kaebuse kontekstis on oluline, et sellised stsenaariumid on tehniliselt realistlikud, mh on neid väikeses skaalas ka demonstreeritud ning on olemas nende läbiviimiseks vajalik näidistarkvara.

60) Vaidlustatud otsuses on toodud järgmist: “Urni ja elektroonilisi hääli hoitakse isikustatavatena võimalike valimiskaebuste lahendamiseks kuni võimalike kaebuste lahendamise tähtajani ja valimistulemuse väljakuulutamiseni.” Lisaks: “Vajadusel on võimalik enne valimistulemuse kinnitamist töötlemisprotseduure korrata või teha täiendavaid auditeid.

61) See pole praktikas teostunud, sj on nii RVT kui VVK ka praegu keeldunud kaebuste lahendamiseks töötlema üksikuid hääli või tegema vigu parandavaid korduslugemisi.

Vastused VVK-le

62) VVK on vaidlustatud otsuses väitnud, et „Kui mõnes kaebuses väidetakse, et elektroonilise hääletamise või e-häälte lugemise korda on rikutud, ei võimaldaks isikustatud e-häälte hävitamine selliste vaidluste lahendamisel tugineda tõenditele ega korraldada ka uut häälte lugemist.”

63) See pole tõsi, sest saab lugeda ka anonüümitud hääli, mida tehakse edukalt nt pabersedelitega hääletamisel jaoskondades.

64) VVK on vaidlustatud otsuses möönnud, et „selliste tundlike isikuandmete töötlemine (hoiustamine) 30 päeva vältel pärast kaebetähtaja möödumist, kui valimiskaebusi ei esitata, võib olla vastuolus minimaalsuse põhimõttega, kuid praegusel juhul sellise olukorraga tegemist ei ole. Valimiskaebused ei ole lahendatud ka Vabariigi Valimiskomisjoni otsuse tegemise ajaks.” Lisaks: “Isikustatud e-häälte töötlemine on vajalik avalikes huvides oleva ülesande täitmiseks ja vastab seetõttu IKÜM art 6 lg 1 punktile e. Isikuandmete töötlemine on praegusel juhul ette nähtud seadusega, neid ei töödelda suuremas ulatuses ega kauem, kui valimistulemuste lõplikuks väljaselgitamiseks on vajalik.”

65) Selline töötlemine on on vajalik ainult kooskõlas ekslike **võimalikkuse** väidetega eelnevalt ja eeldusega, et pole valimiste salajasust vähem riivavat ja samu eesmärke tagavat e-hääletuse arhitektuuri, süsteemi või protokolli.

66) Vaidlustatud otsuses on toodud väide, mille kohaselt "Kaebaja ei ole kaebuses nimetanud konkreetseid näiteid, et riigi valimisteenistus või arendaja oleksid elektroonilise hääletamise süsteemi komponente pahatahtlikult muutnud, vaid on esitanud üksnes teoreetilisi väiteid."

67) VVK on jätnud arvestamata, et kaebaja vaidlustabki isikustatud hääle säilitamist mitte praktilise infoturbe, vaid andmekaitse ja hääletamise salajasuse põhimõtte vaatenurgast. Kaebajal ei ole kohustust tõendada, et valimiste salajasust on praktikas rikutud või et hääletamise andmed on lekkinud – isikuandmete säilitamine ilma õigusliku aluseta on ebaseaduslik ka juhul, kui need ei leki.

68) Kaebaja väited pole siiski teoreetilised, vaid praktiliselt näitlikustatud ka kaebaja enda poolt, sj 15-minuti piir hääle tõendatavusele ei pea paika selle valguses, et häälekonteinerid on võimalik alla laadida ja neid kontrollida piiramatu aja jooksul pärast valimisi.

69) Vaidlustatud otsuses on toodud väide, et "Oht, et nimetatud QR-kood saadetakse valijarakenduse poolt ka mujale kui elektroonilise hääletamise süsteemi, on välistatud turvatestimise läbiviimisega kolmanda osapoole poolt."

70) Väide „**on välistatud**" on sama eksitav nagu varasemad **võimalik** väited ning VVK läheb siin vastuolu omaenda deklareeritud turvaeeldustega – QR-koodiga tegeleb kliendiarvuti, mille turvalisuse tagamine ei kuulu valimiste korraldaja hinnangul turvamudelisse ja selle vastu suunatud ründed on ainsa avaliku ja tervikliku turvaanalüüsi järgi deklareeritud "aktsepteerimist vajavaks riskiks".[10]

71) Vaidlustatud otsuses on väidetud: "Siiski toimub isikuandmete kaitse aspektist isikustatud e-häälte töötlemisega seotud riskide hindamine iga kord enne valimisi. Selleks rakendatakse infoturbe meetmeid, koostatakse riskianalüüs, viiakse läbi turvatestimine ja vaadatakse iga kord üle audiitori soovitusi."

