Riigikohtu põhiseaduslikkuse järelevalve kolleegium
5-26-45

20.11.2026

Dokumendi esitaja:

Kaebuse esitaja:	**MTÜ Ausad Valimised** (registrikood 80339095)
Kaebuse esitaja:	**Märt Põder** (isikukood 37909110298) e-post: tramm@p6drad-teel.net Postiaadress: Jakobi tn 13-2, Tartu linn, Tartu linn, Tartu maakond

AVALDUSE TÄIENDUS

Kuigi meile kui menetlusosalistele ei ole vaatamata 12.11 taotlusele jätkuvalt kättesaadavaks tehtud ühtegi 11.11 menetlusse kaasatud viiest dokumendist ega 18.11 menetlusse kaasatud õigusanalüüsi, jätkame VVK esitatud väidetele vastamist meile kättesaadava teabe põhjal. Kasutame seejuures kaebaja poolt 16.11 iseseisvalt avastatud ja Riigikogu dokumendiregistris osaliselt avaldatud "iOS ja Android m-valijarakenduste tervikluse auditit", millega oleme nüüdseks saanud tutvuda (LISA 1).

iOSi mobiilirakenduse tervikluse kontroll ebaõnnestus

Kohus küsis 17.11 VVK-le esitatud kohtunõude küsimustes 2-3, milline on rakenduspoodide roll lõpliku valijarakenduse faili valmimisel ning mil määral on vaatlejatel võimalik vaadelda või testida rakenduspoodides levitatavaid valijarakendusi koos seal programmeeritud võimalike lisandustega. VVK vastas 18.11, et "rakenduspood rakendust ei muuda ega täienda" ning "rakenduspoest alla laaditava valijarakenduse erinevus riigi valimisteenistuse poolt üles laadimiseks saadetud valijarakendusest ilmneks auditeerimisel" (vastus küsimusele 2, lk 1-2). Mõlemad väited on vastuolus KPMG valijarakenduste tervikluse auditi tulemustega.

KPMG aruande kohaselt muudab Apple rakenduse käivitatavat koodi, rakendades sellele enne App Store'i kaudu levitamist FairPlay-krüpteeringut (punkt 2.4 alapunkt 3, lk 7). KPMG-l ei õnnestunud seda koodi dekrüpteerida (punkt 2.4 alapunkt 2, lk 7; punkt 3.2, lk 10). Selle asemel kontrollis KPMG Riigikogu Kantselei poolt talle edastatud rakenduspaketti, kuid ei suutnud kontrollida, kas selles kontrollitud kood vastab App Store'ist alla laaditud rakenduspaketis sisalduvale krüpteeritud koodile (punkt 2.4 alapunkt 3, lk 7-8). Seega ei suutnud KPMG kontrollida, kas App Store'ist alla laaditud valijarakendus vastab RVT poolt üleslaadimiseks edastatud valijarakendusele. Auditiaruande avalik versioon ei selgita, kuidas oleks võimalik selline kontroll lõpule viia, ning VVK ei ole oma vastuses lahendust tutvustanud. Aruandes kirjeldatud tingimustes puudub seega nii audiitoritel kui ka vaatlejatel tõendatult toimiv võimalus sõltumatult kontrollida App Store'i kaudu levitatava iOSi valijarakenduse käivitatavat koodi, sealhulgas levitamise käigus tehtud võimalikke lisandusi.

VVK osutab oma 6.11 vastuses kohtunõudele, et 2025. aastal jäi mobiilihääletuse lubamise otsustamisel

ebaselgeks, kas "rakenduste poodide kaudu levitatavate rakenduste terviklust on võimalik kontrollida". Kuigi VVK väidab, et "2026. aastal oli komisjonil võimalik tutvuda juba tehtud auditi tulemuste ja piirangutega", näitab KPMG raport, et valijarakenduse tervikluse kontrollimise võimalikkust App Store'is ei ole endiselt võimalik tõendada. Seega ei ole raporti põhjal võimalik kinnitada, et iOSi valijarakenduse kasutamisel oleks rakenduse terviklus tagatud viisil, mis võimaldab selle turvalist ja töökindlat kasutamist valimiste läbiviimisel. VVK-l puudus seetõttu piisav alus iOSi opsüsteemi valijarakenduse loomiseks 29.10 otsusega nr 105 kehtestada.

