

Tallinna Halduskohus

30. mai 2024

Tallinna kohtumaja

Kaebaja: **Märt Pöder**
isikukood: 37909110298

Lepinguline esindaja: advokaat Märt Mürk
Advokaadibüroo EMERALDLEGAL
Ahtri 6A, Tallinn 10151
tel: +372 5560 1177
e-post: menetus@emerald.legal

Vastustaja: **Eesti Vabariik (Riigikogu Kantselei kaudu)**
registrikood: 74000101
adress: Lossi plats 1a, Tallinn 15165
e-post: riigikogu@riigikogu.ee

KAEBUS TOIMINGUST HOIDUMISEKS

ja

ESIALGSE ÕIGUSKAITSE TAOTLUS

RESOLUTSIOON:

- Kohustada Riigi Valimisteenistust hoiduma Eesti Vabariigi Euroopa Parlamendi 2024. aasta valimiste eelhääletamise ajal kaebaja vabalt valitud kandidaadile antud hääle säilitamisest isikustatud elektroonilise häälena elektroonilise hääletamise süsteemis pärast elektroonilise hääle vastuvõtmist elektroonilise hääletamise süsteemi poolt.
- Jätta kõik menetluskulud vastustaja kanda ning mõista menetluskulud vastustajalt kaebaja kasuks välja.

ESIALGSE ÕIGUSKAITSE TAOTLUS:

- Keelata esialgse õiguskaitse korras alates 3. juunist 2024 kell 9.00 Riigi valimisteenistusel kaebaja vabalt valitud kandidaadile Eesti Vabariigi Euroopa Parlamendi 2024. aasta valimistel antud hääle säilitamine isikustatud elektroonilise häälena elektroonilise hääletamise süsteemis pärast elektroonilise hääle vastuvõtmist elektroonilise hääletamise süsteemi poolt.



MENETLUSLIKUD TAOTLUSED:

4. Vaadata asi läbi istungil.

I. KAEBUSE LÜHIÜLEVAADE JA FAKTILISED ASJAOLUD

- 1. Kaebuse lühikokkuvõte.** Kaebuse aluseks on asjaolu, et Euroopa Parlamendi valimistel säilitatakse valijate e-hääli isikustatud kujul. E-valimiste serveris säilitatakse andmeid selle kohta, millise kandidaadi poolt iga e-hääle andnud valija oma hääle andis. Valimiste läbiviijal on seega võimalik tuvastada e-hääle andnud valijate poliitilisi eelistusi.
2. Salajased valimised on üks lääneliku demokraatia alustalasid. Puudub mõjuv põhjus, miks täitevvõimul peaks olema ligipääs valijate poliitiliste eelistuste andmetele. Selliste andmete säilitamine ei ole põhjendatud ning on vastuolus valimiste salajasuse ja delikaatsete isikuandmete töötlemise põhimõtetega.
3. Kaebaja palub, et kohus keelaks vastustajal e-häälte töötlemise isikustatud kujul, st viisil, mis võimaldab e-häält viia kokku selle e-hääle andnud isikuga. Kaebaja põhjendab oma nõuet alljärgnevalt.
- 4. Faktilised asjaolud.** Euroopa Parlamendi valimisinädal toimub alates 3. juunist 2024 kell 9.00 kuni 9. juuni 2024 kella 20.00-ni. Euroopa Parlamendi valimise seaduse (EPVS) § 47² kohaselt kohaldatakse Euroopa Parlamendi elektroonilistele valimistele Riigikogu valimise seaduse (RKVS) 7¹. peatükis sätestatud korda. EPVS § 37 lg 2 p-i 4 kohaselt toimub eelhääletamine kuuendast kuni esimese päevani enne valimispäeva elektrooniliselt. Elektrooniline hääletamine (edaspidi ka **e-hääletamine**) algab 3. juunil kell 9.00 ja kestab kuni 8. juunini kella 20.00-ni (edaspidi ka **hääletamisperiood**).
5. EPVS § 9 lg-e 1 p 1 kohaselt korraldab teiste hulgas Euroopa Parlamendi valimisi riigi valimisteenistus. Riigi valimisteenistus on RKVS § 14 lg 1 kohaselt Riigikogu Kantslei struktuuriüksus.
6. RKVS § 48² lg-e 1 kohaselt haldab riigi valimisteenistus elektroonilist hääletamise süsteemi (edaspidi ka **e-hääletamise süsteem**), millist kasutades saab valija hääletamisperioodil elektrooniliselt hääletada (RKVS § 48⁴ lg 1). Hetkel kehtiva RKVS § 48⁴ lg-e 2 kohaselt tuvastatakse valija isik Vabariigi Valimiskomisjoni (edaspidi ka **VVK**) 09.02.2024 kehtestatud otsuse nr 95 "Tehnilised nõuded elektroonilise hääletamise korraldamise üldpõhimõtete tagamiseks" (edaspidi ka **VVK otsus**) kirjeldatud korras. RKVS § 48⁴ lg-te 3 ja 4 järgi kuvatakse valijale kandidaatide koondnimekiri, mille järel valija märgistab kandidaadi, kelle poolt ta hääletab. Valija kinnitab valiku digiallkirjaga. RKVS § 48⁴ lg-e 5 kohaselt saab valija pärast hääletamise kinnitamist teate hääle vastuvõtmise kohta e-hääletamise süsteemi poolt.
7. Vastavalt VVK otsuse p-le 4.5.1 logitakse e-hääletamise süsteemis valija tuvastamiseks valija nimi ja isikukood, hääletamise alustamise kuupäev ja kellaeg, internetiprotokollide aadress, valija valimisringkond ning internetiprotokollide aadressile vastav asukohariik. VVK otsuse p-i 4.5.2 kohaselt logitakse elektroonilise hääle kinnitamisel ja salvestamisel hääletamise lõpetamise kuupäev ja kellaeg, sertifikaatide väljaandja ning teave sertifikaatide kehtivuse kohta. VVK otsuse p-i 4.5.3 kohaselt logitakse elektroonilise hääle õigsuse kontrollimiseks kontrollimise lõpetamise kuupäev ja kellaeg, internetiprotokollide aadress ning internetiprotokollide aadressile vastav asukohariik. VVK otsuse p 3.5 kohaselt peab valijale tagama õiguse kontrollida pärast valimistoimingu teostamist kontrollrakenduse abil elektrooniliselt antud hääle õigsust 15 minuti jooksul kuni kolm korda.
8. Alates 03.06.2024 jõustuvas (ehk valimiste ajal kehtivas) seaduses on eelviidatud nõuded toodud RKVS § 48⁶ lg-s 5. 03.06.2024 jõustuva RKVS-i § 48⁶ lg 6 sätestab täiendavalt, et



