Riigikohtu põhiseaduslikkuse järelevalve kolleegium
5-26-45

19.11.2026

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

AVALDUS

Kasutame võimalust menetlusosalisena kommenteerida kohtu ja VVK vahel toimuvat arutelu mobiilseadmete kasutamisega seotud riskide teemal.

Mobiiliopsüsteemide tehnilisi riske käsitleti Cybernetica 16.04.2020 raportis [1], mille kohaselt ei seisne probleem üksnes valijarakenduse levitamises, vaid ka selles, et "algset puhtakujulist Androidi arendab Google, kuid on palju seadmete tootjaid, kes võivad oma seadmetega pakendada Androidi kohandatud versiooni" (lk 11).

Seetõttu võivad eri tootjate, näiteks Xiaomi, Huawei ja Samsungi seadmed kasutada küll Androidi opsüsteemi, kuid selle erinevaid versioone ja tootjapõhiseid kohandusi. Need võivad funktsionaalsuse, süsteemikomponentide ja turvaomaduste poolest oluliselt erineda. Erinevalt tavapärastest laua- ja sülearvutitest on mobiiltelefonide puhul kasutaja võimalused opsüsteemi ja selle süsteemikomponentide valimiseks, asendamiseks ning kontrollimiseks üldjuhul oluliselt piiratumad. Enamasti kasutatakse seadme tootja eelpaigaldatud ja kohandatud tarkvarakeskkonda. Seetõttu ei saa üksnes seadme tootja, opsüsteemi nimetuse või versiooninumbri põhjal järeldada, milline on seadme tegelik tarkvarakeskkond ja selle turvatase.

Mobiiltelefonide riist- ja tarkvaraökosüsteemide killustatus, vähene läbipaistvus ning kasutaja piiratud kontroll seadme tarkvarakeskkonna üle raskendavad nende turvalisuse sõltumatut hindamist. Androidi opsüsteemi kasutavate seadmete tootjatel on lisaks Google Playle ka oma rakendustepoed, näiteks Xiaomi GetApps, Huawei AppGallery ja Samsung Galaxy Store [2]. Nende ning muude alternatiivsete rakenduste levitamise kanalite kaudu võib olla võimalik levitada modifitseeritud versioone nii valijarakendusest kui ka häälekontrolli rakendusest. Probleem ei piirdu siiski nn libarakendustega. VVK-le esitatud 17.11 kohtunõude punktis 4 ja VVK 18.11 vastuse samas punktis käsitletud riskid -- häälte soovimatu edastamine või valija tahteavalduse mõjutamine -- ei piirdu rakenduse enda võimalike puudustega. Need võivad realiseeruda ka opsüsteemi, selle süsteemikomponentide või seadme tootja lisatud tarkvara tasemel. Seetõttu ei taga üksnes valijarakenduse tervikluse kontrollimine kogu mobiilse hääletamise lahenduse turvalisust. Seejuures tuleb arvestada, et hääle kontrollimise võimalus on Androidi opsüsteemiga mobiilseadmetes kasutusel juba 2013. aastast ja sellega kaasnevad hääle salajasuse tagatised ei vasta avaldatud raportite alusel

seadusele ka mistahes tehniliste manipulatsioonideta (vt meie 16.11 vastus lk 1-2 ja lk 4, aga ka ODIHR 2019. aasta raporti lk 7 [3]).

Kui rääkida "võõrriigi taseme ründajast" (Cybernetica raport lk 10), võib selline ründaja olla huvitatud just opsüsteemi või selle süsteemikomponentide tasemel toimuvast manipulatsioonist, sest sellist sekkumist võib olla raskem tuvastada kui nn libarakenduse levitamist. Selliste riskidega ei tegele KPMG m-valijarakenduste tervikluse audit [4], mis käsitleb rakenduste levitamist Google Play ja Apple App Store'i kaudu, kuid ei anna hinnangut seadmete opsüsteemide ega nende tootjapõhiste tarkvarakomponentide terviklusele.

Nõustume VVK vastuse punktis 4 esitatud väitega, et "samasugune risk suuremal kujul esineb ka arvutis hääletamisel". Samas puuduvad meie hinnangul terviklikud ja ajakohased avalikult kättesaadavad analüüsid selle kohta, kuidas on maandatud nimetatud riskid elektroonilisel hääletamisel üldiselt ning millised täiendavad riskid kaasnevad mobiilse hääletamisega. Meile pole teada, kas mobiilihääletuse tehnilist turvalisust on analüüsitud ka pärast Cybernetica 2020. aasta raportit, mis valmis enne mobiilihääletuse arenduse algust. Nagu oleme juba korduvalt osutanud, ei ole VVK pärast 2023. aasta sügist arutanud avalikult kättesaadavaid raporteid ega artikleid, milles on käsitletud elektroonilise hääletamise turvalisuse või selle seaduse nõuetele vastava korraldusega seotud puudujääke.

Me ei nõustu VVK vastuse punktis 5 esitatud seisukohaga, mille kohaselt olevat "mobiilseid libavalijarakendusi raskem levitada kui arvutile mõeldud libavalijarakendusi tulenevalt eelnevalt kirjeldatud rakenduspoes avaldamise protseduurist". Androidi seadmetes ei piirdu rakenduste levitamine ühe rakendustepoega: eri tootjad haldavad oma rakendustepoode ning kasutajal on võimalik seadistada ka muid, tootjatest sõltumatuid rakenduste levitamise kanaleid. Seetõttu võib tavapärase rakenduse paigaldamise käigus jõuda kasutajani ka modifitseeritud valijarakendus või hääle kontrollimise rakendus. Kasutajate juhendamine üksnes Google Play või Apple App Store'i kasutamiseks vähendab küll libarakenduse paigaldamise riski, kuid ei kõrvalda seda. Tavakasutajal ei pruugi olla piisavaid teadmisi, et hinnata eri rakenduspoodide usaldusväärsust või kontrollida rakenduse päritolu ja autentsust.

[1] https://www.valimised.ee/sites/default/files/uploads/eng/2020_m-voting-report.pdf
[2] https://en.wikipedia.org/wiki/List_of_Android_app_stores
[3] https://odihr.osce.org/odihr/elections/estonia/424229
[4] https://www.riigikogu.ee/tegevus/dokumendiregister/dokument/cbe34e3e-e605-4672-9caa-d17e9e7d0252/

Lugupidamisega
Märt Põder
Kaebuse esitaja