Mobiilirakenduste tervikluse kontrolli puudulikkus mõjutab ka kontrollrakendusi

VVK kinnitab oma 18.11 vastuses, et "valijarakenduste puhul on keskne küsimus rakenduste autentsuse ja tervikluse tagamine" ning RVT ülesanne on tagada, et "rakenduste levitamise käigus ei oleks neid lubamatult muudetud". RKVS §48³ lg7 järgi ei piirdu see kohustus valijarakendusega, vaid RVT on kohustatud enne valimisi avaldama "valijarakenduse, hääle kontrollrakenduse ning veebilehe autentsuse ja tervikluse tagamiseks vajalikud andmed".

VVK 29.10 otsusega nr 105 kinnitati ka hääle kontrollrakenduste loomine Androidi ja iOSi mobiiliseadmete opsüsteemidele. Kui iOSi valijarakenduse terviklust App Store'is ei olnud võimalik auditiga tõendada ning, nagu märkisime oma 19.11 avalduses, võib eri Androidi opsüsteemi kohanduste kontekstis olla ebapiisav rakenduspoodides avaldatud valijarakenduste tervikluse kontroll, siis tähendab see, et samadel põhjustel ei ole tõendatult tagatud ka hääle kontrollrakenduste terviklus ning kasutamise turvalisus.

Hääle kontrollimise võimalus on RKVS § 48¹⁰ kohaselt elektroonilise hääletuse lahutamatu osa ning valijal peab olema võimalik kontrollida oma häält kogu eelhääletamise ajal. Hääle kontrollrakenduse töötab välja RVT ning avalikustab RKVS § 48³ lg 7 kohaselt selle autentsuse ja tervikluse tagamiseks vajalikud andmed. Kui nende andmete abil ei ole võimalik kontrollrakenduse autentsust või terviklust sisuliselt kontrollida või ei ole see valijale mõistlikul viisil tagatud, ei ole turvaliselt ja töökindlalt tagatud ka RKVS § 48¹⁰ kohane elektroonilise hääle kontrollimise võimalus. Seega puudus VVK-l piisav alus kehtestada oma 29.10 otsusega nr 105 Androidi ja iOSi mobiiliseadmete opsüsteeme kontrollrakenduste loomiseks.

Turvariskide ja maandamise meetmete ebapiisav käsitlemine

Oma 11.11 täiendavates selgitustes kinnitab VVK, et komisjon tutvus 29.10 koosolekul asjakohaste materjalidega, arutas tuvastatud riske ning tegi selle põhjal otsuse. Kaebajad tõid VVK 29.10 koosoleku eel esitatud järelevalvetaotluses välja üle kümne avaldatud raporti või artikli, milles kirjeldatud puudused võivad välistada valijarakenduse ja hääle kontrollrakenduse loomise viisil, mis tagaks elektroonilise hääletuse turvalisuse ja töökindluse kooskõlas valimiste üldpõhimõtetega.

VVK osutatud ja väidetavalt 29.10 koosolekule edastatud materjalidest võimaldab kaebajate 29.10 järelevalvetaotluses kirjeldatud probleemide käsitlemist hinnata üksnes VVK 11.11 selgituste lisas nr 3 esitatud "Elektroonilise hääletamise riskide hindamise dokument". Selles olevat käsitletud "süsteemi turvalisusega seotud riske ja nende maandamiseks kavandatud meetmeid". VVK 29.10 koosoleku

protokollis puudub aga viide selle dokumendi arutamisele, dokumenti koosolekul ei mainitud ning selle päritolu ja koostamise aega ei ole täpsustatud. Samuti ei ole VVK sellele dokumendile hilisemates selgitustes oma seisukohtade põhjendamisel otsesõnu tuginenud. Seetõttu on küsitav, kas ja millises ulatuses oli tegemist dokumendiga, mida VVK 29.10 otsuse tegemisel tegelikult arvestas.