72) Kaebajale ei ole teada, et taolist hindamist oleks dokumenteeritud. Kui VVK soovib sellele väitele tugineda, siis peaks VVK esitama tõendid, mis seda kinnitavad.

Kokkuvõte

73) Eestis alustati e-hääletuse kavandamist 2000. aastal, mil IKÜM ei olnud veel olemas ja Riigikohtu 2005. aastal antud hinnangud hääletamise salajasuse tagamisest on antud hindamata nende kooskõla Euroopa Liidus tänapäeval kehtivate õiguspõhimõtetega. Seejuures lähtusid e-hääletuse algsed arendused eeldusest, et ID-kaardi kasutamine ja valija tahteavalduse isikustatud ja digiallkirjastatud kujul säilitamine on e-hääletuse läbiviimise jaoks olemuslik. Kuigi ka 2003.-2004. aastatel e-hääletuse tehnilise arendamise suunda otsustades oli ID-kaardi sellisele kasutamisele avalikkuses

10 https://www.valimised.ee/sites/default/files/uploads/eh/EH-02-02_2011-01-13.pdf 4.6.2. "Hääletajate arvutite võimalik ebaturvalisus" lk 30

vastuhääli[11], siis loobuti algselt krüptograafide Helger Lipmaa ja Oleg Mürgi soovitatud e-hääletuse süsteemi arendamise stsenaariumist robustselt isikustatud ja krüptograafiliste garantiideta e-hääletuse süsteemi kasuks.

74) Eesti arusaam e-hääletusest ei ole ainuvõimalik ning viidi ellu kiire tehnilise progressi tingimustes ilma muudatusi põhjalikult kaalumata. E-häälte anonüümimine alles hääletuse viimases faasis tekitab tõsiseid probleeme valimissaladuse tagamisel, kuigi saab anonüümida ka esimeses faasis, mis on tüüpiline praktika paljudes teistes riikides, kus e-hääletust on katsetatud (nt Norra või Šveits). Eesti e-hääletuse valik anonüümida viimases faasis tulenes suuresti ID-kaardi kui tehnilise lahenduse kasutamisest ja sellel rakenduse leidmise soovist pärast 2002. aastat, mõistmata valiku tagajärgi valimisõiguse jaoks.

75) E-hääletuse liiga otsest tuletamist ID-kaardi taristust on kirjeldanud ka valdkonda uurivad teadlased, nt Aro Velmet: "Vastupidiselt digivabariigi ergutusrühmale väidan, et e-hääletust ei tuleks mõista mitte demokraatia uuendamise suure ettenägelikkuse kulmineeruva sammuna, vaid pigem perifeerse kõrvalsaadusena ühele teisele digitaalsele taristuprojektile, mis tõi kokku avaliku ja erahuvi – digitaalsele isikutunnistusele."[12] (Originaal: „*I argue, contrary to the digital republic's cheerleaders, that, rather than being the culminating step in a grand vision of democratic renewal, e-voting is best understood as a peripheral byproduct of a different digital infrastructural project that brought together both public and private interests – the digital ID*“)

76) IKÜM polnud veel vastu võetud ega rakendunud ka 2013. aastal QR-koodil põhinevat valija isikliku hääle kontrollimehhanismi sisse viies, vaid Eesti on olnud isikuandmete kaitse üldmääruse suhtes rõhutatult leige, viies selle rakendamiseks vajalikud esmased seadusemuudatused sisse alles 2019. aastal pea seitse kuud pärast IKÜMi kehtima hakkamist[13]. Kontrollmehhanism võeti Riigikogu poolt vastu 2012. aastal intensiivse poliitilise vaidluse tingimustes OSCE/ODIHR 2011. aasta raporti soovitustest lähtuvalt ning nende sisu mõistmata[14], sj mõistmata raportis soovitatud krüptograafiliste kontrollide olemust, mille alamääratletusele juhtis Riigikohus tähelepanu oma 5-19-20 otsuses, kuid mis on jätkuvalt selgelt sätestamata õigustloovates aktides.

