Vabariigi Valimiskomisjon
13. June 2024

Kaebaja: **Märt Põder**
isikukood: 37909110298

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

KAEBUS
toimingu õigusvastaseks tunnistamiseks

RESOLUTSIOON:

1. **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.**

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. E-häälte töötlemine isikustatud kujul on seetõttu ebaseaduslik.
3. **Faktilised asjaolud.** Euroopa Parlamendi valimisnädal toimub alates 3. juunist 2024 kell 9.00 kuni 9. juuni 2024 kella 20.00-ni. Elektrooniline hääletamine (edaspidi ka **e-hääletamine**) algab 3. juunil kell 9.00 ja kestab kuni 8. juunini kella 20.00-ni (edaspidi ka **hääletamisperiood**).

4. Kaebaja andis oma e-hääle 03.06.2024 (**lisa 1**).

5. RKVS § 48^6 lg 5 sätestab, et Elektroonilise hääletamise süsteemis logitakse elektroonilise hääletamise ajal vähemalt järgmised toimingud:

5.1. valija tuvastamisel: valija nimi ja isikukood, hääletamise alustamise kuupäev ja kellaaeg, internetiprotokolli aadress, valija valimisringkond ning internetiprotokolli aadressile vastav asukohariik;

5.2. elektroonilise hääle kinnitamisel ja salvestamisel: hääletamise lõpetamise kuupäev ja kellaaeg, sertifikaatide väljaandja ning teave sertifikaatide kehtivuse kohta;

5.3. elektroonilise hääle õigsuse kontrollimisel: kontrollimise lõpetamise kuupäev ja kellaaeg, internetiprotokolli aadress ning internetiprotokolli aadressile vastav asukohariik.

6. RKVS § 48^6 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 kaebaja häält säilitatakse anonüümimata kujul vähemalt viis päeva.

7. Täiendavalt sätestab RKVS § 48^6 lg 7, et anonüümimata logid hävitab riigi valimisteenistus RKVS § 77^1 lg-s 2 sätestatud tähtajal ehk mitte varem kui üks kuu alates valimispäevast. Nähtub seega, et kaebaja anonüümimata e-häält säilitatakse vähemalt kuu aega.

8. 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 2**). 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 2 p 7.6). Viimases etapis loetakse hääled kokku (vt lisa 2 p 7.7).

9. Riigi valimisteenistuse poolt avaldatud andmekaitsetingimustes teavitatakse, et valimiste valdkonnas on isikuandmete 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 3**).

10. 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. Valimiste korraldaja valdusesse jäävad aga endiselt vähemalt kuuks ajaks ka anonüümimata e-hääled. Anonüümimata hääled hävitatakse alles pärast RKVS § 77^1 lg-s 2 sätestatud tähtaega.

11. Eelnevast järeldub, et kaebaja 03.06.2024 häält säilitatakse anonüümimata kujul vähemalt kuu aega.

12. Isikute poliitiliste eelistuste andmete säilitamine niivõrd pika perioodi jooksul (või üldse) ei ole proportsionaalne, sest see rikub isikuandmete 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 häältega DVD-plaat satub valedesse kätesse, 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.

13. Kaebaja tõi 2023. aasta Riigikogu valimistel välja olulisi puudusi arvutisüsteemide seadistamisel, mida kasutati valimissaladuse tagamise olulisimaks turvagarantiideks olevate elektrooniliste häälte salastamise võtme ja häälte avamise võtmete loomisel ja häälte kokkulugemisel. Kuna valimiste korraldajad ei pea nõutavaks ega vajalikuks operatsioonisüsteemi ja tarkvara räside 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 tagatisi kaebaja hääle salajasuse tagamisel.

14. Kaebaja e-hääle säilitamine niivõrd pika perioodi jooksul ei ole seaduspärane. 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

15. 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.

16. Täiendavalt sätestab Euroopa Liidu lepingu artikkel 14 lg 3, et Euroopa Parlamendi liikmed valitakse viieaastaseks tähtajaks otsestel ja üldistel valimistel vaba ja salajase hääletuse teel. Ka Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni lisaprotokolli 1 artiklis 3 on toodud, et protokolliosalised kohustuvad mõistlike ajavahemike järel

korraldama salajase hääletamisega vabu valimisi tingimustel, mis tagavad rahva vaba tahteavalduse seadusandja valimisel.

17. Eelnevast 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 valija hääletas.

18. E-hääletamise puhul ei ole see nõue praegusel hetkel täidetud, sest valimiste läbiviija säilitab isikustatud andmeid valija hääletamiseelistuse 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-ö sisemisse ümbrikusse). Seejärel kinnitab valija oma valiku digitaalallkirjaga ehk šifreeritud häälele lisatakse isikuandmed (n-ö välimine ümbrik). Kuni häälte kokkulugemiseni valimispäeval säilitatakse isikuandmeid ja šifreeritud hääli koos eesmärgiga kindlaks teha, et isik on hääletanud vaid ühe korra. Pärast korduvhääletamise kontrollimist ja korduvhäälte eemaldamist eraldatakse isikuandmed šifreeritud häältest. 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]

19. Eelviidatud lõigus toodud väide, nagu oleks n-ö sisemise ümbriku avamine võimalik ainult pärast häälele lisatud isikuandmete eemaldamist, on faktiliselt ebaõige. Riigikohus ei ole selles otsuses välja toonud, millel põhineb väide, nagu oleks sisemise ümbriku avamine võimalik ainult pärast isikuandmete eemaldamist.

20. 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.