VVK järelevalvekohustuse sisuliseks täitmiseks ei piisa sellest, kui RVT väidetavalt "hindab, kas kirjeldatud probleem puudutab kasutatavat süsteemi, milline on selle tegelik mõju ning millised meetmed on riski maandamiseks rakendatud" (VVK 11.11 selgitused, lk 3). VVK peab neid asjaolusid kontrollima ka oma järelevalvepädevuse raames. Järelevalve tegelikku teostamist ei tõenda pelgalt väide, et tegemist on RVT-le teadaolevate riskidega, millega on väidetavalt arvestatud.

Kaebajale Märt Põdrale on kohtuasja 5-25-3 menetluse käigus kättesaadavaks saanud elektroonilise hääletuse süsteemi riskide ja nende maandamiseks kavandatud meetmete kirjeldus (LISA 2), millele VVK palus nimetatud kohtuasjas juurdepääsupiirangu kehtestada.

Märt Põder on tutvunud dokumendiga, mille failinime järgi on seda uuendatud 2024. aasta märtsis ja mille metaandmete järgi on seda viimati muudetud 5.03.2025. Tegemist on 105 andmereaga tabeliga, milles hinnatakse riske nende tõenäosuse ja mõju alusel viiepalliskaalal ning mille korrutis moodustab riskiklassi. Tabel käsitleb riske prooviläbimisel ja sellele eelneval perioodil, elektroonilise hääletuse ajal, pärast e-hääletuse lõppu ning töötlemisetapis. Lisaks sisaldab see 20 kirjet m-hääletamise riskide kohta. Kokku on 105 riskist 36 hinnatud keskmiseks, 37 väikeseks ja 32 väga väikeseks; kõrgeks ega väga kõrgeks ei ole hinnatud ühtegi riski.

Pole teda, kas raportites ja artiklites väljatoodud puudujäägid on lisas nr 3 esitatud "Elektroonilise hääletamise riskide hindamise dokumendis" kajastatud.

Isegi juhul, kui 29.10 koosolekule esitati seesama kaebajale 5-25-3 menetlusest tuttav tabel ning seda on hiljem täiendatud ka raportites ja artiklites kirjeldatud puudujääkidega, ei oleks selline tabel iseenesest piisav tõend nende puudujääkide kõrvaldamise kohta. Iga tuvastatud või põhjendatult kahtlustatud puudujäägi puhul eeldab hea auditeerimis- ja infoturbepraktika selle algpõhjuse, võimaliku mõju ning kõrvaldamiseks rakendatud meetmete dokumenteeritud analüüsi (vt ka meie 6.11 kaebuse täienduse lk 2 "Antud vastused ei tõenda probleemide lahendatust"). Kui ilmneb, et mõni turvakontroll või kehtestatud nõue ei ole olnud täidetud, ei piisa selle asjaolu pelgast nentimisest ega üldsõnalisest kinnitusest, et risk on maandatud. Vastutaja peab esitama kontrollitavad tõendid selle kohta, et tuvastatud puudujääk on kõrvaldatud, selle võimalik mõju on välja selgitatud ning see ei saa enam kahjustada süsteemi turvalisust ega valimiste läbiviimise usaldusväärsust.

Sellise praktika lahutamatu osa on ka intsidentide dokumenteeritud ja läbipaistev käsitlemine. Iga olulise intsidendi kohta peaks valmima piisavalt üksikasjalik analüüs, milles kirjeldatakse juhtunu asjaolusid, algpõhjust, võimalikku mõju, rakendatud parandus- ja maandamismeetmeid ning nende tulemuslikkuse sõltumatu kontrolli tulemusi. Arvestades valimiste avalikku iseloomu ja nende erilist tähendust demokraatliku riigikorralduse toimimisele, peaksid sellised analüüsid olema avalikkusele kättesaadavad

vähemalt ulatuses, mis võimaldab hinnata rakendatud meetmete asjakohasust ja tulemuslikkust. Ainult selline tõenduspõhine ja läbipaistev käsitlus võimaldab VVK-l ja demokraatlikul avalikkusel hinnata, kas tuvastatud probleemid on tegelikult lahendatud.

Lugupidamisega
/digitaalselt allkirjastatud/
Märt Põder
Kaebuse esitaja

Tõendid ja lisad

Lisa 1. KPMG_audit_avalik.pdf;
Lisa 2. 4._EHS_riskid_2021_täiendatud-03_2024.asice;