pärast elektroonilise hääletamise lõppemist logid anonüümitakse. See tähendab, et e-hääle andmisel on isik tuvastatav ning isiku e-häält säilitatakse mitteanonüümselt kuni hääletamise lõpuni. Logid anonüümitakse alles pärast hääletamise lõppemist ehk pärast 08.06.2024 kella 20.00-i. Sellest järeldub, et kui isik annab oma e-hääle kohe hääletamisperioodi alguses (03.06.2024 kell 09.00), siis säilitatakse tema e-häält anonüümimata kujul vähemalt viis päeva.

9. Täiendavalt sätestab 03.06.2024 jõustuv RKVS § 48⁶ lg 7, et anonüümimata logid hävitab riigi valimisteenistus RKVS § 77¹ lg-s 2 sätestatud tähtjal ehk mitte varem kui üks kuu alates valimispäevast. Nähtub seega, et anonüümimata e-hääli säilitatakse vähemalt kuu aega.
10. Riigi valimisteenistus on e-hääletamise etappe üldisemalt kirjeldanud oma 06.02.2023 korralduse nr 11 lisas “Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel (edaspidi **üldraamistik**)” (**lisa 1**). Üldraamistiku p 7.5 kohaselt tuvastatakse esmalt hääletaja isik valimisõiguse kindlakstegemiseks (**tuvastamisfaas**). Seejärel teeb hääletaja kandidaatide seast omale sobiva valiku, digiallkirjastab e-hääle ning saadab hääle e-hääletamise süsteemile registreerimiseks (**hääletamisfaas**). Kontrollrakendus võimaldab hääletajal vahetult pärast hääletamist kontrollida antud hääle õigsust. Hääle kohalejõudmist saab kontrollida piiratud aja jooksul teatav arv kordi. Kontrollrakendus kuvab nimetatud aja jooksul hääletaja andmed ja tehtud valiku (**kontrollimisfaas**). E-häältelt eemaldatakse seosed hääletaja isikuga pärast hääletamisperioodi lõppemist ja enne häälte kokkulugemist, mille tulemusel e-hääled anonüümitakse ja segatakse (**töötlemisfaas**) (vt lisa 1 p 7.6). Viimases etapis loetakse hääled kokku (vt lisa 1 p 7.7).
11. Vastavalt VVK otsuse p-le 4.10 on hääled anonüümsed ja jäävad selleks. Riigi valimisteenistuse poolt avaldatud andmekaitsetingimustes teavitatakse, et valimiste valdkonnas on isikandmete vastutav töötleja riigi valimisteenistus. Vastavalt nimetatud andmekaitsetingimuste p-le 1 töötleb riigi valimisteenistus valijate nimekirja elektroonilise hääletamise süsteemis ja edastab elektrooniliselt hääletanute hääletamise fakti ja anonüümitud valiku valimiste infosüsteemi (**lisa 2**).
12. Praktikas tähendab eeltoodu seda, et kuni e-hääletamise lõppemiseni säilitatakse kõiki e-hääli isikustatud ehk mitteanonüümsel kujul. Pärast e-hääletamise lõppemist luuakse kaks andmekogumit – üks, mis on anonüümitud ja teine, mis ei ole. Valimistulemuste arvestamisel loetakse anonüümitud e-hääled. Vastustaja valdusesse jäävad aga endiselt vähemalt kuuks ajaks ka anonüümimata e-hääled. Anonüümimata hääled hävitatakse alles pärast RKVS § 77¹ lg-s 2 sätestatud tähtaega.
13. Isikute poliitiliste eelistuste andmete säilitamine niivõrd pika perioodi jooksul (või üldse) ei ole proportsionaalne, sest see rikub isikandmete töötlemise põhimõtteid ning loob tõsise ohu andmete lekkimiseks. Kaebaja on korduvalt valimistel vaatlejana osalenud ning varasemalt on neid andmeid hoitud DVD-plaadi peal. Tõenäoliselt jätkub see praktika ka selleaastastel valimistel. Kui anonüümimata häälega DVD-plaat satub valedesse kätte, siis võivad kõik e-hääled avalikuks saada. Kaebaja kogemus on, et selle DVD-ga käiakse pärast RIA poolt RVT-le üleandmist ringi väga vabalt, nt jäeti kaebaja 10.03.2023 valimiskasti sisaldanud DVD-ga ilma vahetu järelevalveta RVT ruumidesse.
14. Kaebaja tõi 2023. aasta Riigikogu valimistel välja olulisi puudusi arvutisüsteemide seadistamisel, mida kasutati valimissaladuse tagamise olulisimaks turvagarantideks olevate elektrooniliste häälte salastamise võtme ja häälte avamise võtmete loomisel ja häälte kokkulugemisel. Kuna valimiste korraldajad ei pea nõutavaks ega vajalikuks operatsioonisüsteemi ja tarkvara räsede protokollimist selliste protseduuride puhul ja olukord polnud paranenud ka 2024. aastal läbiviidud samadeks protseduurideks, mis toimusid 20. mail, siis on kaebajal motiveeritud alus mitte pidada piisavaks valimiste korraldaja tagatise kaebaja hääle salajasuse tagamisel.