21. RKVS § 48^3 lg 3 sätestab, et enne elektroonilise hääletamise algust seadistab riigi valimisteenistus elektroonilise hääletamise süsteemi,

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

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.

22. Häälte avamise võtmega on võimalik n-ö sisemist ümbrikku 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.

23. 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.

24. 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. Eksperdirühma 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”).

25. 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 ei soovi, et tema poliitiline eelistus muutub avalikuks.

26. 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 hääl 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 RKVS § 48^6 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".

27. Lisaks on kaebaja koostanud asjatundja arvamuse, mis oli osa Riigikohtu menetluses olnud asja nr 5-23-20 (otsuse p 42) tõendusmaterjalist, mille jättis Riigikohus sisuliselt läbivaatamata ja milles kaebaja näitab, et praktikas ei pea paika ka RKVS § 48^6 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 hääl 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

28. **Hääletaja e-hääles sisalduv valik on isikuandmete eriliik, mille töötlemine on keelatud.** Euroopa Liidu põhiõiguste harta artikkel 8 lg-e 1 kohaselt on igaühel 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. 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.

29. 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 ja kontrollrakenduses valiku kuvamiseks piiratud aja jooksul. Seetõttu on üldraamistiku p-s 7.6 väidetu vastuoluline, sest pärast hääletamisperioodi lõppemist teostatud häälte tühistamise toimingu järel ei tohiks elektroonilisse

valimiskasti alles jääda isikustatud e-hääled. Täiendavalt on vastuoluline, et kuigi RKVS § 48[6] kohaselt tuleb igas hääletamisetapis järgida hääletamise salajasuse põhimõtet, toimub lugemisele minevate e-häälte, st ainult osade antud e-häältest, anonüümimine alles pärast hääletamisperioodi lõppu ja vähemalt enne häälte kokkulugemist.

30. 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.

31. 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.

32. 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.

33. Kaebaja hinnangul tuleb logimise tõlgendamisel piirduda sellele tähenduse andmisel, kas kirjendamisega või ülestähendamisega. Andmekaitsetingimustest kohaselt töödeldakse üksnes hääletamise fakti ja anonüümitud valikut. Andmete anonüümimine tähendab teabest kõikide jälgede kaotamist, mis võiksid viia tuvastatavate isikuteni. Kui pseudonüümimine ja 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.

34. E-hääle edastamise protseduur ja sellest tulenevad andmetöötlusoimingud ei näe ette isikustatud e-hääle säilitamist e-hääletamise süsteemis.

35. **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.

36. 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. Valimiste läbiviijal 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.

37. 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 toimingu 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.

38. Majandus - ja Kommunikatsiooniministeerium tellis 11.05.2022 KPMG Baltics OÜ-lt auditi “Valimiste infosüsteemide ja nendega seotud protsesside turvalisuse terviklik auditeerimine ja hindamine Majandus- ja Kommunikatsiooniministeeriumile” (edaspidi **audit**) (**lisa 5**). 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 5, lk 17 - Tähelepanek 1). Samuti tuvastati puudused riskianalüüside läbiviimisel, mille kirjelduses märgiti järgmist: *ilma põhjaliku riskianalüüsita ei võimalik tuvastada ega ennetada riske, mida vastava analüüsi läbiviimise käigus oleks võimalik tuvastada ning neile reageerida. Riskide mittekäsitlemine võib negatiivselt mõjutada e-valimiste läbiviimise protsesside ja süsteemide toimivust ning turvalisust* (vt lisa 5, lk 18 - Tähelepanek 3).

39. Kaebaja nõustub auditis esitatud järeldustega ning leiab täiendavalt, et kirjeldatud riskide riskiklasside määramine “keskmiseks” on kahetsusväärselt 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.

40. 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 eesmärke arvesse võttes tekib tõenäoliselt füüsiliste isikute õigustele ja vabadustele suur oht, hindab vastutav töötleja enne isikuandmete töötlemist kavandatavate isikuandmete töötlemise toimingute mõju isikuandmete kaitsele (IKÜM artikkel 35 lg 1). Arvestades, et viimastel 2023. aasta Riigikogu valimistel loeti kehtivalt kokku 312 182 e-häält, mis viitab ulatuslikule tundliku teabe töötlemisele ja sellest johtuvalt võib kujutada suurt ohtu, on mõjuhinnangu koostamine enne isikuandmete töötlemist kohustuslik.

IV. TEGEMIST ON VALIMISKAEBUSEGA

41. Ennetamaks võimalikku vastuväidet kaebeõiguse puudumise kohta toob kaebaja välja, et siinses dokumendis toodu on valimiskaebus EPVS § 67 lg 1 mõistes. EPVS § 67 lg 1 kohaselt on kaebus taotlus, mille eesmärk on tunnistada seadusvastaseks valimiste korraldaja toiming. Toiming on HMS § 106 lg 1 kohaselt haldusorgani tegevus, mis ei ole õigusakti andmine ja mida ei sooritata tsiviilõigussuhtes. Anonüümimata e-hääle hoidmine on haldusorgani tegevus. See ei kujuta endast haldusakti ning seda ei sooritata tsiviilõigussuhtes. Tegemist on seega toiminguga, mida on võimalik EPVS-s toodud korras vaidlustada.

Lugupidamisega

(allkirjastatud digitaalselt)

Märt Mürk

[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

Lisad:
1. Kaebaja 03.06.2024 antud e-hääle digifail;
2. Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel;
3. Riigi valimisteenistuse andmekaitsetingimused;
4. ODIHR EET aruanne;
5. KPMG OÜ audit e-valimiste infosüsteemi kohta;
6. Volikiri.