CYBERNETICA

Biomeetrilise näotuvastusmeetme rakendamine elektroonilisel hääletamisel

Tehniline dokument

Versioon 1.1

2. juuli 2021. a.

53 lk

Dok D-16-12

Sisukord

1 Sissejuhatus 5

2 Lühikokkuvõte 6

3 Probleemipüstitus 8
3.1 Alternatiivsed võimalikud lahendused 11

4 Infotehnoloogiline teostatavus 13
4.1 Võimalikud näotuvastuslahendused 13
4.1.1 ABIS 13
4.1.2 Näotuvastus isikut tõendava dokumendi pildi alusel 14
4.2 Eesti i-hääletamise süsteem 15
4.3 Võimalikud valikud 16
4.3.1 Millisel etapil näotuvastust kasutada? 16
4.3.2 Kas tuvastada nägu andmebaasi või dokumendi abil? 18
4.3.3 Millist seadet tuvastamisel kasutada? 18
4.3.4 Millist seadet kasutada hääletamisel? 18
4.3.5 Kas ja kuidas lahendada vaideid? 19
4.4 Võimalikud stsenaariumid kokkuvõtvalt 19
4.4.1 Näotuvastamine dokumendi abil, hääletamine PC-ga 19
4.4.2 Näotuvastamine andmebaasi abil, hääletamine PC-ga 19
4.4.3 Võimalikud alternatiivsed lahendused 20
4.5 Mõju kasutajakogemusele 20

5 Õiguslikud küsimused 22
5.1 Analüüsi ulatus 22
5.2 Lähtekohad 23
5.2.1 Hääletamisõiguse olemus 23
5.2.2 Elektroonilise hääletamise eripärad 23
5.2.3 Näotuvastus kui isikusamasuse kontrollimise viis 24
5.2.4 Näokujutis kui isikuandmed 26
5.2.5 Näotuvastuse lisandumine kui oluline muudatus (valimis)õiguses 27
5.3 Õiguslik analüüs 28
5.3.1 Analüüsi ulatus 28
5.3.2 Püstitatud küsimused 29
5.3.3 Võimalikud riived 30
5.3.3.1 Hääletamisõiguse riived 30
5.3.3.2 Era- ja perekonnaelu ning kodu puutumatusega seotud riived . 30
5.3.3.3 Kaitsepõhiõiguse riived 31
5.3.4 Riivete proportsionaalsus 32
5.3.4.1 Legitiimne eesmärk 32
5.3.4.2 Sobivus 33
5.3.4.3 Vajalikkus 35
5.3.4.4 Mõõdukus 37

5.3.5 Riivete seaduslik alus 38

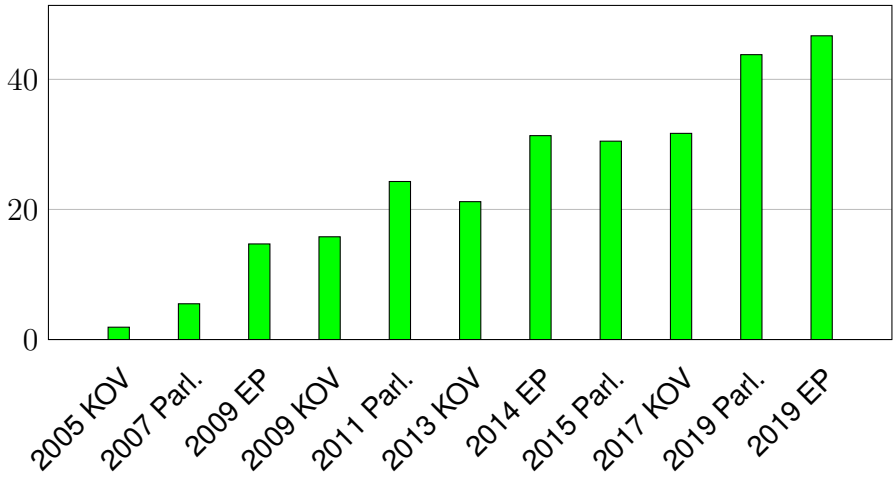
6 Arendustööde mahu hindamine 41
6.1 Eeldused 41
6.2 Jõudlusnõuded 42
6.3 Arendusvajadus osapooliti 42
6.4 Näotuvastusvõimekuse saavutamine 43
6.4.1 Välise näotuvastusteenuse kasutamine 43
6.4.2 Riikliku näotuvastusteenuse loomine 44
6.5 Arendusmahud 44

A Näotuvastusteenusepakkuja küsimustik 46
A.1 Eestikeelne küsimustik 46
A.2 English questionnaire 48

Kirjandus 50

1 Sissejuhatus

Eestis on esinduskogude valimistel olnud võimalik anda oma hääl üle Interneti (i-hääl) alates 2005. aastast. Aastatel 2005-2019 on valimisi korraldatud 11 korral ning selle aja vältel on i-häälte osakaal kõigist loetud häältest tõusnud 46,7%-ni (vt joonis 1)[1].



Joonis 1. I-häälte osakaal kõigist häältest

Eesti i-hääletamissüsteemi on kogu tema eluea jooksul pidevalt täiendatud. Suuremad muutused on aset leidnud 2013. aastal, kui lisandus hääle individuaalse verifitseerimise võimalus, ning 2017. aastal, mil tõsteti oluliselt serveripoole sõltumatu auditeerimise võimekust.

Loomulikult süsteemi arendus sellega ei piirdu ning täiendusi tuleb teha ka edaspidi. Praegune aruanne vaeb küsimust, kas Eesti i-hääletamisele oleks otstarbekas lisada valijate biomeetriline autentimine näotuvastuse teel. Uurime, milliste probleemide vastu see meede millisel määral aitaks, kui palju tõuseks süsteemi keerukus ning millised probleemid kerkiksid lisaks.

[1] `https://www.valimised.ee/et/valimiste-arhiiv/elektroonilise-haaletamise-statistika` (31.05.2021)

2 Lühikokkuvõte

Kuigi paberhääletamine jaoskonnas ja elektrooniline kaughääletamine teenivad ühist eesmärki, on nad tehnilistelt omadustelt väga erinevad. Seega on vaja võrreldava turvataseme saavutamiseks kasutada erinevaid meetmeid.

Üheks heaks näiteks on siinkohal hääletamisvabaduse tagamine. Kui jaoskonnas hääletamisel nõutakse sedeli täitmist kabiini privaatsuses, siis elektroonilise kaughääletamise korral on mõjutamise ohu kompenseerimiseks võimalik uuesti hääletada.

Sarnane olukord tekib ka isikusamasuse tagamisel. Kui jaoskonnas tuvastab jaoskonna töötaja hääletajat pildiga dokumendi alusel (mida on raske teha sajaprotsendilise kindlusega!), siis elektrooniline hääletamine tugineb digitaalsele identiteedile.

I-hääletamine on Eestis saanud võimalikuks tänu sellele, et siin on õnnestunud ellu viia põhimõte, mille järgi ühele füüsilisele isikule vastab (ülimalt) üks digitaalne identiteet. Seejuures on isiku ja digitaalse identiteedi vahelise seose hoidmine inimese enda huvides. Kui ta teeb oma eID vahendi koos PIN-koodidega kättesaadavaks kellelegi teisele, peab ta vastutama ka potentsiaalsete tagajärgede eest (näiteks kandma tema nimel digiallkirjastatud lepingute kohustusi).

Kahjuks ei muuda see digitaalse identiteedi üleandmist või ülevõtmist võimatuks. Nii kerkivad valimiste kontekstis aeg-ajalt üles süüdistused, mille järgi nõrgemal positsioonil olevate inimeste (nt hooldekodu klientide) ID-kaarte on koos PIN-koodidega kokku korjatud ning neid siis kaardiomanike eest hääletamiseks kasutatud. Selliste ohtude maandamiseks on välja pakutud mitmeid lahendusi, sealhulgas füüsilise ja digitaalse identiteedi tugevam sidumine näobiomeetria abil.

Esmapilgul tundub see olevat suurepärane idee, kuivõrd biomeetrilise kaugtuvastamise lahendused on viimase paari aastaga jõudsalt edasi arenenud. Ka Eestis on näobiomeetria põhist autentimist kasutatud näiteks eNotari ja eksamite korral. Sarnase lahenduse juurutamine valimistel tooks aga endaga kaasa terve rea probleeme ning jätab lahtiseks mitmeid küsimusi.

- Hääletamine on olemuslikult pikem protsess ja näotuvastamise kasutamine selle protsessi mingil etapil ei kinnita, et sama isik viis läbi kogu protsessi. Seetõttu ei pruugi näotuvastusest tõusta nii suurt sisulist tulu, kui algul tundub.
- Põhimõtteliselt võib kaaluda kogu protsessi jälgimist videovoo vahendusel. Niisugune lahendus toob aga endaga kaasa rohkem probleeme, kui ta potentsiaalselt lahendaks.
  - Eesti i-hääletamise tipp-perioodidel toimub paralleelselt umbes paarsada seanssi. Nende kõigi reaalajas töötlemine nõuab märkimisväärset taristut. Hetkel Eesti turul saada olevad kommertsiaalsed automatiseeritud näotuvastuslahendused pole ehitatud pikema videovoo jälgimiseks. Inimoperaatoritega videovoogude jälgimine kahandab aga oluliselt kogu süsteemi jõudlust.
  - Hääletaja poolel peaks olema videovoo ülekandmiseks korralik internetiühendus.

Kahjuks ei saa seda tänases Eestis veel kõikjal eeldada. Lisaks pole selge, mida teha voo ajutisel katkemisel. Kui sel juhul nõuda kogu protsessi uuesti alustamist, halvendab see märkimisväärselt valijakogemust.

  - Sadade tuhandete Eesti inimeste kodudest pikema videovoo nõudmine riivab oluliselt nende privaatsust. Väga raske on tagada, et kogu protsessi videopilti ei jää delikaatsed andmed (sh hääle väärtus ja PIN-koodid).

- Privaatsusriive on märkimisväärne ka siis, kui näotuvastamiseks kasutatakse vaid lühiajalist videoühendust või isegi ainult ühte pilti inimesest tema oma kodus. Välisele osapoolele võivad teatavaks saada andmed isiku varandusliku või terviseseisundi kohta, tema religioossed tõekspidamised või poliitilised eelistused. Riive suureneks veelgi, kui tuvastamise käigus tehtud pilte või videosid tuleks hoida pikema aja jooksul hilisemaks vaiete lahendamiseks.
- Näotuvastuse veaprotsent ei saa kunagi olema null, kuna biomeetrial põhinev autentimine on heuristiline protsess. Isiku tuvastamiseks määratud lävendist sõltub nii valepositiivsete kui ka valenegatiivsete tuvastuste hulk. Kui parimate hetkel saadaolevate lahenduste valepositiivsete osakaal viia alla $\frac{1}{100000}$, siis nö kodutingimustes (kehv valgus, suvaline taust, madala lahutusvõimega kaamera) tehtud piltide korral jääks valenegatiivsete hulk 3% juurde. See tähendab, et näiteks 250000-st inimesest ei õnnestuks hääletada ca 7500-l.
- Näotuvastuse lisamine Eesti i-hääletamise protokolli nõuaks nii protokolli keerukamaks muutmist kui ka täiendava riistvara kasutuselevõttu. See tähendab, et protokoll muutub tõrkeohtlikumaks, halvendades samas ka kasutajakogemust.

Kõigi nende probleemidega oleks põhimõtteliselt võimalik leppida, kui tulemusena saadav kasu neid ületaks. Niisiis saab näotuvastamise sisseviimise kaalutlemisel otsustavaks küsimus proportsionaalsusest – mida tähtsam on saavutatav eesmärk, seda rohkem võib selle saavutamise nimel ohverdada, sh sekkuda põhiõigustesse ja -vabadustesse.

Aruande koostamise käigus uurisime meile kättesaadavate materjalide abil mõningaid väiteid hooldekodudega seotud grupihääletamise kohta, kuid ei leidnud tõendeid nende kinnituseks. Seega ainuüksi nn hooldekodude juhtum ei ole piisav, et õigustada seni kasutusel oleva tuvastamisviisi asendamist või täiendamist oluliselt ressursimahukama ning põhiõigusi rohkem riivava näotuvastamisega, mis toob omakorda kaasa uusi probleeme ja riske.

Aruande infotehnoloogilise teostatavuse ja õigusliku analüüsi raames leidsime, et näotuvastuse kasutuselevõtt Eesti i-hääletamise protokollis oleks hetkeseisuga ebaproportsionaalne meede ka sellepärast, et leidub vähem koormavaid, ent võrreldava efektiivsusega alternatiive nende probleemide lahendamiseks, mille vastu näotuvastamine suunatud on (vt jaotis 3.1).

Näotuvastuse kasutuselevõtt elektroonilisel hääletamisel ei oleks pelgalt tehniline uuendus, vaid nõuaks põhimõttelist muudatust ühiskonnas kehtivates normides, sh Eesti õiguskorras. Sellega looks Eesti pretsedendi lääneriikide seas, kus seni on näotuvastust avalike teenuste kontekstis kasutatud üsna kitsalt piiritletud valdkondades (nt piiriületus, kriminaalmenetlus, dokumentide väljastamine). Niisuguse kaaluga pretsedenti oleks mõistlik valmistada ette järk-järgult, alustades ühiskondlikust arutelust ja jätkates pilootprojektidega, et uut tuvastamisviisi paremini hinnata. Valimiste kaasutamine pilootprojektina pole mõistlik.

Tuvastuskindluse tagamise probleem digitaalses keskkonnas ei piirdu vaid i-hääletamisega. Seetõttu peab näotuvastuse rakendusala laiendamisel silmas pidama selle kaugemaleulatuvat mõju. Isegi kui näotuvastuse kasutuselevõtt on teatud tingimustel vastuvõetav meede, tuleb need tingimused eelnevalt ühiskonnas läbi rääkida ja seaduse tasandil kehtestada.

3 Probleemipüstitus

Selle aruande probleemipüstitusena pidid aruande koostajad uurima näotuvastamise rakendatavust ning rakendamisega kaasnevaid probleeme i-hääletamisel.

Uuringu üheks algtõukeks võib pidada endise IT- ja väliskaubandusministri Kert Kingo poolt 2019. aastal kokku kutsutud komisjoni. 11. septembril toimunud istungil väljendas minister seisukohta, mille järgi “peame suutma garanteerida, et hääletav isik on see sama, kelle ID-kaardi abil toimingut tehakse.” [6, lk 68].

Kert Kingo täpsustas hiljem oma muret veebiväljaandes Uued Uudised [34]: “On teada, et vanadekodudes antakse klientide dokumendid, sealhulgas ID-kaart koos PIN-koodidega, võimalike varguste vältimiseks hooldekodu töötaja “turvalisse” valdusesse. Kes garanteerib, et mõni töötaja ei kasuta oma valdusesse saadud ID-kaarte salaja oma poliitiliste eelistuste elluviimiseks?”

Väiteid ID-kaartide kuritarvitamisest hooldekodudes on esitatud juba esimese i-hääletamise kohta 2005. aastal [7]. Meil pole andmeid, kas toonased väited ka õiguskaitseorganiteni jõudsid. Küll uuris politsei sarnast juhtumit 2015. aastal. Tuvastati, et neli pensionäride päevakeskuse klienti hääletas juhataja kabinetis, kuid nad väljendasid seejuures oma vaba tahet, paludes juhatajalt vaid nõu ja abi ID-kaardi toimingute sooritamisel [23].

Uuringu käigus viisime läbi intervjuu Sotsiaalministeeriumi ja Sotsiaalkindlustusameti esindajatega, samuti uurisime ID-kaartide ja PIN-koodide hoiustamise põhimõtteid ühes hooldekodus. Tõepoolest, ka hooldekodu klientidel on tarvis isikut tõendavat dokumenti, näiteks arsti juurde või haiglasse minnes. Kuivõrd ajaloolise kogemuse põhjal kipuvad hooldealuste endi käes olevad dokumendid kriitilistel hetkedel aeg-ajalt kaduma, võidakse neid soovitada hoiustada hooldekodu seifis. Kui klient ei soovi ID-kaarti loovutada, võidakse hoiustada ka selle paberkoopiat.

Hooldekodude klientidel pole enamasti otsest vajadust ID-kaarte elektrooniliselt kasutada. Intervjueeritud hooldekodutöötaja ütles, et enamik kliente tulebki asutusse nii, et neil pole PIN-koode kaasas. Nendel juhtudel, kui hooldusalune või mõni lähedastest on andnud hooldekodu valdusesse ka PIN-koodide ümbriku, hoitakse seda kinnikleebituna ja ID-kaardist eraldi teises seifis.

Seega saab hoolekodude ja teiste kinniste või poolkinniste asutuste ID-kaartide hoiupoliitikat vaadelda kahel tasemel. Esiteks, kas administratsiooni või mõne teise võimupositsioonil oleva isiku poolt hoiustatakse ID-kaarte ning kas seda tehakse koos elektroonilist kasutamist võimaldavate PIN-koodidega. Teiseks tuleb küsida, kuidas tagatakse nende dokumentide hoiustamispoliitika usaldusväärsus ja välistatakse hoiustatud dokumentide väärkasutamise oht.

Igal juhul on selge, et probleem polegi niivõrd selles, kes ID-kaardi valimiste ajal lugejasse paneb, kuivõrd selles, kas nõnda talitades järgitakse kaardiomaniku tahet. Kaalutletava biomeetrilise meetme kontekstis tuleb seega küsida, kas või mil moel aitab näotuvastus kaasa tahtluse

tuvastamisele.

Arvestada tuleb ka, et sadade tuhandete valijate identifitseerimine videopildi kaudu põhjustab märkimisväärse privaatsusriive (vt jaotis 5). Selleks, et hinnata näotuvastuse kui meetme proportsionaalsust, peame kõigepealt selgitama, kui laialt levinud probleemiks on kodanike tahte vastaselt nende ID-kaartidega hääletamine.

Riigi Teataja kohtulahendite otsing[2] andis karistusseadustiku paragrahvide 162 ja 164 (mis käsitlevad valimisvabaduse rikkumist ja häälte ostmist) peale kokku 10 vastet. Valdav enamus neist käib paberhääletamise, mitte i-hääletamise vastaste süütegude kohta. Vaid ühel korral on uuritud väidet, mille alusel kahtlustatav pakkus "*linnas valimisõigusega isikutele sularaha selle eest, et viimased annaksid tema kasutusse ID-kaardi koos PIN-koodidega 2009.a kohaliku omavalitsuse volikogu valimiste ajaks eesmärgiga teostada elektroonilist hääletamist*" [16]. See kahtlustus ei leidnud uurimise käigus kinnitust.

Kohtusse mitte jõudnud, aga konkreetseid isikuid puudutavaid süüdistusi õnnestus meil tuvastada kolm.

- 2005. aastal süüdistati Koluvere hooldekodu juhatajat hoolealuste ID-kaartidega hääletamises [7]. Tollastest sündmustest pole säilinud piisavalt materjali, et neid hinnata; muuhulgas pole meile teada, et politsei oleks kaebuse menetlusse võtnud.
- 2015. aastal süüdistati Võru Pensionäride Päevakeskuse juhatajat eakate eest hääletamises. Politseiuurimine ei tuvastanud seaduserikkumist [23].
- 2017. aastal süüdistati Hummuli vallavanemat hooldekodu eakate elanike ID-kaartidega hääletamises [24].

Ka viimasel juhul ei ole kedagi süüdi mõistetud. 2017. aastast on aga säilinud süsteemi logid, mille alusel saab hinnata, kas hääletamisel esines anomaaliaid. Käesoleva uuringu raames tegi Riigi Valimisteenistus meile kättesaadavaks hääletamistoimingute metainfo anonümiseeritud logid, kus olid iga hääle kohta säilitatud digitaalallkirjastamise ajahetk, hääletaja sugu ja vanus aasta täpsusega, kasutatud operatsioonisüsteem ning IP-aadressi pseudonüüm. Viimase abil pole võimalik tuvastada, millisele kasutajale või asutusele IP-aadress kuulub, küll aga on võimalik kindlaks teha, millised hääled laekusid samalt aadressilt. Seda asjaolu saab ära kasutada grupihääletamise mustrite uurimisel. Täpsustusena märgime, et asutuste sisemisi IP-aadresse valimiste kesksüsteem ei näe ning asutuse võrgu kaudu antud hääled logitakse sama välise IP-aadressi alla.