77) Kui seadusandja soovib e-hääletust võimaldada, ei tohiks siiski seda teha tuues ohvriks põhiõigusi ja valimisseaduste uuendamise häid praktikaid, mis eeldavad valimissüsteemi oluliste muudatuste vastuvõtmist laia avaliku debati ning konsensusega ja aegsasti. Seejuures ei saa olla kaalukausil salajasus vs avalik kontroll valimistulemuste üle, sest mõlemad on demokraatlike valimiste jaoks vajalikud ning olemuslikud, kummagi suhtes ei tohiks iseäranis meie noor demokraatia teha mõtlematult mööndusi.

78) Riigikohus oma 5-24-9 jätab VVK 4.06.2024 taotletud **põhiseaduspära järelevalve** raames sisulise analüüsita nii valimiste vaatlemise kui valimiste salajasuse põhimõtete tagamise kooskõlas põhiseaduse nõuetega ning otsuse punktis 26 lihtsalt deklareerib

11 https://epl.delfi.ee/artikkel/51013899/elmer-joandi-e-valimised-diktaatorite-soovunelm

12 Free to Choose: E-voting, Infrastructure, and The Origins of Estonia's Digital Republic. Contemporary European History [forthcoming]. Internetis viidatatav: https://www.etis.ee/Portal/Publications/Display/7e2b08f1-4d08-4b2a-8f5d-30c198e9a1fe. Siinse dokumendi esitamise seisuga ei ole Aro Velmeti eelviidatud töö veel avaldatud, kuid kaebaja on avaldamisele läinud versiooniga tutvunud.

13 https://triniti.eu/et/uudised/iks-seadus-mida-tuleb-lugeda-koos-maarusega/

14 https://arvamus.postimees.ee/3138897/mart-poder-vaadeldamatu-e-haaletus-pole-usaldusvaarne, saadaval ka blogis https://gafgaf.infoaed.ee/posts/rohkem-kryptot/

kehtiva seaduse ülimuslikkust põhiseaduslike printsiipide ees, olles jätnud e-hääletuse põhiseaduspärasuse küsimused sisuliselt hindamata ka kõigis 2023. aastal esitatud valimiskaebustes.[15]

79) Käibiva e-hääletuse süsteemi põhjendamine on toimunud ja toimub ka käesolevas debatis läbi ekslike ja põhistamata eelduste, mida väljendavad eksitavad väitelised modaalsused **võimalikkuse**, **tegelikkuse** ja **vajalikkuse** kohta, mis puudutavad nii e-hääletuse tehnilisi protokolle, arvutisüsteemide omadusi kui valimiste põhiseaduslikke ja demokraatlikke põhimõtteid. Kaebaja on oma 2023. aasta Riigikogu valimiste vaatlejaraportis nimetanud seda ontoloogiliseks valimispettuseks (*ontological gerrymandering*), mis on termin, mille võttis Eesti ja Hollandi e-hääletuse debattide analüüsimisel oma 2007. aasta doktoritöös "*La volonté machinale*" kasutusele Wolter Pieters.[16]

80) 01.09.2005 otsuses nr 3-4-1-13-05 toodud eesmärk võtta kasutusele uusi infotehnoloogiliste lahendusi ei saa olla niivõrd kaalukas, et õigustada valimiste usaldusväärsuse langemist ning järeleandmiste tegemist hääletamise vaadeldavuse ja salajasuse vallas. Muutuse mõistlikuks ei põhjenduseks ei saa olla muutus ise, st ainuüksi fakt, et tegemist on millegi uuega. Kaebaja palub, et Riigikohus annaks võimalusel siinset kaebust lahendades laiema hinnangu ning käsitleks eelmainitud e-valimiste kitsaskohti, mis on varasemalt jäänud sisulise vastuseta.

81) **Kokkuvõtlikult** leiab kaebaja, et valimiste läbiviijal ei ole õiguslikku alust säilitada kaebaja antud e-häält isikustatud kujul enam kui kuu aega. Taoline toiming ei ole proportsionaalne ning puuduvad piisavad meetmed, mis tagaksid, et kaebaja poliitiline eelistus ei saa avalikuks. Ühtlasi on valimiste läbiviija valduses privaatvõti, millega on võimalik dekrüpteerida kõigi, sh kaebaja, e-hääled ning tuvastada e-hääletanute poliitiline eelistus. Taolise riski olemasolu ei ole mõistlik ega valimiste salajasusega kooskõlas. Kaebaja palub seetõttu, et Riigikohus kaebuse rahuldaks.

Lugupidamisega

(allkirjastatud digitaalselt)

Märt Põder

15 https://p6drad-teel.net/~p6der/kaebus3/valimiskaebus_2024_1_t%c3%a4iendavad_seisukohad.pdf
16 https://infoaed.ee/findings2023/