15. Võttes arvesse, et eelmistel Riigikogu valimistel hääletas ligi 50% valijatest elektrooniliselt, tähendaks andmete lekkimine poolte Eesti valijate poliitiliste eelistuste avalikustamist. Taolisel lekkel oleksid ühiskonna jaoks kaugeleulatuvad tagajärjed, mistõttu ei ole sellise riski loomine mõistlik ega õiguspärane.
16. Kaebaja soovib hääletamisperioodil elektrooniliselt hääletada, s.o alates 3. juunist kell 9.00. Kaebaja hinnangul puudub riigi valimisteenistusel õiguslik alus, sh konkreetne seadusest tulenev alus, e-hääle isikustatud kujul e-hääletamise süsteemis säilitamiseks pärast e-hääle vastuvõtmist e-hääletamise süsteemi poolt ning kontrollrakenduses valiku kuvamist. Isikustatud e-hääle säilitamine pärast selle vastuvõtmist kujutab endast keelatud töötlemistoimingu läbiviimist vastustaja poolt ning rikub valimiste salajasuse põhimõtet.

II. ANONÜÜMIMATA E-HÄÄLTE SÄILITAMINE RIKUB VALIMISTE SALAJASUSE NÕUET

17. Põhiseaduse § 60 sätestab, et valimised on üldised, ühetaolised ja otsesed. Hääletamine on salajane. Kuigi need nõuded on sätestatud Riigikogu valimiste kontekstis, siis on need analoogia korras kohaldatavad ka Euroopa Parlamendi valimistele.
18. Täiendavalt sätestab Euroopa Liidu lepingu artikkel 14 lg 3, et Euroopa Parlamendi liikmed valitakse viieaastaseks tähtjaks otsestest ja üldistel valimistel vaba ja salajase hääletuse teel. Ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni lisaprotokoll 1 artiklis 3 on toodud, et protokollisalisel kohustuvad mõistlike ajavahemike järel korraldama salajase hääletamisega vabu valimisi tingimustel, mis tagavad rahva vaba tahteavalduse seadusandja valimisel.
19. Eelnevalt järeldub, et hääletamise salajasus on läbiv nõue nii Eesti kui Euroopa Liidu õiguses, mida täpsustab Euroopa Nõukogu soovitus CM/Rec (2017)5 e-hääletuse standardite kohta, mis on Riigikohtu praktika järgi põhiseaduse tõlgendamisel kohaseks abivahendiks. Põhiseaduse kommenteeritud väljaandes on toodud, et „Hääletamise salajasuse printsiip kaitseb aktiivset valimisõigust ja tähendab seda, et iga hääletaja peab saama hääletada nii, et keegi ei saaks tema vaba tahte vastaselt teada, kuidas ta hääletas ja kas ta üldse hääletas või käis hääletamas“.¹ Hääletamise salajasuse tagamiseks ei tohi ühelgi isikul – sh ka valimiste läbiviijatel – olla võimalik tuvastada, kuidas isik hääletas.
20. E-hääletamise puhul ei ole see nõue praegusel hetkel täidetud, sest vastustaja säilitab isikustatud andmeid valija hääletamiseeliste kohta. Riigikohus on e-hääletuse salajasust varasemalt käsitlenud ning jõudnud järgmisele seisukohale (RKPSJKo nr 3-4-1-13-05, p 19):
„Elektroonilisel hääletamisel teeb hääletaja oma valiku ehk annab hääle, mis šifreeritakse (asetatakse n-õ sisemisse ümbrikusse). Seejärel kinnitab valija oma valiku digitaalallkirjaga ehk šifreeritud häälele lisatakse isikuandmed (n-õ välimine ümbrik). Kuni hääle kokkulugemiseni valimispäeval säilitatakse isikuandmeid ja šifreeritud hääli koos eesmärgiga kindlaks teha, et isik on hääletanud vaid ühe korra. Pärast korduvhääletamise kontrollimist ja korduvhääle eemaldamist eraldatakse isikuandmed šifreeritud häälest. Nn sisemise ümbriku avamine on võimalik üksnes pärast šifreeritud häälele lisatud isikuandmete eemaldamist Vabariigi Valimiskomisjoni liikmetele jaotatud võtmete abil pärast valimisjaoskondade sulgemist. Seega tagab elektroonilise hääletamise süsteem üksnes ühe hääle arvessemineku ühe inimese kohta, kindlustades samas ka hääle salajassejäämist.“ [allajoonimine lisatud]
21. Eelviidatud lõigus toodud väide, nagu oleks n-õ sisemise ümbriku avamine võimalik ainult pärast häälele lisatud isikuandmete eemaldamist, on faktiliselt ebaõige. Riigikohus ei ole selles otsuses ka selgitanud, millel põhineb väide, nagu oleks sisemise ümbriku avamine võimalik ainult pärast isikuandmete eemaldamist.

¹ Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Paragrahv 60, p 40.