Lähtume tähelepanekust, et kui nn hooldekodu stsenaarium aset leiaks, peaks olema logidest näha, et ühelt IP-aadressilt on hääletanud palju vanemaealisi inimesi, kusjuures tõenäoliselt suhteliselt väikese ajavahemiku jooksul. Niisiis uurisime kõigepealt IP-aadresse, kust on hääletanud vähemalt 10 enam kui 65-aastast inimest. Nende aadresside seast otsisime omakorda niisuguseid, kust tunni aja jooksul on antud kõige rohkem vanemaealiste hääli. Tulemusena leidsime kaks IP-aadressi, kust tunni jooksul on hääletanud viis või enam üle 65-aastast inimest.

- IP1 pealt laekus 05.10.2017 ajavahemikus 13.32–14.32 viis häält enam kui 65-aastastelt valijatelt. Samas laekus sellelt IP-aadressilt kokku 750 häält, sh kõnealusel ajavahemikul 39 häält. 5. oktoober oli i-hääletamise esimene päev ja on teada, et esimesel päeval laekubki väga palju hääli. Arvestades lisaks, et sellelt IP-aadressilt hääle andnute keskmine vanus oli 48,1 aastat, pole kindlasti tegemist hooldekoduga.

[2] `https://www.riigiteataja.ee/kohtulahendid/kriminaalkohtumenetlus.html` (31.05.2021)

- IP2 pealt laekus 05.10.2017 ajavahemikus 09.35–10.35 seitse häält enam kui 65-aastastelt valijatelt. Samas laekus sellelt IP-aadressilt kokku 462 häält, sh kõnealusel ajavahemikul 32 häält. Jällegi oli tegemist i-hääletamise esimese, traditsiooniliselt ühe tihedama päevaga ja IP2 pealt hääletanute keskmine vanus oli 49,7 aastat. Taaskord ei saa tegemist olla hooldekoduga.

Suure tõenäosusega on nende IP-aadresside näol tegemist suurte asutustega, kust antaksegi palju hääli ja osade hääletajate kõrgem vanus ongi statistiliselt ootuspärane.

Selleks, et leida väiksemaid asutusi ja organisatsioone, kust on antud suhteliselt palju vanemaealiste hääli, otsisime teiseks IP-aadresse, kust on antud vähemalt 10 häält ja kus hääletajate keskmine vanus ületab 65 aastat.[3] Ka selliseid aadresse oli kaks, vt tabelid 1 ja 2.

Tabel 1. Hääletamissündmused aadressilt IP3

Kuupäev	Aeg	Sugu	Vanus	OS
05.10.2017	23:53	M	66	Windows 10
05.10.2017	09:04	N	75	Windows 10
07.10.2017	02:26	M	63	Windows 8.1
07.10.2017	08:46	M	73	Windows 7
08.10.2017	12:29	N	66	Windows 10
08.10.2017	15:24	N	79	Windows 10
10.10.2017	12:35	M	70	Windows 7
10.10.2017	09:26	N	75	Windows 7
11.10.2017	11:37	N	33	Windows 10
11.10.2017	06:59	M	78	Windows 10

Tabel 2. Hääletamissündmused aadressilt IP4

Kuupäev	Aeg	Sugu	Vanus	OS
05.10.2017	13:29	M	71	Windows 7
07.10.2017	19:51	M	61	Windows 10
07.10.2017	09:31	N	68	Windows 7
08.10.2017	12:07	M	61	Windows 10
08.10.2017	20:17	M	84	Windows 10
09.10.2017	15:50	M	79	Windows 10
09.10.2017	18:48	N	82	Windows 10
10.10.2017	17:08	N	87	Windows 10
10.10.2017	18:52	N	79	Windows 10
10.10.2017	18:59	M	83	Windows 10
10.10.2017	23:34	N	63	Windows 10

Ajatempleid vaadates näeme, et kummalgi juhul ei esine mustrit, mis vastaks paljude ID-kaartide korraga kasutamisele. 2017. aasta kohalike omavalitsuste valimistel anti hääli 95421 unikaalselt IP-aadressilt. See, et mõnelt neist annavadki hääli peamiselt vanemaealised inimesed, on taaskord statistiliselt ootuspärane.

[3] Isegi arvestades, et hooldekodu IP-aadressilt võivad hääletada ka mõned nooremad inimesed (näiteks töötajad), peaks vanurite eest massilise hääletamise korral hääletanute keskmine vanus 65 aasta piiri oluliselt ületama.

Kokkuvõtteks tõdeme, et meie uuring ei tuvastanud hääletamislogidest mustreid, mis vastaksid vanemaealiste inimeste ID-kaartide massilisele ärakasutamisele.

3.1 Alternatiivsed võimalikud lahendused

Algne ülesandepüstitus küll ei nõudnud ilmutatult alternatiivsete lahenduste kaalumist, kuid täitja hinnangul poleks aruanne terviklik, kui me neid ei käsitleks.

Kui lugeda lahendatavaks probleemiks valijate eest ilma nende teadmise ja nõusolekuta i-hääletamist, siis see eeldab mõne eID vahendi täielikku omaniku kontrolli alt väljumist. Kui tegemist oleks üksikjuhtumitega, oleks nende mõju valimistulemusele väike. Märkimisväärne probleem tekib siis, kui keegi omandab kontrolli suure hulga võõraste eID vahendite üle.

Tänane õigusruum võimaldab ID-kaardi sertifikaati peatada või kehtetuks tunnistada sertifikaadi kasutaja (valija), tema usaldusteenuse pakkuja (nt SK ID Solutions AS), ID-kaardi väljaandja (Politsei- ja Piirivalveamet, Välisministeerium), pädeva asutuse või Andmekaitse Inspektsiooni, kohtu, prokuratuuri või uurimisasutuse algatusel [5, §17 ja §19][14, §9^5 ja §9^6]. Dokumendi väljaandjal on õigus sertifikaat kehtetuks tunnistada, kui "*on põhjendatud alus arvata, et sertifikaadis nimetatud avalikule võtmele vastavat privaatvõtit on võimalik kasutada dokumendi kasutaja nõusolekuta*" [14, §9^6 lg 1 3)]. Samas sertifikaadi omanikul (valijal) on lausa kohustus taotleda sertifikaadi kehtetuks tunnistamist, kui tal "'*on kahtlus, et sertifikaadis sisalduvale avalikule võtmele vastavat privaatvõtit on võimalik kasutada tema nõusolekuta*" [5, §19 lg 3].

Omaette küsimus on sellise olukorra tuvastamine näiteks hooldekodudes – kas ja kuidas on hooldekodu klientidel võimalik teada saada või veenduda, et nende privaatvõtit on kasutatud ilma nõusolekuta. Kui esineb tõendeid võimaluse kohta, et kuritarvitatud on paljude hooldekodu klientide sertifikaate, siis võib näiteks kohus või Andmekaitse Inspektsioon taotleda kõigi mõjutatud sertifikaatide peatamist või kehtetuks tunnistamist. See oleks valimiste kontekstis potentsiaalselt suure mõjuga otsus, mis võib mõjutada valimistulemust. Järelikult ei saa niisugust otsust langetada kergekäeliselt.

Võimalikud on ka pehmemad meetmed. Uuringu käigus läbi viidud intervjuust Siseministeeriumi esindajaga selgus, et näiteks kinnipidamisasutustes kasutatakse PIN-ümbrike hoidmist pitseerituina. PIN-koodide avamiseks ja taaspitseerimiseks on olemas eraldi protseduur. Intervjuu käigus ühe hooldekodu töötajaga selgus, et vähemalt selles hooldekodus midagi sarnast toimubki. PIN-ümbrikke ei hoita küll pitseerituina, küll aga kinnikleebituina ja eraldi seifis. Niisuguse praktika tutvustamine ja juurutamine hea tavana võib anda laialdase efekti hooldekodude stsenaariumiga seotud hirmude mahavõtmiseks.

- **Soovitame hooldekodudes jt (pool)kinnistes asutustes elektroonilise identiteedi haldamise hea tava väljatöötamist ja levitamist. See tava peaks sisaldama PIN-koodide hoidmist ID-kaartidest eraldi ning selgeid reegleid PIN-koodidele ligi pääsemiseks.**

Peale hooldekodu stsenaariumi on veel teoreetilisi võimalusi eID vahendi volitamatuks ülevõtmiseks. Ühele sellisele (mobiil-ID ärakasutamine mobiilseadmes töötava kahjurvara poolt) juhib tähelepanu hiljutine m-hääletamise aruanne [28]. Selles aruandes soovitatud vastumeede aitab maandada ka hooldekodu stsenaariumi riske.

- **Kaaluda sõltumatu tagasisidekanali (nt e-kiri, SMS vmt) sisseviimist, mille abil saaks hääleõiguslik kodanik teada, et tema nimel on antud i-hääl.**

Loomulikult vajab selline meede enne juurutamist täiendavat analüüsi näiteks mõjutusrünnete seisukohast, kuid esialgne analüüs näitab, et hääle muutmise võimalus pakub efektiivset kaitset ka selle ohu vastu [30].

Näotuvastamise ja tagasisidekanali suurim erinevus seisneb selles, et esimene neist on ennetusmeede, mille ambitsioon on püüda kinni kõik potentsiaalsed ründed, aga teine on tuvastusmeede, mille efektiivsus sõltub sellest, kui paljude valijatega riik automaatselt ühendust võtta suudab. Seoses vajadusega COVID-19 pandeemiat efektiivsemalt hallata, suunas riik 2021. aasta märtsis edasi umbes 1,3 miljoni eestimaalase `@eesti.ee` postkastid[4]. Ka laialdaselt kasutatav sõltumatu tagasisidekanal ei garanteeriks iga üksiku väärkasutuse tuvastamist, kuid tõstaks oluliselt vähegi laiema ulatusega ründe vahelejäämise tõenäosust.

Juhime tähelepanu, et ka praegune Eesti õiguslik keskkond ja i-hääletamissüsteem pakuvad mehhanisme eID väärkasutuse ennetamiseks ja kompenseerimiseks. Karistusseadustiku alusel on karistatavad nii teise isiku identiteedi ebaseaduslik kasutamine (§157[2]) kui valimisvabaduse rikkumine (§162).

- **Kui kellelgi on teavet võimaliku kuriteo toimepanemisest, tuleb selle teabe kontrollimiseks pöörduda õiguskaitseorganite poole, aga mitte hakata kuulujutte levitama. Inimesi tuleb õiguskuuleka käitumise (sh kuriteost teatamise võimaluste) osas rohkem teavitada.**

Paneme tähele, et poliitikutel on siinkohal võimalus isiklikku eeskuju näidata.

Kui inimene kahtlustab, et tema ID-kaarti võidakse olla tema teadmata i-hääle andmiseks väärkasutatud, on tal võimalus elektrooniliselt kordushääletada. Tegemist on olulise valimisvabaduse tagamise meetmega, mis on olnud kasutuses juba esimesest i-hääletamisest alates. Kert Kingo on korduvalt avaldanud seisukohta, et see meede tuleks kaotada [6, 34]. Olles uurinud kõiki põhilisi teaduskirjanduses välja pakutud elektroonilise kaughääletamise mõjutuskindluse tagamise meetodeid, on selle aruande koostajad siiski seisukohal, et korduvhääletamise võimalus on ainus praktikas juurutatav meede kaughääletamise korral mõjutuskindluse saavutamiseks [36].

Ehk tekitab arusaamatust see, et võimalus korduvalt hääletada ei hoia mõjutusründeid ära mitte otseselt, vaid kaudselt, vähendades potentsiaalse ründaja motivatsiooni näiteks häält osta. Sel juhul pole mõjutajal garantiid, et ostetud hääl tõepoolest talle jääb, mitte hiljem muutmisele ei lähe. Kui korduvhääletamise meede kaotada, omandaks hääle ostja just kindluse, et hääl jääb kindlasti muutmata. Niisiis on selle jaotise viimane soovitus olemuselt väga lihtne.

- **Korduva i-hääletamise võimalus peab alles jääma. Peale mõjutusrünnete heidutuse on see meede efektiivne ka eID võimalikest väärkasutustest taastumisel.**

[4] `https://tehnika.postimees.ee/7214305/elanike-riiklik-postkast-eesti-ee-suunati-automaatselt-edasi` (31.05.2021)

4 Infotehnoloogiline teostatavus

4.1 Võimalikud näotuvastuslahendused

Uuringu käigus intervjueerisime lisas A toodud küsimustiku alusel nelja näotuvastusteenuse pakkujat. Intervjuude tulemusel selgus, et hetkel on mõeldav kasutada kahte põhimõtteliselt erinevat lahendust.

4.1.1 ABIS

Eestis on olemas riiklikult arendatav automaatse biomeetrilise isikutuvastuse süsteem ABIS [2]. Süsteemi keskmes on riiklik andmekogu, kuhu koondatakse erinevatest andmekogudest pärinevaid ning erinevate riiklike menetluste raames kogutavaid biomeetrilisi isikuandmeid – näo- ja sõrmejäljekujutisi.

ABIS pakub kahte tuvastusliidest.

- Näokujutise ja isiku identifikaatori alusel on võimalik teada saada, kas näokujutis vastab selle identifikaatori all ABISesse talletatud näokujutisele. Põhimõtteliselt on lisaks jah/ei vastusele võimalik tagastada ka tuvastuskindluse skoor.
- Näokujutise abil on võimalik pärida parimad vasted ABISes talletatute hulgast.

I-hääletamise kontekstis on oluline neist esimene. Kuna ABIS kasutab enda sisemisi identifikaatoreid, siis tuleb näiteks isikukoodi ja näokujutise vastavuse tuvastamiseks lisada isikukoodide ja ABISe identifikaatorite vastavustabel. See nõuab mõningast arendust, aga on põhimõtteliselt tehtav.

ABISe arendajad ei paku klientrakendust ega -teeke, niisiis tuleks ka see pool i-hääletamise jaoks lisaks arendada.

ABIS kasutab otseseks nägude tuvastamiseks Idemia poolt arendatud lahendust. NISTi poolt standarditud testide põhjal saadakse kontrollitud keskkonnas väga hea tuvastustäpsus: kui valepositiivsete osakaal viia alla $\frac{1}{100000}$, annab süsteem valenegatiivseid vastuseid alla 1%. Samas kontrollimata keskkonnas tehtud piltide pealt on valenegatiivsete osakaal umbes 3%.[5] See tähendab, et näiteks 250000st i-hääletajast ei õnnestuks tuvastada hinnanguliselt 7500.

Põhimõtteliselt on võimalik valenegatiivsete tuvastustega kaasnevate probleemide lahendamiseks kasutada inimtuvastust, aga vastavat liidest ABIS hetkel ei paku. Kuna inimtuvastuse

[5] `https://pages.nist.gov/frvt/html/frvt11.html` (31.05.2021) Kontrollitud keskkond tähendab siinkohal, et pildid on tehtud heades valgustingimustes, ühtlase taustaga, kvaliteetse kaameraga, otsevaates, jne. Kaughääletamise stsenaariumi puhul neid eeldusi reeglina teha ei saa, seega tuleks aluseks võtta pigem kontrollimata keskkonnas saadud testitulemused.

puhul oleks tegemist hoopis teistsuguse töövooga, nõuaks selle lisamine suuremahulist arendust.

Omaette probleem on jõudlus. Hetkel suudab ABIS töödelda ca 40 päringut minutis. Samas näiteks 2019. aasta parlamendivalimiste ajal esitati tippkoormuse ajal (ca pool tundi enne i-hääletamise lõppu) kuni 212 häält minutis. Arvestades, et i-hääletamise perioodil ei saa ABIS peatada ka teiste rakenduste teenindamist, tuleks tema jõudlust hääletamise jaoks suurusjärgu võrra tõsta. Kui palju see maksma läheb, ei osanud arendajad ilma põhjaliku analüüsita intervjuu käigus öelda.

Jõudlusprobleemi on põhimõtteliselt võimalik lahendada, kui hääletamise ajal nägusid mitte tuvastada, vaid salvestada ainult hääletajate näopildid ja neid siis hiljem järelauditi korras analüüsida. Selline lahendus toob aga endaga kaasa uusi probleeme.

- ABISe hetkejõudlust arvestades kuluks 250000 näokujutise analüüsiks $\frac{250000}{40 \cdot 60 \cdot 24} \approx 4,34$ ööpäeva. See muutuks ajaliseks pudelikaelaks valimistulemuste väljakuulutamisel.
- Pole selge, mida teha siis, kui tuvastamine ebaõnnestub. Anonümiseeritult kokku loetud häälte seast pole enam võimalik midagi kustutada. Kodanikule süüdistuse esitamine identiteedivarguses, tuginedes vaid udusele fotole, on samuti kaheldav lahendus.

4.1.2 Näotuvastus isikut tõendava dokumendi pildi alusel

Turul on mitmeid kommertsiaalseid näotuvastusteenuse pakkujaid. Uuringu käigus intervjueerisime neist kolme.

Kommertspakkujad ei saa oma teenust ehitades tugineda riiklikule biomeetrilisele andmebaasile. Seega realiseerivad nad teistsuguse töövoo, mis kasutab isikut tõendavalt dokumendilt (pass, ID-kaart, juhiluba jmt) andmete ja näokujutise pildistamist, mille järel analüüsitakse dokumendipildi vastavust isiku näole. Muuhulgas suudavad niisugused lahendused lugeda dokumendilt inimese andmeid (nt nime, isikukoodi ja dokumendinumbrit), hinnata dokumendi ehtsust ja tuvastada isiku elusolekut (st et inimese näo asemel ei näidata kaamerasse tema pilti).

Kõigil intervjueeritud kommertspakkujatel on olemas teegid klientrakenduste loomiseks levinumatele mobiilplatvormidele (iOS, Android), mõnel on olemas ka PC ja/või veebikliendi tugi.

Kõik intervjueeritud kommertspakkujad võimaldavad suurema või väiksema vaevaga toetada ka inimtuvastamist. Tüüpiliselt tähendab see eraldi veebiliidest, kuhu jõuab informatsioon toimunud tuvastuste staatuse kohta, võimaldades ebaõnnestunud tuvastuse korral inimoperaatoril pilte üle vaadata. Loomulikult tähendab see teatavat viivitust protsessis. Selle viivituse mõju valijakogemusele on ilma praktikas testimata raske hinnata.

Ka tuvastustäpsuse hindamine nõuab põhjalikumat testimist. Üks kommertspakkujatest viitas sarnastele tulemustele kui ABISe arendajadki, kuid need tulemused on saadud NISTi standardtestandmetel. Arvestades dokumendifotode keskmiselt üsna halba kvaliteeti, on raske uskuda, et praktikas saavutataks ABISega võrreldav täpsus.

Teine kommertspakkuja on teinud teste spetsiifiliselt Eesti dokumentidega ning on saanud valepositiivsete tulemuste osakaaluks 0,04% ja valenegatiivsete osakaaluks 0,16%.

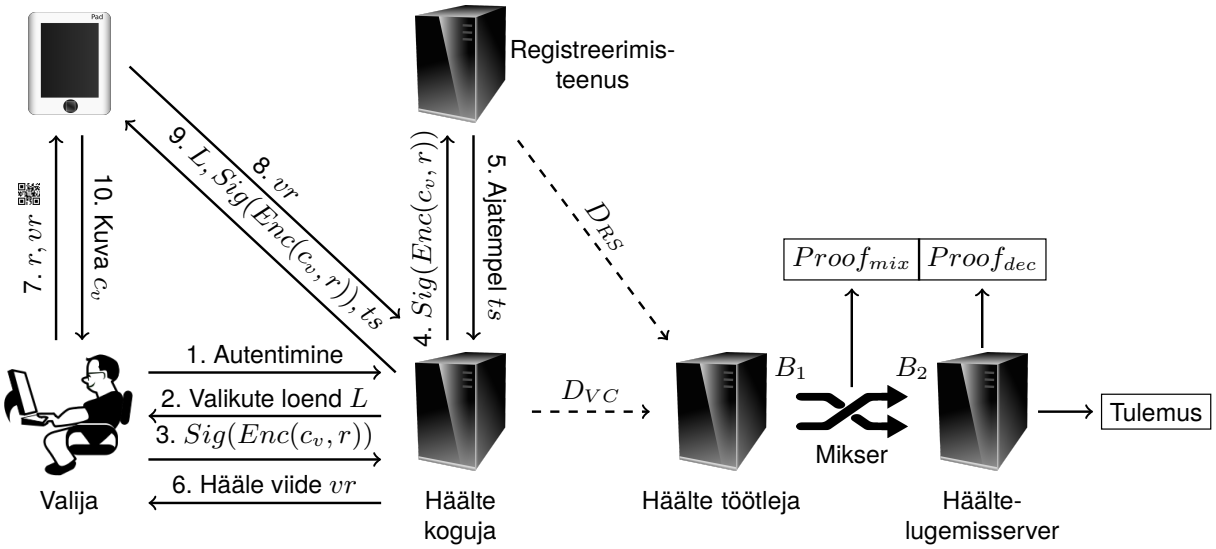
Märgime siinkohal veel, et näotuvastusalgoritmide parameetreid on reeglina võimalik modifitseerida nii, et valepositiivsete ja -negatiivsete osakaalusid muuta. Seejuures tuleb aga arvestada, et valepositiivsete osakaalu vähenedes valenegatiivsete osakaal tõuseb ja vastupidi.

Tuvastamise jõudluse osas võib optimistlikum olla. Olenevalt pakutava lahenduse arhitektuurist saab põhimõtteliselt luua Eesti i-hääletamise koormusele vastu pidava süsteemi. Kaks teenusepakkujat ütles näiteks, et neil on kasutusel mikroteenuste arhitektuur, mille abil nad on suutnud teenindada tuhandeid päringuid minutis. See jõudlus on Eesti i-hääletamise kontekstis piisav.

Küll aga tuleb arvestada, et näotuvastamine pole ise päris reaalajas toimuv operatsioon. Üks teenusepakkuja hindas automaattuvastuse keskmiseks ajaks 6 sekundit, mis inimtuvastuse korral pikeneb 20 sekundini. Arvestades, et need on keskmised hinnangud, võib i-hääletamiskogemus paljude kasutajate jaoks halveneda.

4.2 Eesti i-hääletamise süsteem

Eesti i-hääletamise süsteemi skeem on antud joonisel 2. Skeemi üksikasjaliku kirjelduse leiab huvitatud lugeja allikatest [39, 33, 31].



Joonis 2. Eesti i-hääletamise süsteemi ülevaade

Joonisele kantud sammud kirjeldavad valimisprotsessi. Skeemil tähistab c_v valija poolt tehtud valikut ja r valija arvuti poolt genereeritud juhuslikku väärtust, mida kasutatakse hääle krüptogrammi $Enc(c_v, r)$ moodustamiseks. Signeeritud krüptogramm edastatakse häältekogumisserverisse, mis võtab sellele registreerimisteenusest ajatempli ts, muutes niimoodi võimatuks häälte manipuleerimise koguja poolt.

Kui valija otsustab oma häält verifitseerida, antakse talle süsteemi poolt viide vr, mille alusel saab ta serverist krüptogrammi ja ajatempli oma mobiilseadmesse laadida. Teades juhuväärtust r, saab mobiilseade hääle väärtust auditeerida.

Pärast valimisprotsessi viiakse registreerimis- ja kogumisteenuse töö käigus tekkinud andmekogud D_{RS} ja D_{VC} häälte töötlemiseks mõeldud serverisse ning võrreldakse.

Pärast valimisperioodi lõppemist eraldatakse signatuurid krüpteeritud häältest ning miksimise abil kaotatakse ära seos signatuuridega. Miksimise tulemusena väljastatakse krüptograafiline tõestus ($Proof_{mix}$), mis näitab, et sisendiks antud krüpteeritud sedelite hulk B_1 ning väljundiks saadud rekrüpteeritud sedelite hulk B_2 on omavahel vastavuses. Seejärel dekrüpteeritakse hääled ning antakse selle kohta krüptograafiline tõestus ($Proof_{dec}$), mis näitab, et tulemus arvutati

lugemisserverisse sisestatud häältest. Niimoodi on krüptograafiliste tõestuste abil tagatud, et tulemus arvutatakse häälte töötlejast saadud ning registreerimisteenuse poolt registreeritud häälte põhjal.

Kodaniku vaatest jäljendab süsteem topeltümbrikuga posti teel hääletamist, kus sisemise anonüümse ümbriku rolli mängib hääle c_v krüptogramm $Enc(c_v, r)$ ning välimise ümbriku rolli täidab valija digitaalsignatuur $Sig(\cdot)$.

Niisugune hääletamismeetod erineb olemuslikult jaoskonnas toimuvast sedeliga hääletamisest ja see erinevus on biomeetrilise autentimise rakendamise seisukohast oluline. Sisuliselt kannab jaoskonnas pärast isikusamasuse tuvastamist valijale antav valimissedel muuhulgas autentimispileti funktsiooni. Pabersedeli enda autentsust tagatakse füüsiliste meetmetega (vesimärgid, hologrammid jm turvaelemendid).

Elektroonilises keskkonnas on täpselt samasuguste omadustega lahendust raske saavutada ja seepärast tugineb Eesti süsteem hääle autentsuse tagamisel digitaalse maailma meetoditele, eeskätt digiallkirjale. Sedeli analoogi puudumine tähendab aga seda, et meil pole protokollis loomulikku autentimispiletit, mida eduka biomeetrilise isikutuvastamise korral valijale anda.

Niisiis pole jaoskonnas toimuva valimisprotsessi mehaaniline transleerimine i-hääletamise süsteemi võimalik. Näotuvastuse kasutuselevõtmiseks tuleb langetada hulk valikuid, millel on omad eelised ja puudused, aga mis ei anna ükski täpselt samade omadustega süsteemi kui pabervalimiste korral. Järgnevas jaotises käsitlemegi olulisemaid valikukohti.

4.3 Võimalikud valikud

4.3.1 Millisel etapil näotuvastust kasutada?

Näotuvastamismeetme lisamist planeerides tuleb kõigepealt otsustada, millisel etapil seda täpselt rakendada. Jooniselt 2 näeme, et protokolli samme, mis seonduvad otseselt kasutaja tuvastamisega tema eID vahendi abil, on kaks:

- samm number 1 – autentimine häältekogumisserverisse ja
- samm number 3 – hääle krüptogrammi signeerimine.

Kaaludes näotuvastamist 1. sammul, peame lisaks otsustama, kas eID põhine autentimine jääb näotuvastuse kõrvale alles või mitte (eID-ga signeerimine 3. sammul säilib kindlasti).

Ühest küljest on valija esmane tuvastamine eID vahendiga mingis mõttes mugavusteenus, mis võimaldab efektiivselt ja täie kindlusega tuvastada kodaniku isikukoodi. Isikukoodi alusel omakorda otsustatakse kodaniku hääleõiguslikkuse üle ning selgitatakse välja, millise ringkonna kandidaatide nimekiri talle saata. Põhimõtteliselt on võimalik isikukood skaneerida ka dokumendilt (juhul kui kasutatakse dokumendipildi põhist tuvastamist) või lasta see inimesel endal sisestada (ning kontrollida pärast tema näokujutise vastavust isikute andmebaasist leitud kujutisele).

Teisalt on näotuvastuse lisamine süsteemi mõttekas ainult juhul, kui ebaõnnestunud tuvastus blokeerib hääletamisvõimaluse. See omakorda tähendab, et eID kasutamine lisaks biomeetrilisele tuvastamisele ei anna eriti midagi juurde, küll aga muudab protsessi kasutaja jaoks keerukamaks.

Kokkuvõttes, kui kaaluda näotuvastamist hääletamisprotsessi 1. sammul, soovitamegi selle sammu realiseerimist puhtalt näotuvastuse baasil.

Näotuvastamine osana sammust number 3 (hääle krüptogrammi signeerimine) on põhimõtteliselt samuti võimalik. See annab lisaks veel võimaluse siduda näotuvastuse tulemus (nt mingil kujul esitatud tuvastustõend) või näokujutis signatuuriga krüptograafiliselt. See omakorda võimaldaks näotuvastust järelauditeerida.

Niisugusel lähenemisel on ka oluline puudus. Ebaõnnestunud näotuvastamise tulemusena alles 3. sammul hääletamisprotsessi blokeerimine tähendab valija vaates halba kogemust. Valijal lastakse kandidaatide nimekiri oma arvutisse tõmmata, seda lehitseda ja valikki ära teha ning öeldakse alles seejärel, et tegelikult ta ikka ei saa hääletada.

Lisaks paneme tähele, et pabervalimiste korral pole isikutuvastuse järelauditeerimine võimalik, seega pole otsest põhjust niisugust omadust nõuda ka i-valimistelt.

Kolmas võimalus on mitte piirduda näotuvastusega pelgalt mõnel eID sammul, vaid üritada jälgida videovoo vahendusel kogu protsessi. Selline lähenemine tooks endaga kaasa hulga lisaprobleeme.

- On teada, et keskmine i-hääletamise seansi pikkus on ca 2 minutit. 99% seansse mahub ära 20 minuti sisse, aga esineb ka üksikuid ekstreemse pikkusega seansse [32]. Tipphetkel jookseb paralleelselt suurusjärgus paarsada seanssi. Niisuguse koormuse kandmine esitab süsteemipoolsele taristule suuri käideldavusnõudeid.
- Pole selge, mida ülekantavast videovoost täpselt otsida. Seda, et inimese nägu on kogu aeg otse kaadris? See pole pikema seansi puhul mõistlik nõue, lisaks ei annaks see ikkagi kindlust, et inimene hääletab ise.
- Kui me nõuaks, et videost peab olema näha kogu hääletamise protsess, tekib oht PIN-koodide või hääletaja poolt tehtud valiku lekkimiseks sellesama video kaudu. Niisugune leke pole aktsepteeritav.
- Kui inimene hääletab kodust, tekib ebaproportsionaalselt suur eraelu privaatsuse riive.
- Kas valija juhendamise vältimiseks tuleks lisaks kaamerale kasutada ka mikrofoni? Seeläbi suureneks privaatsusriive veelgi.
- Pole selge, mida teha, kui videoülekanne pole kvaliteetne ning video katkeb või hangub. Kui sel juhul peaks valija kogu seanssi otsast alustama, halvendaks see oluliselt kasutajakogemust.
- Uurisime aruande koostamise käigus ühelt kommertsiaalselt näotuvastusteenuse pakkujalt, kas turul on olemas lihtsalt kasutusse võetav lahendus, mis automaatset videovoo jälgimise ning sealt pideva näotuvastuse stsenaariumi toetaks, ja saime negatiivse vastuse.[6] See tähendab, et tuvastamiseks tuleks suure tõenäosusega kasutada inimoperaatoreid. Tippkoormuse perioodidel peaks neid operaatoreid olema kümneid. Isegi sel juhul tuleb arvestada, et inimese tähelepanu hajub ning tema võimekus kiiresti täpseid otsuseid vastu võtta pole ühtlane.

Kokkuvõttes soovitame peamise variandina kaaluda näotuvastamist protsessi esimesel, autentimissammul, asendades sellega eID põhise autentimise. Krüpteeritud hääle signeerimine eID vahendiga jääb protsessi endiselt alles, sest seda signatuuri kasutatakse protsessi edasistes etappides.

[6] See muidugi ei tähenda, et vastavat tehnoloogiat maailmas ei eksisteeriks. Erinevate riikide jõustruktuurid kasutavad valvekaamerate voogudest nägude tuvastamist juba aastaid. Siinse uuringu autoritele pole teada, kas Eesti kuulub nende riikide hulka, millel sellisele tehnoloogiale ligipääs on, või mida oleks tarvis teha, et niisugune ligipääs tekiks.

4.3.2 Kas tuvastada nägu andmebaasi või dokumendi abil?

Nagu nähtub jaotisest 4.1, on mõlemal lähenemisel oma eelised ja puudused. Kvaliteetse andmebaasi alusel tuvastamine võimaldab paremat täpsust, aga ABISe jõudlus pole hetkeseisuga piisav. Ideaalis tuleks kasutada hübriidlahendust, mis tugineks ABISe paremale andmebaasile, aga pakuks samas kommertspakkujate jõudlust koos lõppkasutajarakenduste loomiseks mõeldud teekide ja liidestega. Niisuguse lahenduse kasutuselevõtt eeldab täiendavaid läbirääkimisi teenusepakkujatega.

4.3.3 Millist seadet tuvastamisel kasutada?

Näotuvastamiseks on vaja kaamerat. Arvutite külge ühendatavate veebikaamerate ja integreeritud kaameratega sülearvutite kohta puudub usaldusväärne statistika. Ka kaameraga varustatud nutiseadmete leviku kohta on raske konkreetseid numbreid leida, kuid me hindame, et nutiseadmed on tänaseks juba rohkem levinud kui PC veebikaamerad.[7] Niisiis on näotuvastuse kättesaadavuse huvides vaja toetada nutiseadmega näotuvastust.

Teine argument nutiseadmete toetamise kasuks on pildikvaliteet. Näotuvastusteenusepakkujad rõhutasid intervjuude käigus, et nutiseadmete kaamerate lahutus on keskmisest PC veebikaamerast oluliselt parem ja see omakorda tähendab paremat tuvastustäpsust.

Eeldusel, et peamiseks hääletamisseadmeks jääb endiselt PC, tähendab eraldi seadme kasutamine näotuvastamiseks muidugi keerukamat protsessi nii kasutaja vaates kui ka hääletamisprotokolli mõttes. Näotuvastus ja hääletamine toimuvad eraldiseisvates seanssides ja nende ühendamiseks tuleb protokolli keerukamaks muuta. See omakorda lisab potentsiaalseid tõrkekohti.

Tegelikult on juba 2013. aastast olemas ka valimiste nutiseadmerakendus, mida saab kasutada hääle individuaalseks verifitseerimiseks. Kui realiseerida näotuvastus mobiilseadmekaamera abil, on mõistlik lisada see funktsionaalsus juba olemasolevale rakendusele. Positiivse kõrvalefektina võib loota, et kui valija on juba kasutanud mobiilirakendust näotuvastamiseks, siis loodetavasti kasutab ta suurema tõenäosusega ka hääle verifitseerimise võimalust.

4.3.4 Millist seadet kasutada hääletamisel?

Kui näotuvastuse sisseviimisel kasvaks nutiseadmete tähtsus i-hääletamise protsessis juba nagunii, võib küsida, kas poleks otstarbekas viiagi kogu valijapoolne rakendus mobiilplatvormi(de)le. Mobiilhääletamise teostatavust uuriti põhjalikult 2020. aastal avaldatud aruandes [28]. Praktiliselt kõik seal välja toodud probleemid on aktuaalsed ka täna:

- sõltuvus mobiilplatvormipakkuja rakenduste levitamise kanalist,
- väikese ekraaniga seotud mured,
- mobiilplatvormide madalam turvatase, palju uuendamata seadmeid,
- kontrollrakenduse kasutamine muutub ebaloomulikumaks.

Positiivse poole pealt võib välja tuua sujuvamat kasutajakogemust ja vähenevat eID pahavaralise ülevõtmise riski võrreldes näotuvastamist mitte kasutava mobiilhääletamisega. Tänase seisuga me PC-platvormil töötavast valijarakendusest loobumist siiski pigem ei soovita.

[7] Vastavalt DIGITAL 2021 aruandele oli Eestis 2021. aasta alguses 1,79 miljonit mobiilset ühendust (IoT seadmeid arvestamata). See arv ei vasta ilmselt küll üksüheselt nutiseadmetele, aga annab suurusjärgust siiski ettekujutuse; vt `https://datareportal.com/reports/digital-2021-estonia` (31.05.2021).

4.3.5 Kas ja kuidas lahendada vaideid?

Erinevalt eID vahendite abil toimuvast autentimisest ei anna näotuvastus alati ühest tulemust. Kindlasti tekivad valenegatiivsed tuvastused, mis tähendab, et osade valijate õigus hääletada blokeeritakse. Suure tõenäosusega pole valimispäeval jaoskonnas hääletamine neile kõigile sobivaks alternatiiviks, mistõttu tuleb ette näha protsessid valenegatiivsete tuvastuste kompenseerimiseks.

Põhimõtteliselt on ka paberhääletamise puhul võimalik, et jaoskonnas ei suudeta tuvastada inimese näo vastavust tema dokumendifotole. Sel juhul suunatakse probleem valla- või linnasekretärile ja kui ka tema ei oska otsustada, peab vaide lahendama Riigi Valimisteenistus (RVT). Sarnase protsessi sisseviimine i-hääletamisse eeldab otsustusõigusega ametniku valvesolekut kogu i-hääletamise perioodil (sh ööpäev läbi).

Eraldi küsimus on, kuidas seda protsessi i-hääletamise protokolli tasemel toetada. Tuleb luua eraldi liides valveametniku jaoks ning lisada protokolli sammud, mis võimaldavad näotuvastusrakendusest selle liidesega ühenduda. See muudab nii protsessi kui ka protokollistiku taaskord keerukamaks ja tõrkeohtlikumaks.

4.4 Võimalikud stsenaariumid kokkuvõtvalt

Jaotises 4.3 toodud kaalutlusi arvestades otsustasime, et keskendume neile stsenaariumitele, kus

- nägu tuvastatakse mobiilseadmega,
- hääletamine toimub PC-ga ja
- näotuvastamine on osa autentimisprotsessist, see asendab PIN1 küsimise.

Seega jääb sõelale kaks põhilist stsenaariumi.

4.4.1 Näotuvastamine dokumendi abil, hääletamine PC-ga

Protsess:

1. Valija avab PC ja selles valijarakenduse.
2. Valija avab nutiseadme ja selles näotuvastusrakenduse.
3. Valija seob kuidagimoodi valimis- ja näotuvastusseansid (näiteks valijarakendus kuvab QR-koodi, millest näotuvastusrakendus skaneerib seansivõtme).
4. Valija näitab oma dokumenti ja nägu mobiilikaamerasse, tuvastatakse isik ja tema isikukood, mis edastatakse ühendatud seansile.
5. Jätkub tavaline hääletamisprotokoll, kus PIN1 enam ei küsita.

4.4.2 Näotuvastamine andmebaasi abil, hääletamine PC-ga

Protsess:

1. Valija avab PC ja selles valijarakenduse.
2. Valija sisestab valijarakendusse oma isikukoodi.

    - Alternatiivina, kui valija sisestab ID-kaardi lugejasse, võidakse isikukood lugeda otse ID-kaardilt.
3. Valijarakendus kuvab QR-koodis seansivõtme, valija skaneerib selle mobiilseadmega ja näitab mobiilikaamerasse oma nägu.
4. Tuvastamisteenus kontrollib andmebaasi vastu, et antud isikukoodile vastab kaamerast leitud nägu.
5. Jätkub tavaline hääletamisprotokoll, kus PIN1 enam ei küsita.

4.4.3 Võimalikud alternatiivsed lahendused

Lisaks kahele ülaltoodud stsenaariumile võib kaaluda ka alternatiive.

Esimene võimalus on lubada (ka) PC külge ühendatud veebikaamera kasutamist. Ühest küljest kaotaks see vajaduse siduda omavahel kahes erinevas seadmes toimuvad seansid ja protokoll muutuks seeläbi lihtsamaks. Teisest küljest tuleb tänu paremale pildikvaliteedile ja laiemale levikule nutiseadmeid nagunii toetada ja mitme alternatiivse lahenduste teostamine pole vähemalt esimese prototüübi korral mõistlik. Kui biomeetrilist tuvastamist otsustatakse katsetada, soovitame esimese pilootrakenduse ehitada nutiseadmete kaameratele; PC-kaamerate võimekuse lisamist võib kaaluda järgmistes etappides.