22. Valimiste läbiviijal on praktikas võimalik n-ö sisemine ümbrik avada ka ilma isikuandmeid eemaldamata ning tuvastada seeläbi, kuidas iga e-hääle andnud isik on hääletanud. On ilmne, et taoline teguviis ei ole lubatav ning kaebajale ei ole teada, et valimiste läbiviija oleks sellist rikkumist kunagi toime pannud, kuid faktiliselt on seda võimalik teha. Taolist võimalust ei tohiks olemas olla, sest see riivab intensiivselt valimiste salajasuse nõuet.
23. 03.06.2024 jõustuv RKVS § 48³ lg 3 sätestab, et enne elektroonilise hääletamise algust seadistab riigi valimisteenistus elektroonilise hääletamise süsteemi, valijarakenduse ning hääle kontrollrakenduse, loob avalikult elektrooniliste häälte krüpteerimiseks häälte salastamise võtme ja häälte dekrüpteerimiseks häälte avamise võtme. Riigi valimisteenistus jagab häälte avamise võtmele ligipääsu vahendid Vabariigi Valimiskomisjoni liikmete ja riigi valimisteenistuse vahel.
24. Häälte avamise võtmega on võimalik n-ö sisemist ümbriku avada ning tuvastada valija eelistus. Valimiste läbiviimise nõuete kohaselt tuleb nn sisemine ümbrik avada alles pärast seda, kui hääled on anonüümitud ning sealt on isikuandmed eemaldatud, kuid faktiliselt on seda võimalik teha ka ilma hääli anonüümimata.
25. Taoliselt on valimisteenistuse ja valimiskomisjoni töötajate valduses olevate ligipääsuvahenditega võimalik tuvastada kõigi e-hääle andnud valijate poliitilised eelistused. Valijad peavad usaldama, et seda võimalust ei kuritarvitata. Samas ei ole välistatud, et erandlike asjaolude – näiteks ähvarduste, füüsiliste mõjutuste, altkäemaksu, varguse vms – tagajärjel võib häälte avamise võti sattuda isiku kätte, kes soovib häälte salajasust murda. Selle riski ennetamiseks on mõistlik hoiduda häälte säilitamisest viisil, mis võimaldab häält kokku viia valijaga, kes selle hääle on andnud.
26. OSCE demokraatlike institutsioonide ja inimõiguste büroo (ODIHR) moodustas 03.03.2019 toimunud Riigikogu valimiste hindamiseks valimiste eksperdirühma (EET), mis leidis samuti, et e-häälte salajasus ei vasta nõuetele. Ekspertühma töö tulemusena valmis aruanne, kus on e-hääletamise peatükis toodud mh järgmist (**lisa 4, lk 7**):
- „ODIHR EET poolt läbi vaadatud tehnilised raamistikud ja toimingud viitavad asjaolule, et siseründaja, kellel on volitus ligi pääseda digitaalsetele valimiskastidele, võiks murda iga valija poolt avaldatud QR-koodi salajasuse, isegi pärast koodi kehtivuse lõppu. See on vastuolus riiklike seaduste ja rahvusvaheliste standarditega, mis puudutavad hääle salajasust.“ [allajoonimine lisatud] (inglise keeles: „an internal attacker with privileged access to digital ballots could break the vote secrecy of any voter who published an image of the QR code online” – „digitaalsetele valimisedelitele ligipääsu omav siseründaja saaks murda iga sellise valija digitaalse hääle salajasuse, kes avalikustab veebis pildi oma QR-koodist”).
27. OSCE eksperdirühma järeldused kinnitavad, et e-hääletamisel ei ole hääle salajasuse nõue piisavalt tagatud. Siseründajal ehk valimiste korraldamisega seotud ametnikul on võimalik murda iga e-hääle andnud valija hääle salajasus ka valijarakenduse poolt kuvatud ja kontrollrakendusele edastatud QR-koodi vahendusel. Kaebaja soovib vältida riski, et tema poliitiline eelistus muutub avalikuks. Kaebaja palub seetõttu, et kohus keelaks vastustajal säilitada kaebaja e-hääle isikustamist võimaldavaid isikuandmeid pärast e-hääle vastuvõtmist.
28. Kaebaja on näitlikustanud OSCE eksperdirühma järeldusi, luues oma rakenduse e-häälte allalaadimiseks QR-koodi kasutava häälekontrolli käigus, mille tulemusel on võimalik valijal või tema hääle QR-koodile ligipääsu omaval isikul salvestada kontrolliprotseduuri raames digiallkirjastatud hääle piiramatuks ajaks ja võimalusega seda QR-koodis edastatud võtmega dekrüptides murda hääle salajasust. See rakendus töötas ja oli kasutatav ka 2024. aasta e-hääletuse prooviläbimise käigus 22. mail, milles kaebaja veendus oma häälte allalaadimise ja dekrüptimisega. Selline võimalus on vastuolus hääletusperioodil kehtima hakkava RKVS § 48⁶ peamiste hääle salajasuse nõuetega, mille kohaselt „igas hääletamisetapis, sealhulgas pärast



elektroonilise hääle tühistamist, järgitakse hääle salajasuse põhimõtet”, sj iseäranis nõudega, et valijarakendus „peab salastama valija hääle selliselt, et hääle edastamisel ei ole võimalik näha, kelle poolt valija hääletas” ja nõudega, et elektrooniline hääletamine ja häälte lugemine „tuleb korraldada selliselt, et ei ole võimalik luua seost valija ning avatud hääle vahel”.

29. Lisaks on kaebaja koostanud asjatundja arvamuse, mis oli osa Riigikohtu menetluses olnud asja nr 5-23-20 (vt p 42) tõendusmaterjalist, mille jättis Riigikohus sisuliselt läbivaatamata ja milles kaebaja näitab, et praktikas ei pea paika ka kehtima hakkava RKVS § 48⁶ lg 9 nõue, et elektroonilise hääletamise süsteem peab tagama, et „kui valija on hääletanud mitu korda, ei ole võimalik valijal kellelegi tõendada, milline tema antud elektrooniline hääle läks arvesse”. Kaebaja tegi selle kohta ka 2023. aasta oktoobris ettekande e-hääletusele spetsialiseerunud teaduskonverentsil E-Vote-ID, mille järel kinnitas e-hääletuse süsteemi arendava AS Cybernetica esindaja ettekandele järgnenud diskussioonis, et selline puudus süsteemil eksisteerib ning pakkus viisi selle parandamiseks. Kaebajale teadaolevalt pole viga 2024. aasta Euroopa Parlamendi valimisteks parandatud.