Kui lähiaastad toovad kaasa märkimisväärse arengu mobiilseadmete turvatasemes, siis võib tulevikus uuesti kaaluda ka mobiilhääletamise võimalust. Muuhulgas võimaldaks see lahendus mugavamalt integreerida mobiilseadme-põhist näotuvastust. Hetkel (2021. aasta seisuga) me mobiilhääletamist siiski veel ei soovita.

4.5 Mõju kasutajakogemusele

Täiendavate sammude lisamine hääletamisele muudab protsessi valija jaoks kindlasti keerukamaks, tõrkeohtlikumaks ja ebamugavamaks.

- Näotuvastuseks tuleb kasutada kas integreeritud kaamerat sisaldavat arvutit, USB-liidesega ühendatavat veebikaamerat või kaamerat sisaldavat mobiilseadet. Ei saa eeldata, et kõigil lauaarvutit omavatel valijatel on välised veebikaamerad või nutitelefonid. Niisugused valijad võivad näotuvastuse nõude korral i-hääletamiselt kõrvale jääda.
- PC külge ühendatav USB-veebikaamera või mobiilseade tähendavad täiendavat vahendit, mis tuleb hääletamiseks valmis seada ja mille võimalik tõrge toob endaga kaasa probleeme.
- Näotuvastuseks vajalik videovoog nõuab küllalt korralikku kasutajapoolset internetiühendust, mida tänases Eestis kahjuks ikka veel kõikjal eeldada ei saa.
- Hääletamisprotokolli lisandub uusi samme, mis võib tekitada segadust ning lisada kohti, kus protsess tõrgub.
- Täisautomaatne näotuvastus pole kontrollimatus keskkonnas mõeldav. Tuvastusprotsessi suunamine inimoperaatorile tekitab samas lisaviivituse. Tavatingimustes piirdub see lisaviivitus paarikümne sekundiga, kuid hääletamise tipp-perioodidel võib see tänu inimoperaatorite piiratud jõudlusele märgatavalt pikeneda.
- Peale ratsionaalsete kaalutluste mõjutab valijakogemust ka subjektiivne hinnang privaatsusriivele, mis tekib paratamatult, kui riik hakkab nõudma pilte või videovoogu sadadelt tuhandetelt valijatelt.

- Kui kasutada näotuvastuslahendust, mis nõuab dokumendilt kaameraga info lugemist, siis vajab see küllaltki täpset kaamera suunamist ja paigalhoidmist. See tegevus ei pruugi olla jõukohane eakamatele või erivajadustega valijatele.

5 Õiguslikud küsimused

5.1 Analüüsi ulatus

Selle analüüsi lähte-eelduseks on olemasoleva elektroonilise hääletamise tehnilise raamistiku põhitunnuste ning hääletamispõhimõtete säilitamine. Tellija poolt ei ole väljendatud soovi valimiste põhiseaduslike printsiipide (nt vabaduse ja salajasuse põhimõtete) ümberkujundamiseks. Pigem on siinse arutelu eesmärgiks analüüsida, kas ja millisel viisil võimaldab näotuvastuse lisamine elektroonilise hääletamise protseduuridesse isikute tuvastuskindlust parendada tagamaks, et valija eest ei hääletataks ilma tema teadmise ja nõusolekuta (vt jaotis 3).

Näokujutist biomeetriliselt töödelda ning selle alusel isikut tuvastada on võimalik erinevates keskkondades:

1. kontrollitud keskkonnas füüsilist tuvastusseadet ja/või eelnevalt tuvastamise eesmärgil ehitatud tehnilist lahendust kasutades või
2. kaugteel, kontrollimata keskkonnas, kasutades isiku valitud tehnilisi vahendeid ning võimalusi (nt kodus, töö juures, avalikus ruumis vms).

Siinne analüüs keskendub eelkõige kaugteel isiku tuvastamisele, mis on elektroonilise hääletamise tingimusi arvesse võttes ainuke võimalik lahendus.

Võimalikke teostatavaid tehnilisi lahendusi analüüsisime jaotises 4.3. Tulemusena leidsime, et tehnilise teostatavuse seisukohast on hetkel mõistlik valida kahe alternatiivi vahel.

1. Näotuvastust kasutatakse isikusamasuse kontrollimiseks riigi andmekogus hoitavate biomeetriliste andmetega võrdlemise teel (edaspidi *näotuvastamine andmebaasi abil*).
2. Näotuvastus viiakse läbi teenusepakkuja poolse teenusena, kus võrreldakse valija enda pildistatavat isikut tõendavat dokumenti isikust hääletamise ajal tehtud foto või lühivideoga (edaspidi *näotuvastamine dokumendi abil*).

Mõlema lahenduse korral asendaks pakutu praeguses protokollis esimese astme tuvastamisviisi, mis põhineb isiku digitaalset tuvastamist võimaldava sertifikaadi kasutamisel PIN1 sisestamisega.

Käesolevas peatükis keskendume õiguslikele võimalustele nende lahenduste teostamiseks.

Analüüs on üles ehitatud järgmiselt:

- esmalt esitatame analüüsi aluseks olevad lähtekohad, sh lühikokkuvõtte kehtivast õigusest ja selle pinnalt tekkivatest küsimustest, mis väljuvad analüüsi raamest;

- seejärel esitatame lähtekohtadele tugineva õigusliku analüüsi, milles hindame andmebaasi ja dokumendi abil näotuvastamise proportsionaalsust Eesti Vabariigi põhiseaduse §11 alusel.

5.2 Lähtekohad

5.2.1 Hääletamisõiguse olemus

Põhiseaduse järgi on hääleõigus igal Eesti teovõimelisel kodanikul, kes on saanud vähemalt 18 aastat vanaks [9, §57]. Hääleõigus on isikuga seotud põhiõigus – seda ei saa teisele isikule üle anda [26, Par 57, p 8]. Hääleõigus hõlmab rahvahääletamisel osalemise õigust ja valimisõigust, neist viimane omakorda hääletamisõigust (aktiivne valimisõigus) ja kandideerimisõigust (passiivne valimisõigus) [26, Par 57, p 6]. Lähtuvalt uuringu fookusest keskendume siinses analüüsis hääletamisõigusele.

Hääletamisõigus kaitseb valijat eelkõige riigi sekkumise eest tema vaba tahte väljendamisse. Hääletamisõigusele vastab riigi kohustus luua selle õiguse perioodiliseks kasutamiseks vajalikud tingimused (eelkõige sätestada printsiipidele vastav hääletamiskord), mis lähtuvad valimiste vabaduse, ühetaolisuse, üldisuse, otsesuse ja hääletamise salajasuse põhimõtteist [20]. Kõik valimisseadused (nende hulka loetakse ka rahvahääletuse seadus) rakendavad kõikide hääletamisviiside põhiseaduslike printsiipide tagamise mehhanisme. Erandina on elektroonilise hääletamise detailne regulatsioon toodud Riigikogu valimise seaduse (*RKVS*) peatükis 7^1 ning see laieneb teistele valimisseadustele viiteliselt. Enamik valimisõiguse põhimõtetest laieneb nii aktiivsele kui ka passiivsele valimisõigusele [26, Par 60, p 1].

5.2.2 Elektroonilise hääletamise eripärad

Elektrooniline hääletamine on üks Eestis kehtestatud hääletamisviisidest, mida kasutatakse kõikidel valimiseaduste alusel korraldatud valimistel ja rahvahääletustel.

Elektroonilise hääletamise rakendamisel tuleb sarnaselt teiste hääletamisliikidega järgida kõiki valimisõiguse põhiseaduslikke printsiipe [26, Par 60, p 46-47]. Samas tuleb arvestada, et inimeste täieliku võrdsuse tagamine valimisõiguse teostamisel ei ole põhimõtteliselt võimalik ega põhiseaduslikult nõutav [19]. Traditsioonilisel viisil (valimisjaoskonna hääletamiskabiinis) ja elektrooniliselt (Internetis väljaspool valimisjaoskonda) hääletavad valijad on sisuliselt erinevas olukorras – esimesel juhul toimub hääletamine kontrollitud, teisel juhul aga kontrollimata keskkonnas. Võrreldes traditsioonilise hääletamisega on elektroonilise hääletamise puhul keerulisem tagada valimiste vabaduse ja hääletamise salajasuse põhimõtet [19, p 23, 24, 28]. Selle ületamiseks on elektroonilise hääletamisviisi kasutajatele antud õigus oma häält piiramatu arv kordi muuta ning arvesse võetakse valija ajaliselt viimane antud hääl [19, p 30]. Lisaks on valijal võimalik oma häält muuta pabersedeliga hääletamisruumis hääletades. Aastatel 2005-2020 sai valija oma häält muuta vaid eelhääletamise päevadel, kuid alates 2021. aastast saab valija oma elektroonilist häält pabersedeliga valimisjaoskonnas muuta lisaks eelhääletamisele ka valimispäeval.

Põhiseaduse kommentaaride autorite hinnangul peab valimiste usaldusväärsuse tagamiseks Interneti teel hääletamine vastama järgmistele tingimustele [26, Par 60, p 49]:

1. valija isik ja hääleõiguslikkus on tuvastatud,
2. igal valijal on üks hääl,
3. valija on saanud hääletada vabalt,

4. tagatud on häälte salajasus,
5. hääl loetakse ning hääletamis- ja valimistulemused tehakse kindlaks korrektselt.

See analüüs puudutab eelkõige esimest tingimust (valija isiku ja hääleõiguslikkuse tuvastamine), kuid mõjutab ka hääletamise vabadust ja salajasust.

5.2.3 Näotuvastus kui isikusamasuse kontrollimise viis

Hetkel kehtiva õiguse kohaselt on Eestis võimalik valijat, kes kasutab elektroonilist hääletamist, tuvastada seaduse alusel väljastatud digitaalse dokumendiga [26, Par 60, p 57]. Seda reguleerivad isikut tõendavate dokumentide seaduse (*ITDS*) §18[1] ning volitusnormi sisaldav Riigikogu valimise seadus (*RKVS*) §48[4] lõige 2, mis annab Vabariigi Valimiskomisjonile (*VVK*) õiguse määratleda, millises korras isik elektroonilise hääletamise süsteemis tuvastatakse. Isikut tõendavaks dokumendiks on mh ka isikutunnistus ehk ID-kaart, millele kantakse digitaalset tuvastamist võimaldav sertifikaat ning digitaalset allkirjastamist võimaldav sertifikaat [14, §2 lg 2 p 1, §19[1] lg 1].

ITDS §18[1] lg 1 kohaselt tehakse dokumendi kasutaja isikusamasuse kontrollimisel dokumendi kasutaja isik kindlaks dokumenti kantud andmete ning isiku võrdlemise teel. Sama sätte järgi võib isikusamasuse kontrollimisel võrrelda dokumendi kasutajalt võetud biomeetrilisi andmeid dokumenti kantud biomeetriliste andmetega. Seejuures pole täpsemalt reguleeritud, kas mõeldakse dokumendi kiibile kantud biomeetrilisi andmeid (nt tulevikus lisatakse ID-kaardi kiibile ka näokujutis ja kaks sõrmejälge) või rakendub see vahetult dokumendi füüsilisele andmekandjale kantud andmetele (nt foto, allkirjakujutis). Samuti pole täpsustatud, kas kontrolli peab teostama inimene või võib seda teha ka automatiseeritud lahendus (masin).

ITDS §18[1] lg 2 näeb ette täiendava tuvastamisviisi – dokumendi kasutaja isikusamasuse digitaalne kontrollimine –, mis toimub digitaalset tuvastamist võimaldava sertifikaadi abil. Digitaalse kontrollimise puhul tuleb eeldada, et lähtuvalt selle tuvastamisviisi olemusest saab isikusamasust tuvastada üksnes automatiseeritud lahendus. ITDS §18[1] lg 3 sedastab, et avalik-õigusliku teenuse elektroonilisel osutamisel on õigus nõuda ITDSi alusel välja antud isikutunnistusele, elamisloakaardile või digitaalsele isikutunnistusele kantud digitaalset tuvastamist ja digitaalset allkirjastamist võimaldava sertifikaadi kasutamist. Kui isik keeldub digitaalset tuvastamist ja digitaalset allkirjastamist võimaldava sertifikaadi kasutamisest, võib jätta talle avalik-õigusliku teenuse osutamata.

Digitaalset kontrolli rakendatakse hetkel ka elektroonilisel hääletamisel. Valija peab hääletamiseks sisse logima hääletamisrakendusse, kasutades digitaalset tuvastamist võimaldavat sertifikaati, mis nõuab PIN1 koodi sisestamist. Kui ta seda ei tee, siis hääletada ei ole võimalik. Vastav protseduur on ette nähtud VVK otsusega kehtestatud tehnilistes nõuetes elektroonilise hääletamise korraldamise üldpõhimõtete tagamiseks [18, §48[2] lg 3 p 1, §48[4] lg 2].

Täiendavat analüüsi vajavad järgmised küsimused.

- Kas VVK-l on elektroonilisel hääletamisel kasutatava tuvastamisviisi otsustamisel laiendatud diskretsiooniõigus otsustada ka ITDS-is ning e-identimise ja e-tehingute usaldusteenuste seaduses (*EUTS*) reguleerimata isikutuvastusviiside kasuks? Senine menetluspraktika ning VVK otsustusloogika on lähtunud üldseadusega reguleeritud või volitusnormi alusel välja antud isikutuvastusvahenditest. Üldseadusega reguleerimata vahendite lisamisel tuleks samuti hinnata sarnase regulatsiooni rakendamise vajadust tavahääletamise puhul, hääletamiskohtades, tagamaks mh valimiste ühetaolisuse põhimõtte täitmist. Pa-

bersedeliga hääletades ei ole praeguse praktika kohaselt võimalik ITDS-is reguleerimata dokumendiga isikut tuvastada.

- Kas isikut tõendavate dokumentide andmekogus olevaid biomeetrilisi andmeid on võimalik kasutada ITDSis ning EUTSis reguleerimata isikutuvastusviiside puhul? Dokumendi kasutaja kohta dokumendi väljaandmise menetluse käigus kogutud biomeetriliste andmete töötlemine on lubatud ainult seaduses sätestatud juhtudel ja tingimustel [14, §9[2] lg 5]. Üheks selliseks seaduses sätestatud juhuks on töötlemine isikut tõendavate dokumentide andmekogus [14, §15[2] lg 1]. Ka elektroonilise hääletamise kontekstis on mõeldav lubada ITDSi alusel kogutud biomeetriliste andmete töötlemist vastavas valimisseaduses kehtestatud õiguslikul alustel (sellist alust hetkel valimisseadustes ei ole).
- Kui elektroonilisel hääletamisel võetakse kasutusele uus isikutuvastusviis – näotuvastamine andmebaasi või dokumendi abil –, siis kas see eeldab, et tuleb muuta ka Eesti poolt Euroopa Komisjonile nn eIDAS määruse [13] alusel teavitatud e-identimise süsteeme või teatada uutest e-identimise süsteemidest? Elektroonilistelt võivad Riigikogu valimistel ja ravhahääletustel hääletada üldjuhul ainult Eesti kodanikud, kes saavad oma isikut tõendada ainult Eestis tunnustatud eID vahendiga. Muu ELi liikmesriigi kodanik on hääleõiguslik kohaliku omavalitsuse volikogu valimistel ning Euroopa Parlamendi valimistel. Eestis elav ELi mittekuuluva riigi kodanik või kodakondsuseta isik saab hääletada kohaliku omavalitsuse volikogu valimistel, kuid ei saa volikokku kandideerida[8]. Seega tekib küsimus, kas eIDAS määrus [13] kohaldub nendel juhtudel, kus elektroonilisel hääletamisel saavad osaleda teiste riikide kodanikud. Kui jah, siis järgmine küsimus on, milliseid teiste riikide e-identimise viise peaks Eesti riik eIDASe alusel tunnustama, et lubada nende riikide kodanikel osaleda elektroonilisel hääletamisel Eesti kohaliku omavalitsuse volikogu valimistel ning Euroopa Parlamendi valimistel. Sellega seonduvalt kerkib ka küsimus, kas selleks, et lihtsustada teiste riikide kodanikel Eesti elektroonilisel hääletamisel osalemist, tuleks uuendada Eesti e-identimise süsteeme.
- Kuidas mõjutab näotuvastamine andmebaasi või dokumendi abil valija kui isikuttõendava dokumendi kasutaja ja e-identimise sertifikaadi omaniku nö omavastutust dokumendi ja sertifikaadi õige kasutamise eest?
- Kuidas mõjutab näotuvastamist andmebaasi või dokumendi abil see, kui ID-kaardile lisatakse täiendavaid biomeetrilisi andmeid (näokujutis ja kaks sõrmejälge)? Alates 02.08.2021 hakkab kehtima uus määrus nr 2019/1157 [12], mis reguleerib isikutunnistuste ja elamislubade turvalisuse suurendamist ning laieneb ka Eestis elektroonilisel hääletamisel kasutatavatele ID-kaartidele. Selle määruse järgi võivad isikutunnistuse andmekandjale salvestatud biomeetrilisi andmeid kasutada pädevate asutuste ja Euroopa Liidu asutuste nõuetekohaselt volitatud töötajad kooskõlas liidu ja liikmesriigi õigusega üksnes selleks, et kontrollida isikutunnistuse ehtsust ja dokumendi omaniku isikusamasust otseselt kättesaadavate võrreldavate tunnuste abil, kui isikutunnistuse esitamine on õiguse kohaselt nõutav.
- Kuidas mõjutab näotuvastamist andmebaasi abil see, kui võetakse vastu Siseministeeriumi poolt välja töötatud eelnõu ITDSi ja teiste seaduste muutmiseks, millega tehakse muudatusi 14 seadusesse eesmärgiga luua õiguslik alus ABIS andmekogu asutamiseks [2]?
- Kuidas mõjutab näotuvastamist dokumendi abil see, kui võetakse vastu EUTSi, ITDSi ning riigilõivuseaduse muutmise seadus[9], mis on selle aruande kirjutamise ajal (mai 2021) Riigikogu menetluses?

[8] `https://www.valimised.ee/et/valimiste-meelespea/haaleoigus` (31.05.2021)

[9] E-identimise ja e-tehingute usaldusteenuste seaduse, isikut tõendavate dokumentide seaduse ning rii-

5.2.4 Näokujutis kui isikuandmed

Alates 25.05.2018 reguleerib isikuandmete töötlemist Euroopa Liidu liikmesriikides otsekohalduv isikuandmete kaitse üldmäärus (*General Data Protection Regulation*, GDPR) [11]. GDPR määratleb biomeetrilised andmed kui konkreetse tehnilise töötlemise abil saadavad isikuandmed isiku füüsiliste, füsioloogiliste ja käitumuslike omaduste kohta, mis võimaldavad kõnealust füüsilist isikut kordumatult tuvastada või kinnitavad selle füüsilise isiku tuvastamist, näiteks näokujutis ja sõrmejälgede andmed [11, Art 4 p 14]. Isiku näokujutist sisaldavad fotod on hõlmatud biomeetriliste andmete määratlusega üksnes siis, kui neid töödeldakse konkreetsete tehniliste vahenditega, mis võimaldavad füüsilist isikut kordumatult tuvastada või autentida [11, põhjenduspunkt 51].

Biomeetrilised andmed, sh näokujutis, on eriliiki isikuandmed, mida on üldjuhul keelatud töödelda [11, Art 9 lg 1]. Erandid on lubatud ainult GDPR artikkel 9 lg-s 2 loetletud juhtudel, kusjuures liikmesriikidel on õigus kehtestada täiendavaid tingimusi ja piiranguid seoses biomeetriliste andmete töötlemisega [11, Art 9 lg 4].