III. ANONÜÜMIMATA E-HÄÄLTE SÄILITAMINE RIKUB ISIKUANDMETE KAITSE NÕUDEID

30. **Hääletaja e-hääles sisalduv valik on isikuandmete eriliik, mille töötlemine on keelatud.** Euroopa Liidu põhiõiguste harta artikkel 8 lg-e 1 kohaselt on igapähe õigus oma isikuandmete kaitsele. Isikuandmete kaitse ei piirdu mitte üksnes nende kaitsmises õigusvastase avaldamise eest, vaid ka õiguses kaitsta andmeid õigusvastase töötlemise eest. 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. Vastustaja 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.
31. Ükski e-hääletamise etapi kirjeldus ei loo alust isikustatud e-häält e-hääletamise süsteemis talletada kauem kui see on vajalik e-hääletamise süsteemi poolt e-hääle vastuvõtmiseks (vt ülal p-s 2.4) ja kontrollrakenduses valiku kuvamiseks piiratud aja jooksul. Seetõttu on üldraamistiku p-s 7.6 väidetud vastuoluline, sest pärast hääletamisperioodi lõppemist teostatud häälte tühistamise toiming järel ei tohiks elektroonilise valimiskasti alles jääda isikustatud e-hääled. Täiendavalt on vastuoluline, et kuigi VVK otsuse p 4.10 ja vastustaja andmekaitsetingimused üheselt kõnelevad andmete anonüümimise töötlemisest, siis toimub lugemisele minevate e-häälte, st ainult osade antud e-häälest anonüümimine alles pärast hääletamisperioodi lõppu ja vähemalt enne häälte kokkulugemist (vt ülal p-s 2.4).
32. Riigikohtu hinnangul põhiseaduse tõlgendamisel kohaseks abivahendiks oleva Euroopa Nõukogu soovitusel CM/Rec (2017)5 e-hääletuse standardite kohta rakendusjuhiste IV peatükis toodud nõuetest hääletamise salajasuse tagamiseks ei täida kaebaja hinnangul e-hääletuse süsteem punktide 19-26 täielikult ühtegi ning on otseses vastuolus nõudmistega 23, 25 ja 26.
33. 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 andmetööstustoiming. Andmete töötlemisahelas toimuv igasugune tööstustoiming nõuab eraldiseisvat õiguslikku alust. Vastustajal puudub kehtivast õigusest tulenev alus andmete



eriliikide töötlemiseks. Isikustatud e-hääle säilitamine pärast selle vastuvõtmist e-hääletamise süsteemi poolt on andmetöötlustoiminguna keelatud.

34. E-hääle vastuvõtmisega seotud andmetöötlustoimingute loogika ja tingimused tuleb tuletada mitme allika kaasabil. RKVS § 48⁴ kirjeldatud elektroonilise hääletamise kord, VVK otsuse p 4.5, üldraamistikus kirjeldatud etapid ning riigi valimisteenistuse andmekaitsetingimused on loogilises kattuvuses, sh õiguslikus käsitluses. Ükski andmetöötluse eesmärk, selle saavutamiseks vajalik andmete koosseis ega töötlustoiming ei kirjelda e-hääle säilitamist selliselt, et nõutav oleks e-hääle seostamine valija isikuga pärast e-hääle vastuvõtmist ja kogu järgneval valimisperioodil.
- 34.1. Esiteks, RKVS § 48⁴ lg 2 loob õigusliku aluse valija tuvastamiseks. VVK otsuse p 4.5.1 täpsustab ja määratleb andmetöötlustoimingu eesmärgi ja selleks vajalike andmete koosseisu (vt ülal p-s 2.3). Üldraamistik kirjeldab seda tuvastamisfaasis (vt ülal p-s 2.4).
- 34.2. Teiseks, võimaldavad RKVS § 48⁴ lg-ed 3 ja 4 teha valijal vabalt valitud kandidaadi poolt valik. VVK otsuse p 4.5.2 täpsustab ja määratleb täpselt eesmärgi ja andmete koosseisu, milliseid andmeid e-hääle kinnitamiseks ja salvestamiseks töödeldakse (vt ülal p-s 2.3). Üldraamistik kirjeldab seda hääletamisfaasis (vt ülal p-s 2.4).
- 34.3. Kolmandaks, võimaldab RKVS § 48⁴ lg 5 anda valijale kinnituse e-hääle vastuvõtmise kohta, mida täpsustab andmetöötluse eesmärgi ja andmete koosseisu kohta VVK otsuse p 4.5.3 (vt ülal p-s 2.3). Üldraamistikus kirjeldatakse seda kontrollimisfaasis (vt ülal p-s 2.4).
35. Tulenevalt VVK otsuse p-st 4.5 tuleb andmetöötlust toimetada viisil, mis võimaldab nende logimist. Kaebaja hinnangul tuleb logimise tõlgendamisel piirduda sellele tähenduse andmisel, kas kirjendamise või ülestähendamisega. Vastustaja andmekaitsetingimustest kohaselt töödeldakse üksnes hääletamise fakti ja anonüümitud valikut. Samasugune nõue e-hääle anonüümitult töötlemiseks tuleb VVK otsuse p-st 4.10. Andmete anonüümimine tähendab teabest kõikide jälgede kaotamist, mis võiksid viia tuvastatavate isikuteni. Kui pseudonüümimine ja krüptimine (krüpteerimine) on tagasipööratav umbisikustamine, siis anonüümimine tähendab tagasipööramatut ehk lõplikku umbisikustamist. E-häälte töötlemisel võib seega neid töödelda üksnes anonüümitud kujul pärast nende vastuvõtmist e-hääletamise süsteemi poolt.
36. E-hääle registreerimiseks kehtestatud andmetöötlustoimingud ja nendega saavutatavad eesmärgid on eeltoodust tulenevalt üksikasjaliku detailsusega VVK otsuses kirjeldatud. E-hääle edastamise protseduur ja sellest tulenevad andmetöötlustoimingud ei näe ette isikustatud e-hääle säilitamist e-hääletamise süsteemis. Seetõttu on mõistlikult järeldatav, et VVK otsuse p 4.5 viitab andmete logimisele (kirjendamisele) ning vastustaja töötleb üksnes andmeid hääletamise fakti ja anonüümitud valiku kohta. Seejuures on oluline märkida, et seadus ei näe elektroonilise hääletamise korras vaidlusalust töötlustoimingut ette ning vastustaja ega VVK ei saa seda omal initsiatiivil kehtestada. Vastustajat tuleb kohustada hoiduma vaidlusalusest andmetöötlustoimingust.
37. **Eriliiki isikuandmete töötlemisel tuleb järgida ettevaatuspõhimõtet.** Eriliiki isikuandmete töötlemine on keelatud, kuivõrd see hõlmab äärmiselt tundlikku teavet, mille ilmsikstulek võib andmesubjekti õigustele ja vabadustele kujutada suurt ohtu. Edasine mõju võib andmesubjektile kaasa tuua olulise varalise või mittevaralise kahju. Sellest tulenevalt on isikuandmete eriliikide töötlemise juhud äärmiselt erandlikud.
38. Riigivastutuse seaduse § 5 lg-e 1 kohaselt võib nõuda halduse toimingu sooritamata jätmist, kui haldusakt või toiming rikuks tema õigusi ja tooks tõenäoliselt endaga kaasa tagajärje, mida ei saaks kõrvaldada haldusakti või toimingu hilisemal vaidlustamisel. Kaebaja hinnangul tuleb isikuandmete eriliikide põhjendamatul töötlemisel lähtuda andmesubjekti huve teenivast ettevaatuspõhimõttest. Täiendavalt tuleb järgida IKÜM artikkel 5 lg 1 p-s c sätestatud



võimalikult väheste andmete kogumise põhimõtet, mille kohaselt peavad isikuandmed olema piiratud sellega, mis on vajalik nende töötlemise eesmärgi seisukohalt. Vastustajal ei ole valimiste läbiviimiseks vajalik säilitada kaebaja ega teiste valijate anonüümimata e-hääli. Seda kinnitab asjaolu, et välisriikide praktikas ei säilitata anonüümimata e-hääli mh põhjusel, et see loob ebamõistliku riski. Näiteks Šveitsi e-hääletamisel ei säilita valimiste korraldaja isikuandmeid, mis võimaldaksid valijat tema antud häälega seostada.

39. Kaebaja leiab, et olukorral, mis seisneb eriliigiliste isikuandmete õigusvastases töötlemises, on iseenesest andmete ilmsikstuleku tõenäosust suurendav mõju. See kujutab endast riski ehk tegevust, mis soodustab mõne muu tegevuse või tegevusetuse tagajärjel andmete võimalikku õigusvastast avaldamist. Sellist andmetöötlust tuleb kohelda ennetava ettevaatusega, et välistada põhjendamatu ja õigusvastase toiminguga tagajärjel võimalik kahju tekkimine. Seetõttu tuleks kaebaja õiguskaitse vajadust jaatada olukorras, kus õigusrikkumise tagajärg ei ole veel realiseerunud ega objektiivselt mõõdetav. Tänapäevases poliitiliselt polariseerunud maailmas on isiku poliitiline või filosoofiline veendumus kõnekas fakt või asjaolu, mille ilmsikstulek mõjutab kindlasti ühiskonna tunnetust ja suhtumist isikusse ja võib isikule kaasa tuua pöördumatu kahju.
40. Majandus - ja Kommunikatsiooniministeerium tellis 11.05.2022 KMPG Baltics OÜ-lt auditi “Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse terviklik auditeerimine ja hindamine Majandus- ja Kommunikatsiooniministeeriumile” (edaspidi **audit**) (**lisa 3**). Audit tuvastas, et turvatestimise protsessi kirjeldus on puudulik. Viimast kirjeldati järgmiselt: *VIS3 ja EHS puudulike turvatestimise läbiviimise protsesside kirjelduste tõttu võivad olulised turvanõrkused jääda õigeaegselt tuvastamata. Tuvastamata turvanõrkused võivad tulevikus kompromiteerida e-valimiste infosüsteeme ning seetõttu ei ole võimalik e-häält anda* (vt lisa 3, lk 17 - Tähelepanek 1). Samuti tuvastati puudused riskianalüüside läbiviimisel, mille kirjelduses märgiti järgmist: *ilma põhjaliku riskianalüüsi ei võimalik tuvastada ega ennetada riske, mida vastava analüüsi läbiviimise käigus oleks võimalik tuvastada ning neile reageerida. Riskide mitte käsitlemine võib negatiivselt mõjutada e-valimiste läbiviimise protsesside ja süsteemide toimivust ning turvalisust* (vt lisa 3, lk 18 - Tähelepanek 3).
41. Kaebaja nõustub auditis esitatud järeldustega ning leiab täiendavalt, et kirjeldatud riskide riskiklasside määramine “keskmiseks” on kahetsusväärset madal. Iseenesest puudused riskide kindlakstegemisel viitavad, et teave võimalike ohtude ja süsteemi nõrkuste kohta on vähene. See omakorda ei võimalda anda süsteemile endale terviklikku hinnangut selle kasutamiseks eriliiki isikuandmete töötlemisel. Kuigi kaebajale on teada välisekspertide teadusartikleid,² mis osutavad e-hääletuse süsteemi tervikliku turvamudeli ja „selgete turvanõuete puudumisele“, ei väida kaebaja kaebuse kontekstis, et e-hääletamise süsteem sisaldab turvanõrkusi. Sellegipoolest ei tuleks alahinnata riskianalüüside põhjalikku koostamist ning ohtude igakülgset kindlakstegemist ja hindamist, kuivõrd ilma selleta ei saa kindlaks teha ühegi süsteemi usaldusväärsust. Kaebaja on seisukohal, et õigusvastase andmetöötluse lubatavus ei saa olla sõltuvuses turvalisuse küsimusest.
42. Samuti ei nähtu avalikest allikatest, et e-hääletamise süsteemi kohta oleks vastustaja isikuandmete vastutava töötlejana koostanud IKÜM artikkel 35 kohase andmekaitsealase mõjuhinnangu. Kui teatavat tüüpi isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise tulemusena ning isikuandmete töötlemise laadi, ulatust, konteksti ja eesmarke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht, hindab