Biomeetriliste andmete (nagu näokujutis) töötlemisel tuleb läbi viia andmekaitsealane mõjuhinnang [11, põhjenduspunkt 91, Art 35 lg 3 b)]. Üldjuhul on andmekaitsealane mõjuhinnang nõutav juhtudel, kus isikuandmete töötlemise, eelkõige uut tehnoloogiat kasutava töötlemise, tulemusena tekib füüsiliste isikute õigustele ja vabadustele suur oht, arvestades töötlemise laadi, ulatust, konteksti ja eesmärke [11, Art 35 lg 1]. Sellise ohu olemasolu eeldatakse, kui isikuandmeid töödeldakse automaatselt, selle põhjal hinnatakse süstemaatiliselt ja ulatuslikult füüsiliste isikute isiklikke aspekte ning tehakse otsuseid, millel on füüsilise isiku jaoks õiguslikud tagajärjed või mis samaväärselt mõjutavad oluliselt füüsilist isikut, samuti avalike alade ulatuslikul süstemaatilisel jälgimisel ning isikuandmete eriliikide, sh biomeetriliste andmete töötlemisel. Nimetatud juhtudel ei ole vastutaval töötlejal võimalust mõjuhinnangu läbiviimisest loobuda [11, Art 35 lg 3 a)-c)].

Vastavalt GDPR artikkel 35 lg-le 7 peab andmekaitsealane mõjuhinnang hõlmama vähemalt järgmist:

1. kavandatud isikuandmete töötlemise toimingute ja töötlemise eesmärkide süstemaatiline kirjeldus;
2. isikuandmete töötlemise toimingute vajalikkuse ja proportsionaalsuse hindamine eesmärkide suhtes;
3. andmesubjektide õigusi ja vabadusi puudutavate ohtude hinnang ning
4. ohtude käsitlemiseks kavandatud meetmed, sealhulgas tagatised, turvameetmed ja mehhanismid isikuandmete kaitse tagamiseks ja GDPRi järgimise tõendamiseks, võttes arvesse andmesubjektide ja teiste asjaomaste isikute õigusi ja õigustatud huve.

Lisaks nõuab GDPR artikkel 35 lg 9, et vastutav töötleja küsiks asjakohasel juhul ka andmesubjektide või nende esindajate seisukohti kavandatava töötlemise kohta, ilma et see piiraks ärivõi avalike huvide kaitset või isikuandmete töötlemise toimingute turvalisust. Täpsemad nõuded andmekaitsealase mõjuhinnangu protsessile ja soovitused selle läbiviimiseks on kehtestanud

gilõivuseaduse muutmise seadus 376 SE. Eelnõu. https://www.riigikogu.ee/tegevus/eelnoud/eelnou/3372edbf-3201-44b6-99b3-8a0c90e177f2/E-identimise%20ja%20e-tehingute%20usaldusteenuste%20seaduse,%20isikut%20t%C3%B5endavate%20dokumentide%20seaduse%20ning%20riigil%C3%B5ivuseaduse%20muutmise%20seadus (26.05.2021)

Artikkel 29 Andmekaitse Töögrupp [1], kelle juhiseid on tunnustanud ka Euroopa andmekaitsenõukogu [22, p 6].

Eraldiseisva andmekaitsealase mõjuhinnangu tegemine ei ole kohustuslik ainult juhul, kui Euroopa Liidu või liikmesriigi õiguses on kehtestatud õiguslik alus, mis reguleerib kõnealust kõrge riskiga isikuandmete töötlemist ja andmekaitsealane mõjuhinnang on teostatud selle õigusliku aluse vastuvõtmise raames läbiviidud üldise mõjuhinnangu osana [11, Art 35 lg 9]. Näiteks kui näotuvastuse kasutuselevõtuks elektroonilisel hääletamisel muudetakse Eestis kehtivat valimisõigust ja vastava eelnõu ettevalmistamise raames viiakse läbi ka andmekaitsealane mõjuhinnang, siis ei ole täiendava mõjuhinnangu läbiviimine hiljem vajalik. Küll aga võib see vajadus kerkida juhul, kui toimub oluline muudatus eelnõu raames tehtud mõjuhinnangu aluseks olnud asjaoludes või riskiprofiilis, näiteks kui arendatakse välja uued näotuvastustehnoloogiad [1].

5.2.5 Näotuvastuse lisandumine kui oluline muudatus (valimis)õiguses

Näotuvastuse kasutamine isikusamasuse tuvastamiseks on kasvav trend. COVID-19 levikuga kaasnenud kriis on veelgi suurendanud vajadust mugavate, kuid samas tõsikindlat tuvastamist võimaldavate lahenduste järgi ja näotuvastus pakub siin uusi võimalusi. Erasektoris on viimaste aastate jooksul turule tulnud palju erinevaid näotuvastusel põhinevaid teenusepakkujaid. Nende peamiseks klientuuriks on erasektori organisatsioonid, kes vajavad abi inimeste isiku kindlakstegemisel. Biomeetria-põhised identifitseerimisviisid kontrollimata keskkonnast on kasutusel nt pankades [4, 21] ja notaribüroodes [17]. Kontrollitud keskkonnas toimuvat näotuvastust kasutatakse piiratud ulatuses ka avalikus sektoris. Näiteks võeti hiljuti käiku automatiseeritud piirikontrolli väravad Tallinna lennujaamas ja Narva maanteepiiripunktis [8].

Hoolimata laienevast kasutusalast ei ole näotuvastust Eesti õigusruumis põhjalikult reguleeritud. Kui ITDS välja arvata, on näokujutise töötlemist seaduse tasandil käsitletud veel vaid liiklusseaduses ja välismaalaste seaduses, sedagi uue dokumendi taotlemiseks või kättesaamiseks vajaliku isikusamasuse tuvastamise kontekstis. ELi õiguses on näotuvastust reguleeritud lisaks GDPRile veel ka Schengeni ala reguleerivates õigusaktides piiriületusel isikusamasuse kontrollimise kontekstis ning kriminaalmenetluse piiriüleses koostöös. Seega õiguslikust vaatest on tegemist nähtusega, mida on seni reguleeritud pigem rangelt valdkonnapõhiselt. Uue regulatsiooni kehtestamine näotuvastuse kasutuselevõtuks elektroonilise hääletamise kontekstis laiendaks näotuvastuse regulatsiooni seni reguleerimata valdkonda. Konteksti erinevuse tõttu ei saa siin tugineda varasema regulatsiooni eeskujule – näotuvastus elektroonilisel hääletamisel vajab iseseisvat lähenemist. Sellega seoses tekib küsimus loodava regulatsiooni ulatusest – kas see peaks laienema üksnes elektroonilisele hääletamisele või ka muudele (avalikele) teenustele?

Analüüsi üheks ajendiks olnud nn hooldekodude küsimus kerkib lisaks elektroonilisele hääletamisele ka muudel kasutusjuhtumitel, kus vanemaealised vajavad abi elektroonilise identifitseerimisvahendi kasutamisel. Näiteks võivad kõrges eas vanemad anda oma ID-kaardi (lapse)lapse või hooldekodu töötaja valdusse, et teostada igapäevaseid pangatehinguid või vaadata terviseandmeid patsiendiportaalis. Ka nimetatud paari näite puhul on vaja tagada, et kaardiomanik kasutab oma kaarti ise või kasutab selleks kõrvalist abi nii, et järgitakse kaardiomaniku tahet. Seega vajadus tagada, et inimene kasutab oma ID-kaarti ise, esineb mitte ainult elektroonilise hääletamise puhul, vaid ka muudes olukordades. Kui elektroonilisel hääletamisel näotuvastuse kasutuselevõtu eesmärgiks on täita nõuet, et inimene peab oma ID-kaarti ise kasutama, siis see ei ole valimisõiguse ainuvajadus.

Hetkel kehtiva regulatsiooni kohaselt kasutatakse elektroonilise hääletamise juures tuvastusla-

hendusi, mis on universaalsed, pikaajalise kasutusajalooga ning laialdaselt kasutusel ka teiste riiklike teenuste juures. Näotuvastuse lisamine oleks kõrvalekalle sellest väljakujunenud praktikast, kuivõrd näotuvastuse kasutamine ei ole veel nii laialt levinud, eriti riiklikes teenustes. Õigusselguse ja õiguskindluse huvides tuleks esmalt läbi analüüsida biomeetrilise (kaug)näotuvastuse õiguslik staatus ja reguleerimisvajadus Eesti õiguses tervikuna ning seejärel hinnata eriseadustes ja spetsiifilisi teenuseid reguleerivates õigusaktides sellise tuvastusviisi sätestamise üksikasju.

Valimisseaduste muutmisel tuleb lisaks tähele panna erinõudeid, et muudatused oleks sisse viidud aegsasti enne valimisi (hea rahvusvahelise tava kohaselt vähemalt 1 aasta või minimaalselt 6 kuud enne järgmisi valimisi) [26, Par 60, p 109][3]. Samuti on oluline rõhutada, et elektrooniline hääletamine ja valimiskorraldus laiemalt on olulisel määral kasutajate usaldusele ning tunnetuslikule usaldatavusele tuginevad lahendused. Seni riiklikes teenustes laialdaselt rakendamata ning väljakujunemata kasutajakogemusega näotuvastusteenuse rakendamine esmakordselt (katseliselt) elektroonilise hääletamise juures võib kaasa tuua ennustamatuid tagajärgi kasutajakogemusele ning seeläbi valimisosalusele laiemalt.

5.3 Õiguslik analüüs

5.3.1 Analüüsi ulatus

Näotuvastuse lisamine elektroonilise hääletamise protseduuridele toob endaga paratamatult kaasa mitmeid võimalikke põhiõiguste ja -vabaduste kaitseala riiveid (edaspidi *riived*), mille lubatavust tuleks iga konkreetse lahenduse valikul põhjalikult analüüsida. Kuivõrd praeguse analüüsi fookuseks on näotuvastuse kasutuselevõtt Eesti elektroonilise hääletamise teenuses, siis lähtume riivete määratlemisel ja lubatavuse hindamisel põhiseaduse §-st 11. Järgmistes analüüsides, kui on leitud põhiseadusega kooskõlaline lahendus näotuvastuse kasutuselevõtuks, tuleb võimalikke riiveid analüüsida ka rahvusvahelise õiguse ja inimõiguste valguses. See puudutab eriti muude ELi liikmesriikide kodanike (kohalike omavalitsuste volikogude ja Euroopa Parlamendi valimistel) ning Eestis püsivalt elavate teiste riikide kodanike või kodakondsuseta isikute (kohalike omavalitsuste volikogu valimistel) õiguste riivet.

Siinses uuringus saab käsitleda selliseid võimalikke riiveid, mis seonduvad näotuvastamisega dokumendi või andmebaasi abil ning on teada analüüsi valmimise hetkel. Samal ajal tuleb arvestada määramatusega järgmistes küsimustes.

1. **Näotuvastus kui sotsiaalne nähtus on alles kujunemisjärgus.** Näotuvastuse kasutamine isikusamasuse tuvastamiseks ei ole üksnes elektroonilise hääletamise keskne probleem, vaid puudutab potentsiaalselt kõiki elualasid. Tegemist on tehnoloogiavaldkonnaga, mis on avalikus sektoris seni kasutust leidnud vaid väga piiratud juhtumitel (isikut tõendavate dokumentide taotlemine ja kontroll, rahvusvaheline koostöö kriminaalmenetluses, reisimine). Erasektoris on näotuvastuse kasutamine sisuliselt reguleerimata (tegemist on poolte vahel võlaõiguslikult kokkulepitud reeglite alusel toimuvate tehingutega), mis on võimaldanud erinevate näotuvastuslahenduste laialdast levikut, kuid sellega on kaasnenud ka kõrgendatud ohud põhiõigustele. Esimesed seonduvad vaidlused on teistes riikides juba kohtusse jõudnud [38], kuid Eestis vastavat kohtupraktikat autoritele teadaolevalt veel pole. Seega puudub nii rahvusvahelisel kui ka siseriiklikul tasandil välja kujunenud hea tava näotuvastuse rakendamiseks kooskõlas kõikide juriidiliste ja eetiliste normidega, olgu siis avalike või eraõiguslike teenuste puhul.

2. **Vajadus reguleerida kõrvalise isiku abi elektrooniliste avalike teenuste kasutamisel.** Kogu uuringu üheks motivatsiooniks on nn hoolekodude juhtum, kus osadelt klientidelt korjatakse ID-kaadid hoiule (vt jaotis 3). Selline praktika on mõistetav olukorras, kus hooldekodu kliendid ei suuda kas tervislikel või muudel põhjustel ise tagada oma ID-kaardi turvalist säilitamist ning hooldekodu pakub selleks oma abi. Küsimus kerkib aga juhtumitel, kus hoolealused vajavad abi ka ID-kaardi kasutamisel, nt rahaasjade ajamisel netipangas, retseptide tellimisel ja nende alusel ravimite ostmisel, sotsiaaltoetuste taotlemisel jne. Sarnaseid küsitavusi võivad põhjustada ka olukorrad, kus ID-kaarte haldavad vanemaealiste pereliikmed ja lähedased – puuduvad selged ja ühtsed reeglid, mis tingimustel võib osutada kõrvalist abi elektrooniliste identifitseerimisvahendite kasutamisel. Seega nn hooldekodude juhtum illustreerib laiemat probleemide ringi Eesti ühiskonnas. Ühelt poolt on erinevate elektrooniliste lahenduste kasutus nii avaliku kui ka erasektori teenustes lihtsustanud nende inimeste elu, kellel on kõrge vanuse, haiguse, puude, eemalviibimise tõttu või muul põhjusel raskendatud teenuse saamiseks isiklikult kohale ilmumine. Teisalt ei ole kõik teenused alati kohandatud eri ühiskonnagruppide vajadustele[10]. Mida rohkem selliseid teenuseid pakutakse, seda enam kasvab vajadus ka kõrvalise isiku abi järele, vähemalt seni, kuni elektrooniliste teenuste disainis ei ole kohustust arvestada erivajadustega. Hetkel kehtiv õiguslik raamistik ei toeta elektroonilise hääletamise korral sellise abi osutamist, ilma et abistaja peaks riskima väär- või koguni kuriteo toimepanemisega [15, §157[2], §165, §166, §349]. Samas on kõrvalise abi võimalust tunnustatud näiteks hääletamissedeli täitmisel valimisjaoskonnas [18, §39 lg 7]:

   > *Valija täidab hääletamissedeli ise. Kui valija ei ole füüsilise puude tõttu võimeline hääletamissedelit ise täitma, võib seda tema palvel ja tema juuresolekul teha teine valija, kuid mitte tema elukohajärgse valimisringkonna kandidaat.*

   Kõrvalise abi osutamist võiks sarnasel moel reguleerida ka elektroonilisel hääletamisel, kuid see vajaks eelnevalt põhjalikku analüüsi ja tõenäoliselt ka avalikku diskussiooni, sest tegemist oleks olulise valimisvabaduse (salajasuse) riivega.

Ülalkirjeldatud määramatuse tingimustes ei anna järgnev analüüs ammendavat vastust küsimusele riivete lubatavusest, sest paljud hindamise aluseks olevad asjaolud on kas selgumisel või muutumises. Sellegipoolest on analüüsi koostamisel püütud ette näha võimalikke tuleviku arengusuundi ja pakutud viise, kuidas riiveid omavahel tasakaalustada. Senise informatsiooni täpsustumisel ja uue informatsiooni selgumisel tuleks ka riived uuesti kaardistada ning nende lubatavust muutunud asjaolude valguses uuesti hinnata.

5.3.2 Püstitatud küsimused

Lähtuvalt eeltoodust on analüüsi keskmes järgmised küsimused.

1. Milliseid võimalikke põhiõiguste ja -vabaduste riiveid toob endaga kaasa näotuvastuse lisamine elektroonilise hääletamise protseduuridesse analüüsis pakutud viisidel?
2. Kas need riived on proportsionaalsed?

Järgnevas analüüsis käsitletakse mõlemat küsimust nii näotuvastamisel andmebaasi kui ka dokumendi abil. Keskendutakse üksnes nendele võimalikele riivetele, mis kaasnevad näotuvastuse

[10] Juhime tähelepanu, et ühiskonna erinevate rühmade poolt elu- ja infokeskkonna võimaluste kasutamise uurimiseks on loodud ka Riigikantselei ligipääsetavuse rakkerühm `https://riigikantselei.ee/ligipaasetavus` (24.05.2021).

lisamisega olemasolevatele elektroonilise hääletamise protseduuridele. See tähendab, et analüüsi raames ei hinnata võimalikke riiveid, mis on põhjustatud hetkel kasutusel olevate elektroonilise hääletamise lahenduste poolt. Eeldame, et vastavad hinnangud on teostatud varasemalt või tuleks läbi viia eraldiseisvalt.

5.3.3 Võimalikud riived

5.3.3.1 Hääletamisõiguse riived

Hääletamisõigus kaitseb valijat põhiseaduse §57 alusel eelkõige riigi sekkumise eest tema vaba tahte väljendamisse ning paneb riigile kohustuse sätestada valimisprintsiipidele vastav hääletamiskord (vt jaotis 5.2.1). Kui senisele hääletamiskorrale lisatakse näotuvastuse nõue, siis see riivab valija hääletamisõigust niivõrd kuivõrd näotuvastus piirab või takistab tema vaba tahte väljendamist. Niisugune riive tuleb kõne alla eelkõige juhtudel, kus valijat jälgitakse hääletamisõiguse teostamise ajal. Jälgimine võib põhjustada valijas ärevust ja teda survestada, isegi kui see ei ole suunatud konkreetse valiku tegemisele. Sarnast ärevust on kirjeldatud näiteks COVID-19 tingimustes kaamera jälgimise all toimunud eksamite korral [27]. Samasugust reaktsiooni võib eeldada ka dokumendi abil näotuvastamise ühe alternatiivi puhul, kus elektroonilise hääletamise protsessi jälgitakse algusest lõpuni videovoo vahendusel (vt jaotis 4.3.1).

Valija vaba tahte väljendamise tagamiseks on valimisõiguses kasutusel ka hääletamise salajasuse printsiip. Eesti valimisõigus lähtub põhimõttest, et hääletamise salajasus pole eesmärk omaette, vaid see kindlustab hääletamise vabaduse põhimõtet [37]. Hääletamise salajasus toetub kahele alampõhimõttele – hääletamistoimingu privaatne sooritamine ja hääle anonüümsus [41].

Videovoo-põhise alternatiivi puhul tekib vastuolu hääletamistoimingu privaatse sooritamise alampõhimõttega, sest valija ei saa oma valikut teha välistest tema poolt kontrollimatutest faktoritest segamata. Elektroonilise hääletamise puhul on mõjutuskindluse tagamise peamiseks vahendiks hääle muutmise võimalus ning hääletamiseks sobivaima (ja privaatseima) keskkonna valiku vabadus (nn virtuaalne hääletamiskabiin). Katkematu videovoo või enda ja tahtmatult ka oma ümbruse pildistamise tingimustes on sellise keskkonna valik valija jaoks oluliselt raskendatud.

Kõne alla tuleb ka hääle anonüümsuse alampõhimõtte rikkumine, kui näotuvastusel kajastatakse valija hääle sisu. Sõltuvalt valija teadmistest, oskustest, arusaamadest ja hoiakutest pole välistatud, et foto või videovoo tegemiseks kasutatav kaamerasilm on paigutatud või seadistatud moel, mis kuvab valija arvutiekraani koos isiku nime või muu vastusevariandiga, mille poolt valija oma hääle andis või kavatseb anda. Valija võib ka muul moel avaldada oma valiku sisu, näiteks unustades valitud poliitiku nimega märkmepaberi kaamera vaatevälja või näidates näotuvastuse jaoks foto tegemisel oma soosiku nimega plakatit.

5.3.3.2 Era- ja perekonnaelu ning kodu puutumatusega seotud riived

Omaette grupi moodustavad isiku privaatsust puudutavad põhiõigused, mida kaitsevad vastavalt põhiseaduse §26 (era- ja perekonnaelu puutumatus) ning §33 (kodu puutumatus). Näotuvastuse lisamisel on suur tõenäosus riivata mõlemat nimetatud põhiõigust, kui valija hääletab elektrooniliselt oma kodus ja/või oma perekonnaliikmete juuresolekul või nende vahetus läheduses. Riive oht on eriti kõrge siis, kui näotuvastust teostatakse videovoo abil – hääletamisprotsessi kestel võivad lisaks valijale sattuda kaadrisse ka tema (alaealised) lapsed, abikaasa või elukaaslane, vanemad, sõbrad ja muud lähedased, kes konkreetsesse hääletamistoimingusse ei puutu, vaid elavad taustal oma igapäevaelu. Samuti võimaldab näotuvastus – nii foto kui ka videovoona –

saada infot valija kodusest keskkonnast ja interjöörist, mis võib omakorda anda infot valija varalisest seisundist (nt hinnaline mööbel, tuntud kunstniku maal seinal), väärtustest ja tõekspidamistest (nt religioosse tähendusega esemed riiulitel, plakatid lemmikkangelastest), isegi geograafilisest asukohast (nt vaade aknast tänavale või kõrvalmajja). Selline lisainfo on kitsalt elektroonilise hääletamise eesmärgist lähtuvalt ebavajalik.

Lisaks tuleb arvestada, et ka näokujutis iseseisvalt – olgu foto või videovoona – võimaldab isiku kohta teada saada informatsiooni, mis ei ole seotud ainult tema identiteediga. Näiteks võib inimese näost välja lugeda tema rassilist kuuluvust, sugu, emotsionaalset seisundit, haigusi, geneetilisi tunnuseid ja kõrvalekaldeid, teatud ainete tarvitamist jne. Valija ei saa sellise info kogumist vältida, s.t see on näotuvastuse protseduuri vaikimisi nö sisse ehitatud [25] – info võib avalduda juba üksnes valijast näotuvastusel tehtud fotolt, rääkimata videovoost. Järelikult on tõenäoline, et isiku kohta kogutakse näotuvastusel üleliigset infot, mida pole elektrooniliseks hääletamiseks tegelikult vaja.

5.3.3.3 Kaitsepõhiõiguse riived

Näotuvastuse lisamine elektroonilisele hääletamisele võib teatud tingimustel kaasa tuua ka põhiseaduse §-st 13 tuleneva kaitsepõhiõiguse riive. Selline riive esineb juhul, kui seadus ei sätesta põhiõiguse kandjale vajalikku kaitset [26, Par 13, p 12].

Nagu 4. jaotises välja tõime, kaasneksid näotuvastusega mitmed uued riskid. Näiteks võib juhtuda, et näokujutise pildistamise või videovoo salvestamise käigus jäädvustatakse valija poolt sissetoksitav PIN-kood või kandidaadi number, kelle poolt ta hääle andis. Samuti on võimalik, et kõrvalised isikud jäädvustavad valija nägu eesmärgiga anda tema nimel hääl tema enda teadmata. Inimene ei pruugi aru saada, et tema poole suunatud mobiilseadme kaamerat kasutatakse tema kui valija tuvastamiseks. Samuti on võimalik, et valija nägu tuvastatakse ja tema nimel antakse hääl olukorras, kus ta on ise teadvuseta või ei suuda muul põhjusel enda eest hääletamist ära hoida.

Lisaks täiendavatele riskidele peab näotuvastuse lisamisel arvestama, et seeläbi töödeldakse ka täiendavat hulka isikuandmeid – isiku näokujutis, tema hääletamiskeskkond ning selles viibivad teised isikud jne. Isegi kui vastav isikuandmete töötlemise õiguslik alus on kehtestatud seadusega ega vaja isiku nõusolekut, peab sellegipoolest tagama vajalikud GDPRiga ettenähtud andmesubjekti õigused, näiteks õigus saada teavet isikuandmete töötlemise kohta [11, Art 12-14], õigus andmetega tutvuda [11, Art 15], õigus andmete parandamisele [11, Art 16], õigus andmete kustutamisele [11, Art 17], õigus töötlemise piiramisele [11, Art 18], õigus esitada vastuväiteid [11, Art 21] jne. Kas ja mil määral võib andmesubjekti õigusi ja muid GDPRist tulenevaid kohustusi seoses näotuvastuse kasutuselevõtuga piirata [11, Art 23, Art 6 lg-d 2-3], tuleb eraldi analüüsida (näiteks tulevikus näotuvatuse kasutuselevõtuks õiguslikku alust võimaldava seaduseelnõu ettevalmistamise raames).

Kirjeldatud riskide maandamiseks ja isikuandmete töötlemiseks peab riik kasutusele võtma täiendavaid kaitsemeetmeid, vastasel korral võib olla tegemist kaitsepõhiõiguse riivega. Näiteks tuleb ette näha protsessid valenegatiivsete tuvastuste kompenseerimiseks (vt jaotis 4.3.5) ning näotuvastusel kasutatud isikuandmete töötlemise kohta vastuväidete esitamiseks. Täiendavate kaitsemeetmete valik eeldab eraldiseisvat analüüsi, mis väljub siinse aruande käsitlusalast. Kuna kaitsepõhiõiguse riive on praeguses etapis üksnes teoreetiline võimalus, mis sõltub tulevikus selguvate kaitsemeetmete proportsionaalsusest, siis me seda aruandes põhjalikumalt ei käsitle.

5.3.4 Riivete proportsionaalsus

Riive olemasolu ei tähenda tingimata selle õigusvastasust. Riive on põhiseadusega kooskõlas, kui see on proportsionaalne. Proportsionaalse riivega on tegemist siis, kui see täidab järgnevaid nõudeid [26, II peatüki sissejuhatus]:

1. sellel on legitiimne eesmärk,
2. see on sobiv eesmärgi saavutamiseks,
3. see on vajalik ning
4. mõõdukas (proportsionaalne kitsamas mõttes).

5.3.4.1 Legitiimne eesmärk

Riivete proportsionaalsuse hindamiseks tuleb esmalt määratleda riive eesmärk. Lähtuvalt probleemipüstituse peatükis toodust (vt jaotis 3) on näotuvastuse lisamise peamiseks otstarbeks vähendada valija eest elektroonilise hääle andmist ilma tema teadmise ja nõusolekuta, seda nii näotuvastamisel dokumendi kui ka andmebaasi abil toimuva tuvastuse puhul. See on omakorda seotud vajadusega tagada avalik usaldus elektroonilise hääletamise protsessi vastu ja seeläbi kindlustada demokraatlikku korda Eestis.

Eesmärgi legitiimsus sõltub põhiõigusest, mida piiratakse [26, Par 11, p 22]. Ülal tuvastasime kaks peamist põhiõiguste riivete gruppi.

1. **Hääletamispõhiõiguse riive** Tegemist on seadusereservatsioonita põhiõigusega, mille piiramisel võib olla legitiimne üksnes põhiseaduses otseselt või kaudselt ette kirjutatud eesmärk [26, Par 11, p 22]. Valija õige tuvastamine täidab valimiste üldisuse [26, Par 60, p 56] ja ühetaolisuse [26, Par 60, p 57] tagamise eesmärke, mis tulenevad põhiseaduse §-st 60 ja on seega legitiimsed eesmärgid.
2. **Era- ja perekonnaelu ning kodu puutumatuse riived** Nii põhiseaduse §26 kui ka §33 on kvalifitseeritud põhiõigused, mille puhul legitiimsed eesmärgid on loetletud vastavates sätetes endis.
    - Era- ja perekonnaelu põhiõiguse piiramine on põhiseaduse §26 järgi lubatud seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks.
    - Kodu puutumatust võib piirata seadusega sätestatud juhtudel ja korras avaliku korra, tervise või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks, kurjategija tabamiseks või tõe väljaselgitamiseks kriminaalmenetluses.

    Kummalgi juhul ei sisalda legitiimsete eesmärkide loetelu võimalust piirata põhiõigust konkreetselt demokraatliku korra tagamise huvides, rääkimata elektroonilise hääletamise vajadustest lähtuvalt (valija teadmata ja nõusolekuta tema eest hääle andmine). Kõige lähemal seisvaks eesmärgiks võiks lugeda mõlemas sättes nimetatud avaliku korra kaitse eesmärki, kuid see ei kohalduks antud konteksti. See ei oleks kooskõlas elektroonilise hääletamise (ja valimiste kui terviku) kui privaatse iseloomuga avaliku teenuse olemusega. Samuti ei oleks kuriteo tõkestamine või kurjategija tabamine eesmärgid, mis võiks õigustada laiaulatuslikku ja kõikidele valijatele ühetaoliselt rakenduvat näotuvastust [10]. Seega põhiseaduse §26 ja 33 ei sisalda legitiimset eesmärki, mis lubaks neid põhiõigusi elektroonilisel hääletamisel näotuvastuse lisamisega piirata.

Sellegipoolest leitakse põhiseaduse kommentaarides, et "*[k]a kvalifitseeritud seadusereservatsiooniga põhiõigusi saab riivata teistel, sättes loetlemata alustel, kui eesmärk seondatakse mõne põhiseaduse sättega, st näidatakse, et tegu on n-ö põhiseaduslikku järku väärtusega.*" [26, Par 11, p 22] Niisiis tekib küsimus, mis võiks olla see põhiseaduslikku järku väärtus, mis õigustaks era- ja perekonnaelu ning kodu puutumatuse põhiõiguste riivet sellisel kujul nagu seda eeldab näotuvastamine dokumendi või andmebaasi abil.

Autorite hinnangul võiks selliseks põhiseaduslikku järku väärtuseks olla põhiseaduse §-s 60 sätestatud valimiste vabaduse põhimõte, mille kohaselt peab kõigil valimistel osalejatel olema võimalik veenduda hääletamise ja selle tulemuste usaldusväärsuses [26, Par 60, p 52]. Sellega seondub ka elektroonilisel hääletamisel kasutatava süsteemi üldine usaldusväärsus [26, Par 60, p 54]. Näotuvastuse kasutuselevõtt on suunatud hääletamise ja selle tulemuste ning hääletamist võimaldava süsteemi usaldusväärsuse parandamisele.

Lisaks tulevad põhiseaduslikku järku väärtustena kõne alla valimiste üldisuse ja ühetaolisuse põhimõte, mis on samuti sedastatud põhiseaduse §-s 60. Valimiste üldisuse põhimõtet tagatakse kõigile kättesaadava valija elektroonilise tuvastamise võimaluse loomise kaudu [26, Par 60, p 56]. Valimiste ühetaolisuse põhimõtte kohaselt tuleb mh valija isik hääletamisel üheselt tuvastada [26, Par 60, p 57]. Seega, kui olemasolev tuvastamisviis – seaduse alusel väljastatud digitaalse dokumendi alusel – asendatakse uue tuvastamisviisiga – näotuvastamine dokumendi või andmebaasi abil –, on see suunatud valimiste üldisuse ja ühetaolisuse saavutamisele.

Eelnevast tulenevalt oleks antud tingimustel legitiimse eesmärgi nõue täidetud nii näotuvastamisel dokumendi kui ka andmebaasi kasutamise korral.

5.3.4.2 Sobivus

Riive eesmärgi saavutamiseks taotletav abinõu on sobiv, kui see soodustab vastava eesmärgi saavutamist [26, Par 11, p 31]. Riigikohtu selgituste järgi on sobivuse nõude sisuks kaitsta isikut avaliku võimu tarbetu sekkumise eest – piisab sellest, et eesmärki on põhimõtteliselt võimalik vaidlusaluse meetmega saavutada [26, Par 11, p 36].

1. **Hääletamispõhiõiguse riive** Sobivuse kriteeriumi täitmiseks peaks senise tuvastamisviisi asendamine näotuvastamisega dokumendi või andmebaasi abil soodustama valimiste üldisuse ja ühetaolisuse tagamise eesmärke. Selline soodus mõju kaasneb juhul, kui näotuvastuse lisamine aitab kaasa valija elektroonilise tuvastamise võimaluse kättesaadavusele (valimiste üldisuse põhimõte) [26, Par 11, p 56] ning valija ühesele tuvastamisele hääletamisel (valimiste ühetaolisuse põhimõte) [26, Par 11, p 57].

    a. **Elektroonilise tuvastamise võimaluse kättesaadavus (valimiste üldisuse põhimõte)** Võrreldes olemasoleva, digitaalsel kontrollimisel põhineva tuvastamisega, kus isikult ei nõuta tema näo või näokujutise näitamist kaamerasse, oleks näotuvastuse puhul tegemist lahendusega, kus valija peab rakendama lisatehnikat ja -oskusi, et hääletamisteenusele ligi pääseda. Teatud ühiskonnagruppide jaoks eeldab see üsna järsku õppimiskõverat, mille läbimine on eelduseks elektroonilisel hääletamisel osalemisele. Nende gruppide jaoks ei aita näotuvastuse lisamine elektroonilise tuvastamise võimalust kättesaadavamaks teha.

    Tuvastamise võimaluse kättesaadavust raskendab näotuvastuse lisandumisel ka täiendava seadme (foto- ja/või video jäädvustamise funktsionaalsusega mobiiltelefon) nõue. See seade peab täitma näotuvastuseks aktsepteeritava kvaliteediga foto-

või videojäädvustuse tegemiseks teatud tingimusi. Kõik valijad ei pruugi omada sellistele tingimustele vastavat isiklikku seadet. Praktikas on valijal võimalik näotuvastuseks kasutada ka teise isiku seadet, kuid see tähendab potentsiaalselt hääle andmise protsessi osalist väljumist valija enda kontrolli alt.

Seega, näotuvastamine nii dokumendi kui ka andmebaasi abil põhimõtteliselt võimaldab valija ühest tuvastamist ning on seega sobiv meede valimiste üldisuse saavutamiseks. Samas ei ole võimalik üheselt väita, et valija elektrooniline tuvastamine muutuks tänu näotuvastusele paremini (lihtsamini) kasutatavaks või kättesaadavamaks võrreldes olemasoleva tuvastamisviisiga.

b. **Valija ühene tuvastamine (valimiste ühetaolisuse põhimõte)** Hääletamisprotsessi alul valija biomeetrilise autentimise sisseviimise motivatsiooniks oli soov visuaalselt veenduda, et hääletamisel osaleb sama isik, kellele kuulub elektrooniline identifitseerimisvahend. Paneme aga tähele, et pärast biomeetrilist autentimist on eID vahendi üleandmine endiselt võimalik. Samuti on nn hooldekodu juhtumil täiesti võimalik saada kaamera ette vanainimene, kes kogu protseduuri otstarvet täiel määral ei adu.

   Näotuvastuse praktikast on teada, et see protsess ei ole 100% täpne, alati esineb teatav hulk valepositiivseid ja -negatiivseid tuvastusi (vt jaotised 4.1.1 ja 4.1.2). Samuti võivad esineda teatud erijuhtumid, kus näotuvastuse teel ei saa valijat üheselt kindlaks teha (nt kaksikud, näol avalduvate haigustunnustega isikud).

   Kuna empiirilised võrdlusandmed puuduvad, siis on raske hinnata, kas selline uus tuvastamisviis parandab valija ühest tuvastamist võrreldes olemasoleva tuvastamisviisiga. Küll aga võib öelda, et kummalgi juhul on võimalik võrreldava jõupingutusega hääletada mõne valija nimel tema teadmise ja nõusolekuta.

   i) Praegu kasutusel oleva elektroonilise tuvastamisviisi puhul peaks pahatahtlik ründaja lisaks ID-kaardi valdusele saama teada ka valija PIN-koodid. Seda rünnet saab ennetada, kui kehtestada täiendavad organisatsioonilised meetmed ID-kaartide ja PIN-koodide haldamiseks (nt kehtestada (pool)kinnistes asutustes ID-kaartide haldamise ja elektroonilise hääletamise kord) ning jõustada tugevamalt hetkel kehtivaid regulatsioone (nt seadusest tulenev kohustus peatada sertifikaadid nendel ID-kaartidel, mis pole inimese enda kontrolli all). Põhimõtteliselt võib kaaluda ka uute meetmete sisseviimist (nt kontroll, et valija tagasisidekanal oleks aktiivses kasutuses), aga nende otstarbekohasust tuleb sel juhul täiendavalt analüüsida.

   ii) Uue tuvastamisviisi – näotuvastamisel andmebaasi või dokumendi alusel – puhul tuleks lisaks ID-kaardi omastamisele näidata valija nägu hääletamisel kasutatava kaamera ees. Rünnet saab läbi viia ka nii, et valija ei pea olema tingimata teadvusel ega enda pildistamisest või filmimisest teadlik.

   Eelneva põhjal saab järeldada, et näotuvastamine nii dokumendi kui ka andmebaasi abil (võttes arvesse tehnilisi piiranguid) võimaldaks valija ühest tuvastamist ning valimiste ühetaolisuse põhimõtte tagamine oleks seeläbi võimalik. Samas ei saa väita, et elektrooniline tuvastamine muutuks tänu näotuvastusele täpsemaks või kindlamaks võrreldes olemasoleva tuvastamisviisiga. Mõlemat tuvastusviisi on võimalik teatud jõupingutusega rünnata. Küll aga saab öelda, et praegu kasutusel olevat elektroonilist tuvastamisviisi on võimalik tõhustada ka väheminvasiivsete vahenditega kui näotuvastuse lisamine.

2. **Era- ja perekonnaelu ning kodu puutumatuse riive** Sobivuse kriteeriumi täitmiseks peaks senise tuvastamisviisi asendamine näotuvastamisega dokumendi või andmebaasi

abil soodustama valimiste vabaduse tagamise eesmärki. Selline soodus mõju kaasneb juhul, kui näotuvastuse lisamine aitab kaasa hääletamise ja selle tulemuste ning hääletamist võimaldava süsteemi usaldusväärsusele.

Näotuvastamine kui valija tuvastamise viis võib valijale olla paremini tajutav ja mõistetav lahendus kui tuvastamine digitaalse dokumendi abil. Seda eelkõige tänu igapäevapraktikas levinud lahendustele, kus näotuvastust kasutatakse tarbijale suunatud teenustes (nt nutitelefoni ja arvutisse sisselogimine või näotuvastust nõudvate mobiilirakenduste kasutamine). Tänu varasemale kasutajakogemusele teistes valdkondades võib näotuvastus teatud valijagruppidele olla aktsepteeritavam ja mugavam lahendus kui olemasolev digitaalse dokumendi põhine tuvastamine. Nendes kasutajagruppides aitaks näotuvastuse lisamine parandada ka hääletamist võimaldava süsteemi arusaadavust ja seeläbi selle usaldusväärsust.

Samas ei ole kõik näotuvastusteenused sarnaselt üles ehitatud ning hõlmavad endas erinevaid riske. See, milline on tarbija jaoks aktsepteeritav tuvastusvahend igapäevastes eraelulistes toimingutes (nt pangateenuste kasutamine, suhtlusvõrgustikud jne), ei pruugi olla samavõrd aktsepteeritav avalike teenuste puhul, eriti kui tegemist on sedavõrd kriitilise teenusega nagu elektrooniline hääletamine. Võimalikku näotuvastusega kaasnevat valijate usaldusmäära muutust elektroonilise hääletamise süsteemi suhtes tuleks edaspidi sotsiaalteaduslike meetoditega põhjalikumalt uurida (nt valijaküsitlused, konsultatsioonid ekspertidega jms).

Eelneva põhjal saab järeldada, et näotuvastamine nii dokumendi kui ka andmebaasi abil oleks sobiv viis hääletamise ja selle tulemuste ning hääletamist võimaldava süsteemi usaldusväärsuse tagamiseks, aidates kaasa valimiste vabaduse põhimõtte tagamisele. Samas ei ole antud aruande raames võimalik hinnata, mil määral see aitaks elektroonilise hääletamise usaldusväärsust tõsta – selline hinnang vajab täiendavaid uuringuid.

Eeltoodu põhjal võib järeldada, et sobivuse nõue on täidetud näotuvastamisel nii dokumendi kui ka andmebaasi kasutamise korral.

5.3.4.3 Vajalikkus

Põhiõigusi piirav abinõu on vajalik, kui taotletavat eesmärki ei ole võimalik saavutada mõne teise, isikut vähem koormava abinõuga, mis on vähemalt sama efektiivne kui esimene [26, Par 11, p 31].