² „Vea avastasid Austraalia ja Prantsusmaa ülikoolide krüptograafid, kes informeerisid sellest meie e-hääletuse arendajaid, nii et viga jõuti enne valimisi parandada. Kuid autorid ütlevad 2023. aasta lõpul avaldatud teadusartiklis, et see turvaauk oli eriti murettekitav, sest viga oleks pidanud hakkama silma ka süsteemi lähtekoodiga tutvumata. Nende hinnangul sai olla selline viga siiani avastamata auditeeritavuse viletsa taseme ja selge turvamudeli puudumise tõttu. Kuna Eesti e-hääletuse lähtekood vastab autorite hinnangul vaid ühele üheksast väljatoodud arendusstandardist, siis oletavad nad oma avastust üldistades, et sarnaseid puudusi on süsteemis veel.” <https://arvamus.postimees.ee/7989447/mart-poder-e-valimiste-turvalisus-on-illusioon>



vastutav töötaja enne isikuandmete töötlemist kavandatavate isikuandmete töötlemise toimingute mõju isikuandmete kaitsesele (IKÜM artikkel 35 lg 1). Arvestades, et viimastel 2023. aasta Riigikogu valimistel loeti kehtivalt kokku 312 182 e-häält, mis viitab ulatuslikule tundlikku teabe töötlemisele ja sellest johtuvalt võib kujutada suurt ohtu, on mõjuhinnangu koostamine enne isikuandmete töötlemist kohustuslik.

43. Riigikohus on sedastanud, et kui isiku õiguste rikkumisega võib kaasneda pöördumatuid tagajärgi, võib isik oma õigusi rikkuva toiminguga sooritamata jätmist ennetavalt nõuda ka siis, kui selleks on muu põhjendatud huvi (RKHKo 3-3-1-3-04 p 13). Kaebaja hinnangul ei ole põhjendatud taluda vastustaja toiminguga kaasnevat kaebaja õiguste rikkumist. Samas soovib kaebaja kasutada riigi poolt võimaldatud hüve, mis seisneb elektroonilises hääletamises. Õigusriigi ja seaduslikkuse põhimõtete valguses oleks põhjendamatu asuda seisukohale, et riik jätab kaebajale valiku, kas hääletada elektrooniliselt, millega kaasneb kaebaja õiguste õigusvastane rikkumine ja tõenäosuse suurenemine kaebajale suure ohu tekkimiseks, või alternatiivselt riivist hoidumiseks hääletada hääletussedeliga valimispäeval. Igal juhul puudub riigil õigus riigielu õigusvastaselt tegutsedes korraldada. Riik peab olema oma kodanikele eeskujuks nii oma sisekorralduse organiseerimisel kui ka oma tegevustes, millel on vahetu puutumus kodanikega.
44. Kaebaja selgitab, et käesoleval juhul ei ole tegemist EPVS § 66 lg-e 1 kohase kaebusega, kuivõrd selles kirjeldatud kaebuse esitamise eelduseks on juba toimunud õigusrikkumisega või seaduse rikkumisega seotud asjaolude vaidlustamine. Käesoleva kaebusega taotleb kaebaja tulevikus kaebajale tekkiva õigusrikkumisest hoidumist ja seda põhjustava toimingust hoidumist. Eeltoodut arvesse võttes leiab kaebaja, et käesoleva kaebuse aluseks olevad asjaolud ja nõue toimingust hoidumiseks on põhjendatud.