Esmalt juhime tähelepanu, et dokumendi abil näotuvastamise videovoo-põhine alternatiiv ei ole vajalik – ega lõppkokkuvõttes proportsionaalne – lahendus, kuivõrd sama efektiivset tulemust võimaldab ka dokumendi abil näotuvastamise foto-põhine alternatiiv, mis on valijatele vähem koormav nii privaatsuse aspektist kui ka hääle salajasuse aspektist. Lisaks esinevad kaalukad tehnilised ja organisatsioonilised põhjused, kus videovooga saavutatav võimalik lisaväärtus isikute täpsema tuvastamise näol ei kaalu üles ressursse, mis tuleb rakendada videovoo-põhise näotuvastussüsteemi loomiseks ja ülalpidamiseks (vt jaotis 4.3.1).

Teiseks märgime, et puuduvad kaalukad põhjused, mis sunniksid välistama hetkel elektroonilisel hääletamisel kasutatavat tuvastamisviisi (digitaalsel kontrollimisel põhinevat autentimist) kui sama efektiivset ja vähem koormavat alternatiivi näotuvastamisele dokumendi või andmebaasi abil. Proportsionaalsuse testi eelmises astmes – sobivuse hindamine – asusime seisukohale, et näotuvastus ei paranda oluliselt valija elektroonilise tuvastamise võimaluse kättesaadavust ega valija ühest tuvastamist; ka selle panus elektroonilise hääletamise süsteemi usaldusväärsuse

tõstmisse on ebaselge. Seetõttu leiame, et olemasolev tuvastamisviis on endiselt sobiv abinõu, et vähendada valija eest elektroonilist hääletamist ilma tema teadmise ja nõusolekuta. Samas mööname, et leidub mitmeid võimalusi olemasoleva lahenduse parandamiseks.

Jaotises 3.1 on välja toodud võimalikke alternatiivseid lahendusi, mis täidavad näotuvastuse lisamisega vähemalt osaliselt sama eesmärki, s.o aitavad vähendada valija eest elektroonilise hääle andmist ilma tema teadmise ja nõusolekuta, seda nii näotuvastamisel dokumendi kui ka andmebaasi abil. Siinkohal käsitleme mõnesid neist lähemalt.

Sõltumatu tagasisidekanali sisseviimine Valija vaatest oleks tegemist teavitusega, mis saabub näiteks valija e-postiaadressile või mobiiltelefonile SMSina juhul, kui valija nimel on antud hääl (olgu elektroonilisel hääletamisel või muul viisil hääletades). Seeläbi saab valija teada, kui tema nimel on hääle andnud keegi teine (sh juhul kui valija ise ei osalenud hääletamisel). See omakorda võimaldab võtta kasutusele meetmeid oma hääletamisõiguse kaitseks (nt pöörduda kaebusega politseisse, RVT või VVK poole või kohtusse, taotleda oma e-identifitseerimise ja e-allkirjastamise sertifikaatide peatamist või kehtetuks tunnistamist) ning minna kordushääletama.

Näotuvastus ja tagasisidekanal on oma olemuselt erineva toimemehhanismiga meetmed. Kui näotuvastus toimub enne hääle andmist ja ennetab väärkasutust, siis sõltumatu tagasisidekanal rakendub pärast hääle andmist ja võimaldab rünnet tuvastada (vt jaotis 3.1). Seejuures tagasisidekanal on seda efektiivsem, mida laiemalt ta kasutuses on. Arvestades, et Eesti riigil on olemas valdava osa hääleõiguslike kodanike kontaktandmed (vt jaotis 3.1), on näotuvastus ja tagasisidekanal kui inimese eest tema teadmata hääle andmise vastu võitlemise meetmed võrreldava efektiivsusega. Siinkohal mängib olulist rolli ka võimalus eID väärkasutuse tuvastamisel oma häält elektrooniliselt või pabersedeliga muuta.

Paneme tähele, et näotuvastus oleks mõne stsenaariumi puhul isegi nõrgem meede kui tagasisidekanal. Kui näotuvastuse korral õnnestub petturil kasutada nii valija näokujutist kui ka tema eID-d, läheks petturi poolt valija nimel antud hääl arvesse ilma, et valija sellest teada saaks. Tagasisidekanal on aga üldine ja universaalne meede, mis edastab hääle andmise fakti kõigile valijatele, sh ka neile, kelle eest on antud hääl nende teadmata ja nõusolekuta. Nn hooldekodu stsenaariumi välistamiseks võib põhimõtteliselt kaaluda hooldekodu kliendi eest hääletamise fakti teavituse saatmist ka tema lähedastele. Kuidas selline meede mõjutaks vanurite valimisvabadust üldisemas kontekstis, vajab eraldi analüüsi.

Lisaks tuleb hinnata ka alternatiivse meetme koormust valijale. Tagasisidekanal on võrreldes näotuvastusega oluliselt vähem koormav, sest puudub vajadus valija näokujutise ja muu taustainfo töötlemiseks.

Tuleb arvestada, et nii näotuvastusel kui ka tagasisidekanalil on ka teisi funktsioone. Tagasisidekanal pakuks täiendavaid tõendeid valimiste ajal ja järel toimuvaks järelevalvemenetluseks, sh valimispettuste tuvastamiseks ja petturite vastutusele võtmiseks. Näotuvastus on aga mõeldud eelkõige isikusamasuse tuvastamiseks tuvastusprotsessi osana ning vajadust isiku näokujutise pikemaajaliseks salvestamiseks ei ole. Siiski oleks tulevikuperspektiivis mõeldav, et näotuvastusel saadud näokujutis (lühiajaliselt) salvestatakse, et oleks võimalik järelkontrolli teostamine olukorras, kui valija näokujutis ei kattu häälele digiallkirja andnud isiku omaga. Hääletamisprotseduuri ei ole võimalik sellisel juhul küll lõpule viia, kuid petmiskatsest saadud tõendid võimaldaks menetluse algatamist. Kas selline lahendus oleks proportsionaalne, vajab tulevikus eraldi hindamist.

Laiemas kontekstis on järgmine samm **üldine eID kaitsemehhanismide arendamine**. Kehtiva

õiguse kohaselt käsitletakse isikut, kellele on väljastatud isikuttõendav dokument, sellise dokumendi kasutajana ning tema vastutus dokumendi kasutamise eest on piiratud. Olukorras, kus eteenuseid pakutakse üha laialdasemalt, tuleks kaaluda isikut tõendava dokumendi kasutaja omavastutuse suurendamist, aga seda loomulikult koos kasutajale pakutavate kaitsemehhanismide valiku laiendamisega. Näiteks on mõeldav teavituse sisseviimine alati, kui inimese nimel on antud digitaalallkiri. Vastav analüüs väljub siinse aruande raamidest, kuid selle tulemused aitaksid kaasa ka antud aruandes tõstatatud probleemide ja määramatuse lahendamisele seoses elektroonilise identiteedi kasutamisega.

Teadlikkuse tõstmine ja koostöö parandamine Kehtiva õiguse alusel on valijal võimalik pettuse kahtluse korral pöörduda politsei, RVT, VVK, Andmekaitse Inspektsiooni, usaldusteenuse pakkuja, ID-kaardi väljaandja või kohtu poole ning lisaks menetluslikult taotleda oma e-identifitseerimise ja e-allkirjastamise sertifikaatide peatamist või kehtetuks tunnistamist. Neid võimalusi tuleb valijatele veelgi rohkem teadvustada ja tutvustada. Samuti tuleb i-hääletamise üldise turvataseme tõstmiseks valijaid rohkem teavitada oma hääle kontrollimise ja hääle muutmise võimalustest.

Olulise üldise meetmena tuleks kaaluda valimiste-aegse hea tava kokkuleppe sõlmimist valitsusasutuste, valimiste korraldajate ja hoolekandeasutuste vahel, et teadvustada riske ning pakkuda paremaid lahendusi elektroonilist tuvastamist võimaldavate isikut tõendavate dokumentide hoiustamisel.

Näiteks ID-kaartide tsentraalsel hoiustamisel hooldekodu administratsiooni poolt ei pruugi hooldekodu kliendid õigeaegselt teada saada, kui nende ID-kaartidega on midagi juhtunud. Tavaolukorras on kaardi kasutajal kohustus teavitada dokumendi välja andnud valitsusasutust 24 tunni jooksul, kui ID-kaart on muutunud kasutamiskõlbmatuks, läinud kaotsi või hävinud [14, §14 lg 2]. Sellele vastab ID-kaardi välja andnud asutuse kohustus tunnistada ID-kaart kasutamiskõlbmatuks muutumise, kadumise või hävimise korral kehtetuks [14, §13 lg 1 4) ja 6), §15 lg 4 ja 5]. Hooldekodu näite puhul võiks kaaluda ööpäevaringse teatamiskohustuse seadmist hooldekodu administratsioonile, kes peaks ühtlasi informeerima hooldekodu kliente. Kui hävimine või kaotsiminek toimub mitme hooldekodu kliendi ID-kaartidega valimiste ajal, siis pole välistatud, et nad kaotavad võimaluse elektrooniliselt hääletada ning see võib omakorda mõjutada valimistulemust. Järelikult tuleb püüda ennetada juhtumeid, kus korraga muutub kasutuskõlbmatuks suur hulk ID-kaarte.

Eeltoodu põhjal saame teha järelduse, et vajalikkuse nõue pole täidetud näotuvastamisel ei dokumendi ega ka andmebaasi abil, sest paralleelselt olemasoleva (s.o digitaalsel kontrollimisel põhineva) tuvastamisviisiga saab kohaldada vähemalt üht võrreldava efektiivsusega, aga vähem koormavat meedet – sõltumatut tagasisidekanalit. Koosmõjus täiendavate meetmetega (ülehääletamise võimalus, teadlikkuse tõstmine ja koostöö parandamine) on see alternatiivne meede piisav, et saavutada näotuvastuse lisamisega taotletud eesmärki, s.o vähendada valija eest elektroonilise hääle andmist ilma tema teadmise ja nõusolekuta.

5.3.4.4 Mõõdukus

Proportsionaalsuse testi viimane etapp on hinnata riive mõõdukust. Selle üle otsustamiseks tuleb kaaluda ühelt poolt põhiõigusse sekkumise ulatust ja intensiivsust, teiselt poolt aga eesmärkide tähtsust [26, Par 11, p 31].

Mööndes, et siinse aruande aluseks olevas lähteülesandes ei täpsustatud näotuvastuse lisamise lõppeesmärke, sõnastasid aruande autorid selleks eesmärgiks vajaduse piirata valija eest elekt-

roonilise hääle andmist ilma tema teadmise ja nõusolekuta. Sellest eesmärgist lähtuvalt leidsime, et näotuvastus on küll sobiv meede, aga esineb vähem koormav ja võrreldavalt efektiivne meede, mis muudab näotuvastuse kasutuselevõtu elektroonilisel hääletamisel ebavajalikuks. Seetõttu ei ole põhimõtteliselt tarvis proportsionaalsuse testi viimast astet – mõõdukuse hinnangut – teostada.

Isegi juhul kui peaks esinema asjaolud ja argumendid, mis võimaldavad väita, et näotuvastuse lisamine on vajalik (nt kui vähem koormav ja võrreldavalt efektiivne meede langeb ära), on aruande koostajad seisukohal, et kokkuvõttes tooks näotuvastuse lisamine praktikas kaasa rohkem uusi probleeme, kui aitaks lahendada olemasolevaid. Toome siinkohal välja järgmised põhjused.

1. Kuigi nn hooldekodude stsenaarium on meedias populaarne argument, pole ühtegi juhtumit õnnestunud kinnitada ei politseiuurimise ega logianalüüsi käigus (vt jaotis 3). Kui see stsenaarium mõnikord harva ka esineb, siis mitte nii palju, et õigustada kogu i-hääletamise süsteemi ümbertegemist.
2. Elektrooniline tuvastamine ei muutu tänu näotuvastusele paremini kättesaadavamaks, võrreldes olemasoleva tuvastamisviisiga (vt jaotis 5.3.4.2).
3. Elektrooniline tuvastamine ei muutu tänu näotuvastusele täpsemaks ega kindlamaks, võrreldes olemasoleva tuvastamisviisiga (vt jaotised 4.1.1, 4.1.2, 5.3.4.2).
4. Näotuvastuse lisamine Eesti i-hääletamise protokolli muudab protokolli enda keerukamaks ja seega ka tõrkeohtlikumaks.
5. Näotuvastamine eeldab täiendava riistvara kasutuselevõttu, mis halvendab kasutajakogemust ning toob sisse täiendava tõrkekoha.
6. Kaamera kasutamine toob kaasa konfidentsiaalse info lekkimise riski. Näiteks võib kaamera vaatevälja jääda üleskirjutatud PIN-kood või kandidaadi number. Samuti saab kaamerapildist potentsiaalselt teha järeldusi inimese majandusliku või tervisliku seisukorra, religioossete tõekspidamiste ja muude delikaatsete andmete kohta. See risk suureneb veelgi, kui näotuvastuse käigus tehtud pilte või videosid salvestatakse pikemaks ajaks, nt hilisemate vaiete lahendamise eesmärgil.

5.3.5 Riivete seaduslik alus

Põhiseaduse kommenteeritud väljaandest loeme [26, Par 11, p 26]:

> *Küsimusele, millisel juhul peab põhivabaduse piirang olema sätestatud seadusega, millisel juhul võib seda teha määrusega, ei ole ühest ja selget vastust. Määravaks kriteeriumiks tuleb pidada piirangu olulisust – seda nii ühiskonna seisukohast üldiselt kui üksikisiku, kelle põhiõigusi piiratakse, seisukohast. Põhiõiguste piiramise otsustamisel õigustloova aktiga tuleb hinnata nii avalikku huvi (legitiimset eesmärki) kui üksikisiku kaalul olevaid õigusi ning kui isegi üks neist on oluline, tuleb sellekohane otsustus, kas piirangut lubada või mitte, teha demokraatia põhimõttest lähtudes seadusandjal.*

Näotuvastuse lisamisel nii andmebaasi kui ka dokumendi abil on tegemist intensiivse sekkumisega isiku era- ja perekonnaelu sfääri ning potentsiaalselt ka kodu puutumatusse, eriti juhul kui see toimub videovoo vahendusel. Arvestades, et õigusliku analüüsi eelnenud osades tuvastatud riivete proportsionaalsuse hinnangu kohaselt ei ole videovoo vahendusel näotuvastamine proportsionaalne põhiõiguste piirang, siis selle võimalikke õiguslikke aluseid me siinkohal eraldi ei

käsitle. Seetõttu keskendume alljärgnevalt eelkõige era- ja perekonnaelu ning kodu puutumatuse riivetele, mis puudutavad aruandes pakutud näotuvastusviise – näotuvastamine andmebaasi ja dokumendi abil.

Siinse aruande õigusliku analüüsi raames ei tuvastatud kehtivas õiguses sellise seadusest või alamalseisvast aktist tuleneva aluse olemasolu, mis otsesõnu lubaks näotuvastuse kasutuselevõttu elektroonilisel hääletamisel, olgu andmebaasi või dokumendi abil. Seega tuleb kaaluda, kas ja kuidas sellist seaduslikku alust kehtestada ning milliseid kriteeriume see peab täitma. Näiteks vajab lahendamist küsimus, kas näotuvastuse nõude võib kehtestada VVK oma otsusega või peab seda tegema seaduse tasandil või selle alusel kehtestatud määrusega. Põhiseaduse kommentaaride autorite hinnangul ei ole see küsimus üheselt lahendatav ning vajaks põhjalikku avalike ja erahuvide kaalumist. Selline kaalumisülesanne ei ole antud aruande käsitlusalas ning tuleks lahendada eraldiseisvalt.

Isikute privaatsust ja andmekaitset puudutavate riivete reguleerimisel peab arvestama Eestis otsekohalduva isikuandmete kaitse üldmäärusega GDPR. Näokujutise andmed on GDPR artikkel 9 lg 1 järgi eriliiki isikuandmed, mida on lubatud töödelda ainult GDPR artikkel 9 lg-s 2 loetletud juhtudel. Enamik GDPRi alusel loodud võimalustest eriliiki isikuandmete töötlemiseks käsitlevad andmesubjekti erahuve või muude isikute era- ja avalikke huve seoses töö- ja tervishoiu, sotsiaalkaitse, õigusmõistmise, teaduse, statistika ja arhiveerimisega, mis ei ole antud kontekstis asjakohased. Näokujutise kasutamiseks elektroonilistel valimistel isikusamasuse kontrollimiseks tulevad kõne alla üksnes kaks võimalust, mida käsitleme lähemalt allpool.

1. **Andmesubjekti nõusolek kui näotuvastuse õiguslik alus elektroonilisel hääletamisel [11, Art 9 lg 2 p (a)]**

   Andmesubjekti nõusolek on "*vabatahtlik, konkreetne, teadlik ja ühemõtteline tahteavaldus, millega andmesubjekt kas avalduse vormis või selge nõusolekut väljendava tegevusega nõustub tema kohta käivate isikuandmete töötlemisega.*" [11, Art 4 p 11] Niisiis, andmesubjekti nõusolekule kui õiguslikule alusele tuginemise esimene eeldus on, et see antakse vabatahtlikult.

   Elektroonilise hääletamise kontekstis tekib küsimus, kas andmesubjekt saab anda nõusoleku oma näokujutise kasutamiseks vabatahtlikult, sest elektrooniline hääletamine on oma olemuselt avalik teenus, mida riik pakub üksikisikutele avalik-õigusliku suhte raames. "*Nõusolekut ei tohiks lugeda vabatahtlikult antuks, kui andmesubjektil pole tõelist või vaba valikuvõimalust või ta ei saa kahjulike tagajärgedeta nõusoleku andmisest keelduda või seda tagasi võtta.*" [11, põhjenduspunkt 42] Näiteks ei ole vabatahtlikult antud nõusolekuga tegemist siis, kui andmesubjekt ja vastutav töötleja on selgelt ebavõrdses olukorras, eriti juhul, kui vastutav töötleja on avaliku sektori asutus. Sellisel juhul on ebatõenäoline, et nõusolek anti selle konkreetse olukorra kõigi asjaolude puhul vabatahtlikult [11, põhjenduspunkt 43].

   Näokujutise kasutamisel isikusamasuse kontrollimiseks elektroonilisel hääletamisel on valija ja riik ebavõrdses olukorras – ilma nõusolekut andmata ei saa valija elektroonilist häält anda. Kuigi valimiskorralduses on valijale tagatud mitmeid hääletamisviise, siis elektroonlise hääletamise alternatiivid võivad teatud olukordades (nt välisriigis) osutuda ebaproportsionaalselt kulukateks või tegelikult võimatuteks. Sellises olukorras puudub valijal sisuline valikuvõimalus, kas lubada end näokujutise alusel tuvastada või mitte. Järelikult ei sobi andmesubjekti nõusolek antud juhul õiguslikuks aluseks.

2. **Olulise avaliku huviga seotud põhjus kui näotuvastuse õiguslik alus elektroonilisel hääletamisel [11, Art 9 lg 2 p (g)]**

Analüüsi lähteülesandes on analüüsitava muudatuse eesmärk väga üldiselt defineeritud. On mõistetav, et tellija sooviks on tagada elektroonilise hääletamise turvalisus ja üldine usaldusväärsus ajas, sh arvestades uusi tehnoloogilisi võimalusi ja sellega kaasnevaid riske. Samas ei ole tehnoloogia areng iseenesest piisav argument, et selle kasutuselevõtuga riivata isikute põhiõigusi. Seega tuleks näokujutise töötlemise eesmärk täpsemalt määratleda, et oleks võimalik hinnata, kas see on seotud olulise avaliku huviga.

Aruande koostajad on teinud ettepaneku määratleda näokujutise eesmärgiks valija ühene tuvastamine, et vähendada elektroonilise hääle andmist valija eest ilma tema teadmise ja nõusolekuta. Tulenevalt valimiste olulisusest demokraatlikus ühiskonnas ning eriti elektroonilise hääletamise tähtsusest Eestis kui maailmas tunnustatud digiriigis võib eeldada, et see eesmärk on seotud olulise avaliku huviga. Järelikult on mõeldav, et näokujutise andmeid võiks töödelda näotuvastuse kasutuselevõtuks elektroonilisel hääletamisel GDPR artikkel 9 lg 2 p (g) tingimustele vastava Eesti siseriikliku õigusnormi alusel. Järgmiseks tuleks lahendada küsimus, millises õigusaktis see õigusnorm võiks paikneda, isegi kui seda hetkel ei eksisteeri. See küsimus väljub siinse aruande käsitlusalast.