IV. ESIALGSE ÕIGUSKAITSE TAOTLUS

45. Halduskohtumenetluse seadustiku (HKMS) § 249 lg-e 1 kohaselt võib kohus kaebaja taotlusel või omal algatusel teha määruse esialgse õiguskaitse kohta, kui vastasel juhul võib kaebaja õiguste kaitse kohtuotsusega osutada oluliselt raskendatuks või võimatuks. Esialgse õiguskaitse määrusega võib kohus keelata vaidlustatava toiminguga tegemise (HKMS § 251 lg 1 p 2).
46. Kaebaja vaidlustatavaks toiminguks on Riigi valimisteenistuse (vastustaja) poolt valija isikuga seotud poliitilist eelistust sisaldava e-hääle töötlemine, mis seisneb selle isikustatud kujul säilitamises e-hääletamise süsteemis pärast e-hääle vastuvõtmist e-hääletamise süsteemi poolt. Kaebaja e-hääles sisalduv teave tema valiku kohta on käsitatav isikuandmete eriliigina (IKÜM artikkel 9 lg 1). Kaebaja e-hääle säilitamine anonüümimata kujul on ühtlasi vastuolus valimiste salajasuse põhimõttega ning tekitab riski, et kolmandad isikud saavad teada kaebaja valimiste käigus väljendatud poliitilise eelistuse.
47. Kaebuse eesmärk on keelata isikustatud e-hääle säilitamise toiminguga tegemist. Esialgse õiguskaitse taotluse eesmärk on välistada vastustajal kaebaja e-hääle isikustatud kujul säilitamine ajaks, kui käesolevas asjas pole veel lõplikku lahendit. Riigikohus on selgitanud, et esialgse õiguskaitse kohaldamiseks peab kaebajat ähvardama tagajärg, mille kõrvaldamine põhiasjas tehtava hilisema kohtulahendiga on võimatu või ebamõistlikult raske (RKHKo 3-3-1-19-17 p 15).
48. RKVS § 48² lg-e 1 kohaselt haldab vastustaja e-hääletamise süsteemi. Vastustaja tegutseb e-hääle töötlemisel vastutava töötlejana IKÜM artikkel 4 p 7 mõttes. Kaebaja leiab, et vastustajal puudub seadusest tulenev alus valija isikustatud e-hääle säilitamiseks elektroonilise hääletamise süsteemis pärast e-hääle vastuvõtmist e-hääletamise süsteemi poolt. Vabariigi Valimiskomisjoni 09.02.2024 kehtestatud otsuse nr 95 "Tehnilised nõuded elektroonilise hääletamise korraldamise üldpõhimõtete tagamiseks" p-de 4.5.1 kuni 4.5.3 kohaselt toimub



üksnes isikuandmete logimine ehk kirjendamine. Sama otsuse p 4.10 kohaselt on e-hääled anonüümsed ja neid tuleb töödelda anonüümselt. Vastustaja teavitab avaldatud andmekaitsetingimuste p 1 kohaselt, et valimiste infosüsteemi edastatakse üksnes elektrooniliselt hääletanute hääletamise fakt ja anonüümitud valik.

49. Seejuures kirjeldab vastustaja poolt kehtestatud e-hääletamise süsteemi kirjeldav dokumentatsioon e-hääletamise süsteemi toimimist sellisel, et pärast e-hääle vastuvõtmist e-hääletamise süsteemi poolt salvestatakse e-haal isikustatuna valija isikuga e-hääletamise süsteemis, sh kogu eelhääletamise perioodi kestel ja vähemalt kuni ajani, mis jääb hääletamisperioodi lõppemise ja häälte kokkulugemise vahele (vt lisa 1, üldraamistik p 7.6). Sellest johtuvalt väljub isikuandmete töötlemine selle aluseks olevast õiguslikust raamistikust.
50. Kaebaja leiab, et arvestades käesoleva esialgse õiguskaitse taotluse aluseks oleva kaebuse esitamise kuupäeva ja kaebaja e-hääle andmise vahele jäävat lühikest ajaperioodi, ei jõua kohus eelduslikult asjas sisulise lahendini enne eelhääletamise (s.o elektrooniline hääletamise) perioodi algamist ega ka selle toimumise ajal. Kaebaja isikuga seotud e-hääle säilitamine e-hääletamise süsteemis on keelatud ja seetõttu on tegemist õigusvastase andmetöötlusega, mis kujutab kaebajale põhjendamatu õigusriivet. Andmetöötlusest hoidumist ei ole vastustajalt võimalik tagasiulatuvalt nõuda. Kaebaja minevikus toimunud õiguste rikkumist on võimatu kaebaja nõude rahuldamisega tagasi pöörata. Kohtul tuleks sellisel juhul kaebus jätta läbi vaatamata, kuivõrd kaebuse rahuldamisega ei ole võimalik saavutada kaebuse eesmärki (HKMS § 151 lg 2 p 1 koosmõjus § 121 lg 2 p 2). Seega jääks kaebaja ilma õiguskaitsest, mis on käesoleva esialgse õiguskaitse taotluse esitamise ajendiks.
51. Esialgse õiguskaitse korras kaebaja esitatav taotlus toimingust hoidumiseks on proportsionaalne. Riigikohus on selgitanud, et esialgset õiguskaitset tuleb kohaldada vaid niipalju, kui see on vajalik kaebaja õiguste kaitseks. Kaebaja õiguste kõrval tuleb samaväärselt arvestada ka avalike huvidega ja võimalike kolmandate isikute õigustega. Kohtu ülesanne on prognoosida nii esialgse õiguskaitse taotluse rahuldamata jätmise kui ka kohaldamise tagajärgi (RKHKo 3-20-349/51 p 11). Kaebaja hinnangul ei ole isikuandmete säilitamise toimingut keelamisel ülemäärast mõju teistele isikutele ega avalikele huvidele. Samuti ei koorma vaidlusalusest toimingust hoidumine vastustajat ülemääraselt.

V. MENETLUSLIKUD KÜSIMUSED

52. Kaebaja soovib asja läbivaatamist kohtuistungil.
53. RLS § 60 lg 1 kohaselt tuleb halduskohtule kaebuse esitamisel tasuda riigilõiv 20 eurot. Täiendavalt tuleb RLS § 60 lg 6 kohaselt tasuda esialgse õiguskaitse taotluse esitamiselt riigilõivu 20 eurot. Kaebajal tuleb seega tasuda riigilõivu kokku 40 eurot.

Lisad:

1. Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel;
2. Riigi valimisteenistuse andmekaitsetingimused;
3. KPMG OÜ audit e-valimiste infosüsteemi kohta;
4. ODIHR EET aruanne.

Lugupidamisega

(allkirjastatud digitaalselt)



Märt Mürk