Kehtiv ITDS võimaldab iga avalik-õigusliku teenuse puhul valida, kas selle osutamiseks on nõutav eelnev tuvastamine isikutunnistusele, elamisloakaardile või digitaalsele isikutunnistusele kantud digitaalset tuvastamist võimaldava sertifikaadi abil. Seejuures pole ette nähtud, kas see valik tuleb teha seaduse tasandil või sellest alamalseisva aktiga, sh millistel institutsioonidel on vastav diskretsiooniõigus. Põhimõtteliselt ei ole ITDSi alusel välistatud ka isikut tõendavale dokumendile salvestatud biomeetria kasutamine isikusamasuse kontrollimiseks. Seda on tulevikus võimalik teha elektroonilisel hääletamisel üksnes ID-kaardile kantud biomeetriliste andmete ja valija näokujutise võrdlemise teel. Vastav õigusmuudatus ootab ees tulenevalt 02.08.2021 kehtima hakkavast uuest määrusest nr 2019/1157 [12], mille alusel ka Eestis elektroonilisel hääletamisel kasutatavatele ID-kaartidele on plaanis lisada näokujutis ja kaks sõrmejälge.

Igal juhul tuleks kavandatavat olulise avaliku huviga seotud põhjust näotuvastuse lisamiseks elektroonilisele hääletamisele ühiskonnas põhjalikult arutada ja hinnata, kas näotuvastus on proportsionaalne saavutatava eesmärgiga, austab isikuandmete kaitse õiguse olemust ning tagab sobivad ja konkreetsed meetmed andmesubjekti põhiõiguste ja huvide kaitseks [11, Art 9 lg 2 p (g)].[11] Need küsimused väljuvad siinse analüüsi raamidest.

Eesti kehtivas õiguses ei ole selget seaduslikku alust biomeetriliste andmete, sh näokujutise kasutamiseks isikusamasuse kontrollimiseks elektroonilisel hääletamisel. Näotuvastuse kasutuselevõtul elektroonilisel hääletamisel tuleb tuvastamisviisi valiku tegemisega seonduvat täpsemalt reguleerida.

[11] Juhime tähelepanu, et Euroopa Andmekaitseinspektor on kutsunud üles kehtestama moratooriumi seoses biomeetria ja muude inimlike tunnuste automaatse tuvastamisega avalikus ruumis, et võimaldada selleteemalist informeeritud ja demokraatlikku arutelu [40, 29].

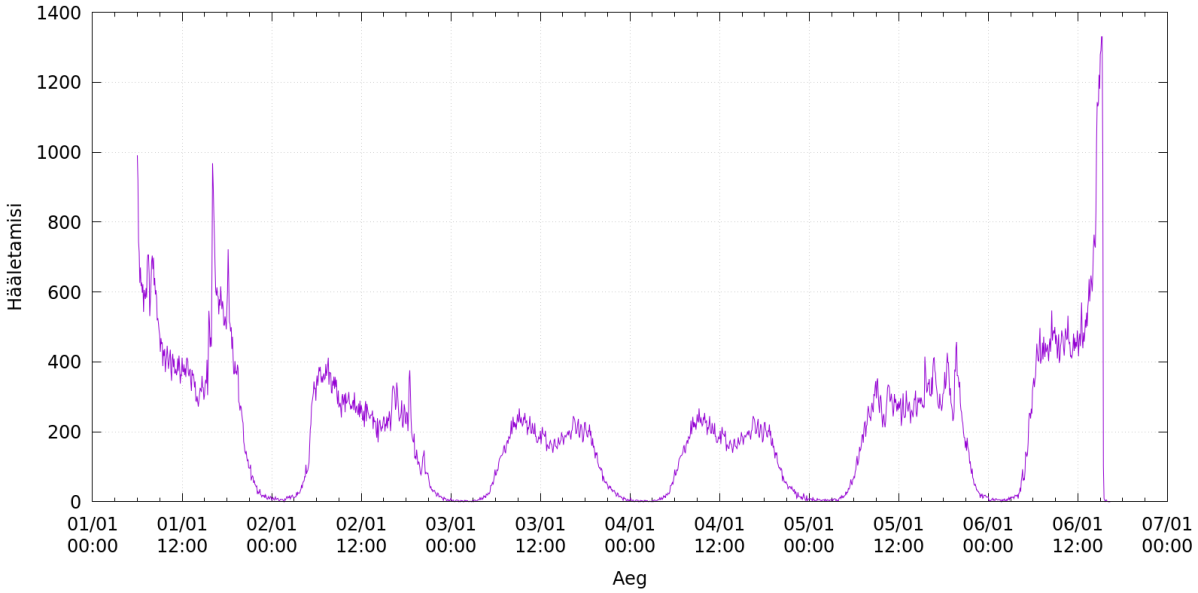
6 Arendustööde mahu hindamine

Arendusmahtude hindamiseks dokumenteerime kõigepealt eeldused näotuvastuse rakendamisele, seejärel fikseerime jõudlusnõuded, kaardistame vajalikud muudatused elektroonilise hääletamise süsteemis (EHS) ja seda ümbritsevas keskkonnas, defineerime kaks lähenemisviisi näotuvastusvõimekuse saavutamiseks ning anname lõpuks esialgse hinnangu arendusmahtudele ja -kulule.

6.1 Eeldused

Hinnanguid andes lähtume järgmistest eeldustest.

- Näotuvastamisel kasutatakse mobiilseadet. Senist i-hääletamise praktikat silmas pidades tuleb toetada nii Android kui iOS platvorme.
- Hääletamine toimub PC-ga, kuid PC osas puudub vajadus liidestuda veebikaameratega.
- Näotuvastamine on osa autentimisprotessist, mille tulemusel selgub valija isikukood.
- Arvestame 6-päevase i-hääletamisperioodiga. Senised i-hääletamised on olnud 7-päevased, kuid aastast 2021 on i-hääletamisperiood lühem. Perioodi lühenemine mõjutab süsteemi jõudlust, sest sama hulk hääletajaid tuleb teenindada lühema aja jooksul.
- Arvestame 320000 hääletamisseansiga (korduvhääletamisi on ligi 3%, mistõttu need 320000 seanssi esindavad hinnanguliselt 310000 valijat). Seansside arvu valime lähtudes senisest suurimast i-häälte hulgast (RK2019, 253572 häält, unikaalseid valijaid 247232). Valime koormuse nii, et senine teadaolev maksimumkoormus rakendaks 80% uue süsteemi võimekusest.
- Kasutades varasematest i-hääletamistest teadaolevat hääletamismustrit [32], modelleerime 6-päevase i-hääletamise koormusjaotust soovitud seansside arvu korral (joonis 3). Tulemusena näeme, et kõige suurema koormusega 10-minutilise perioodi vältel esitatakse eeldatavasti ca 1350 häält, sealhulgas tippkoormusega minuti jooksul 295 häält.
- Arvestame, et masinliides talletab kuni 8 sekundit videot hääletamisseansi kohta. Kokku tekib umbes 30 päeva ulatuses videomaterjali, mis talletamise mõttes probleemi ei kujuta. Lähtume intervjuu käigus viidatud keskmisest automaatseansi kestusest 6 sekundit, millesse suhtume konservatiivselt.
- Arvestame inimverifitseerimise ajakuluks 25 sekundit. Lähtume intervjuu käigus viidatud keskmisest automaatseansi kestusest 20 sekundit, millesse suhtume konservatiivselt.
- Arvestame inimliidesesse suunatavate seansside arvuks 5% igal ajahetkel. Lähtume intervjuu käigus kinnitatud automaattuvastuse valenegatiivsete hulgast 3% ning suhtume sellesse konservatiivselt.



Joonis 3. I-hääletamise modelleeritud koormusjaotus 10 minuti kaupa 320000 seansi ja 6-päevase hääletamisperioodi korral

- Arvestame automaattuvastuse ja inimtuvastuse koosmõjus toimiva lahenduse korral valenegatiivseteks 0,2% kõigist vastustest. Lähtume intervjuu käigus viidatud väärtusest 0,16%, millesse suhtume konservatiivselt.

6.2 Jõudlusnõuded

Eelnevalt kirjeldatud parameetrid aitavad meil hinnata nõudeid tuvastusteenuse jõudlusele. Süsteemi aktiivsushetked on hästi prognoositavad ning hääletamise esimese tunni aktiivsuse pealt saab teha paikapidavaid järeldusi kogu hääletamisperioodi aktiivsuse kohta. Need järeldused omakorda võimaldavad paindliku ressurssi olemasolul süsteemi skaleerida.

Automaattuvastuse mõttes tähendab see, et ressurssivajaduse dünaamilisele muutumisele vastamiseks on vajalik kas süsteemi üledimensioneerimine või horisontaalne skaleeritavus.

Lisaks automaattuvastusele tuleb hinnata nõudeid inimtuvastuse jõudlusele. Tippkoormuse ajal tuleb teha ca 15 inimkontrolli minutis (5% tippkoormuse seanssidest). See tähendab, et inimressurssi 80% hõivatusega on tipphetkedel (hääletamise esimene päev, hääletamise viimased tunnid) vaja 8 inimoperaatorit. Hindame, et tavalisel hääletamispäeval katab inimvajaduse 8 tunni ulatuses 1 operaator ja 16 tunni ulatuses 2 operaatorit. Eeldame, et ühe kontrolli raames teeb otsuse üks inimene. Vajadus olla valmis ootamatult suuremaks valimisaktiivsuseks sunnib lahendust üledimensioneerima, suurendades tippkoormuse aegset teenindusvõimsust 9 paralleelse operaatorini, mis võimaldaks toetada tippkoormust 21 inimkontrolli, ehk 420 häält minutis.

6.3 Arendusvajadus osapooliti

Lähtudes ülaltoodud eeldustest ning jõudlusnõuetest on võimalik kirjeldada arendusvajadus osapooliti.

Valija. Valijalt nõuab kohustuslik näotuvastus täiendavalt ligipääsu nutiseadmele, piisavalt kvaliteetset võrguühendust 8-sekundilise video edastamiseks ning näotuvastuseks sobivate valgus-

tingimuste ja taustaga keskkonda.

EHS. Elektroonilise hääletamise infosüsteemi vaatest saame näotuvastustust käsitleda eraldi autentimismeetodina, mille liidestamine toimub sarnaselt Mobiil-ID või Smart-ID teenuse liidestamisega. Kõik intervjueeritud kommertsiaalsed teenusepakkujad pakuvad *back-end* APIt ning lõppkasutaja rakendusi. EHSi arendusvajadus seisneb *back-end*i liidestamises, sisemise suhtlusprotokolli spetsifitseerimises ning valijarakenduse täiendustes näotuvastuse ja hääletamise seostamiseks. Need arendused on pigem väikesemahulised – orienteeruvalt 9 inimkuud tarkvaraarendust, dokumenteerimist ja testimist 6 kalendrikuu vältel. Arvestades tarkvaraarendustööde hindu 2021. aastal on sellise projekti ligikaudseks maksumuseks 72000 eurot.

Valimiste korraldaja vaatenurgast tähendab kohustuslik näotuvastus olulist muudatust elektroonilise hääletamise protokollis. Sellelaadseid muudatusi on varasema praktika kohaselt rakendatud järk-järgult (nt individuaalne kontrollitavus 2013.–2015. aastal) ning neile on eelnenud avalikud piloothääletamised.

Valimiste korraldajat mõjutab ka näotuvastusteenuse olemuslik omadus anda valenegatiivsed tulemusi. Lähtudes eelpooltoodud parameetritest (0,2% valenegatiivseid kõigist seanssidest) võime öelda, et ligikaudu 620–640 hääletajat ei saa valimisel elektrooniliselt oma häält anda, kuna näotuvastamine nende jaoks ei toimi.

Kõige mahukam on küsimus **näotuvastusteenuse osutajast** endast. Siinkohal peame silmas teenust, mida iseloomustavad järgmised omadused.

1. Eksisteerib usaldusväärne referentsandmebaas kvaliteetset näotuvastamist võimaldavate andmetega kõigi hääleõiguslike isikute kohta
2. On realiseeritud sobiva veaprotsendiga automaattuvastusmeetod.
3. On realiseeritud piisavat jõudlust pakkuv automaattuvastusteenus, mida katab hääletamisperioodi vältel valimiste jaoks sobiv teenuse taseme leping.
4. Eksiseerib inimoperaatoritest koosnev tagavaraliides – inimesed, töökeskkond, protseduurid ja töö teostamiseks vajalik tarkvara.
5. On olemas funktsionaalsus seansside salvestamiseks järelauditi tarbeks – inimesed, töökeskkond, protseduurid ja tarkvara auditite teostamiseks.
6. Eksisteerib *back-end* API EHSi (ja teiste analoogsete teenuste) integreerimiseks.
7. Eksisteerib lõppkasutaja rakendus Android platvormil.
8. Eksisteerib lõppkasutaja rakendus iOS platvormil.

6.4 Näotuvastusvõimekuse saavutamine

Vajalike omadustega näotuvastusvõimekuse saavutamiseks on kaks võimalikku teed – EHSi integreerimine mõne olemasoleva näotuvastusteenusega või riikliku näotuvastusteenuse loomine.

6.4.1 Välise näotuvastusteenuse kasutamine

Kõik kommertsiaalsed teenuseosutajad katsid eelpool identifitseeritud nõuded mingis ulatuses. Lahknevused tekkisid ennekõike inimliidese juures ning järelauditi võimekuses. Kõiki teenuseosutajaid ühendas referentsandmebaasi puudumine ning verifitseerimine lähtudes dokumendifotost. Kirjeldatud lahendused toimisid teenusmudelis; kliendipoolne majutamine ja opereerimine ei ole osa intervjueeritud teenuseosutajate tavapärasest ärimudelist.

Intervjuudes puudutasime ka näotuvastusteenuse hinnastamist ning küsisime, kuidas saab valimise korraldaja prognoosida valimissündmusega seotud tuvastusteenuse kulu. Kaks kommertsiaalset teenusepakkujat hinnastavad teenust päringupõhiselt, üks tellimuspõhiselt. Mittekommertsiaalne teenusepakkuja vastas: “Küsimus vajab pikemat, haldusalade vahelist arutelu ja kokkulepet.” Vastus võtab hästi kokku ka kommertsiaalsete teenusepakkujate lähenemise. Väljaspool ametlikku hankeprotsessi, kus nõuded oleksid siduvad ja detailsed, ei ole täpsete rahanumbrite andmine võimalik.

Ainult üks kommertsiaalsetest pakkujatest avalikustab hindu veebis ning ühe verifitseerimise hind jääb vahemikku 1,25–1,73 eurot. Võime öelda, et selle teenuse kasutamisel eelmainitud hindadega jääks i-hääletamise näotuvastuskulu vahemikku 400000–554000 eurot valimise kohta. Viitame, et 2017. aasta KOV valimisel hinnati ühe e-hääle maksumuseks 2,32 eurot [35]. Näotuvastusteenuse kasutamine tõstaks i-hääle hinda, kuid iiski oleks jätkuvalt tegu soodsaima hääletamisviisiga – valimispäeval jaoskonnas antud hääle maksumus 2017. aastal oli 4,37 eurot [35].

6.4.2 Riikliku näotuvastusteenuse loomine

Alternatiivina olemasoleva teenuse kasutamisele võib riik kaaluda ise nõuetele vastava teenuse loomist. Selles suunas on liikumas projekt ABIS, mille eeliseks on usaldusväärse referentsandmebaasi olemasolu, kuid vähemalt hetkel ei ole jõudlusnäitajad i-hääletamise jaoks piisavad. Puudub ka inimliides tagavaraväljapääsuna valenegatiivsete tuvastustega tegelemiseks.

Kuna üks kommertsiaalsetest teenuseosutajatest on registreeritud Eestis, on võimalik tutvuda tema majandusaasta aruannetega, kust nähtub, et ettevõtte esimese kolme-nelja aasta kulud on suurusjärgus 2500000 eurot, mis annab samuti hinnangu vajalike omadustega näotuvastusteenuse loomise ajakulule ja maksumusele.

6.5 Arendusmahud

Sobivate omadustega kommertsiaalsetel alustel pakutava teenusega integreerumine (vt. tabel 3) võib olla otstarbekas nii alginvesteeringu suurust kui tootessejõudmise graafikut silmas pidades. Siiski tuleb arvestada EHSi arendustöödega integreerumiseks ning referentsandmebaasi loomisega teenuseosutaja poolel.

Tabel 3. Välise näotuvastusteenuse kasutamine

Tegevus	**Kestvus**	**Maht**	**Kulu**
Alginvesteering			
EHSi integreerimine	6 kuud	9 inimkuud	72000 eurot
Referentsandmebaasi loomine	N/A	N/A	N/A
Püsikulu			
Näotuvastusteenus valimisele	1 valimine	320000 päringut	400000 – 554000 eurot

Riikliku näotuvastusteenuse kasuks kõneleb asjaolu, et alates 2018. aastast kuni tänaseni on projekti ABIS näol tehtud märkimisväärses suurusjärgus investeeringuid ning 2021. aasta riigieelarve planeerib ajavahemikus 2020–2024 rahastada tegevusi 9450000 euro ulatuses. Projekti üheks sõnastatud eesmärgiks on aidata kasutada mugavalt nii riigi- kui erasektori teenuseid.

Valimiste vaatevinklist võib riikliku teenuse tekkimine vähendada püsikulu, samas tuleb eraldi hinnata lahknevust projektis planeeritu ning valimiste vajaduste vahel. Küsimus on nii võimalikus vajalikus lisafinantseeringus kui ka teenuse eeldatavas turule jõudmise ajas.

A Näotuvastusteenusepakkuja küsimustik

A.1 Eestikeelne küsimustik

1. Milliseid arhitektuurseid lahendusi näotuvastusteenuse liidestamiseks infosüsteemiga toetate?
    - Milline on näotuvastusteenuse ja infosüsteemi vaheline suhtlusprotokoll?
    - Millist eelinfot vajab näotuvastusteenus kasutajate ja infosüsteemi kohta?
    - Milline on näotuvastusteenuse poolt infosüsteemile antava vastuse koosseis? Kas see vastus on signeeritud?
    - Mis kujul tuleb süsteemile ette anda isikute-nägude andmekogu? Kuidas toimub selle andmekogu uuendamine (näiteks juhul kui valijate nimekiri valimiste käigus muutub)?
2. Kas kasutate automaattuvastamist, inimtuvastamist või mõlemat?
    - Kui mõlemat, siis kuidas otsustatakse, kumba rakendada?
    - Kuidas toimub ühelt tuvastusviisilt teisele lülitumine?
3. Kuidas toimub näotuvastus kasutajavaates?
    - Millised on nõuded kasutatavale riistvarale?
    - Millised on nõuded kasutatavale tarkvarale?
4. Milline on näotuvastuse töökindlus?
    - Kuidas tagatakse see, et näotuvastuseks ei saa kasutada salvestust?
    - Milline on süsteemi tuvastustvigade protsent (nii valepositiivsed kui valenegatiivsed)?
    - Millest tuvastusvigade protsent sõltub?
    - Kui palju erinevad tingimused (kaamerapildi kvaliteet, valgus, inimese vananemine jne) tuvastustäpsust mõjutavad?
    - Millised on nõuded kasutatavale kaamerale?
    - Kuidas on lahendatud kaksikute tuvastamine?
5. Kuidas võiks teie näotuvastusteenuse abil realiseerida kasutusjuhtumit, kus kasutaja on infosüsteemi poolt juba mõne autentimisvahendi abil (nt. eID) tuvastatud ning vaja on kontrollida, kas kasutaja on sama isik kui autentimisvahendi omanik?
    - Kuidas oleks seda kasutusjuhtumit võimalik realiseerida selliselt, et kasutaja ei peaks oma dokumente kaamerasse näitama (sest ID-kaart võib sel ajal lugejas olla)?
6. Milliseid muid aspekte lisaks isikusamasusele on võimalik tuvastada (nt et inimene on ruumis üksi või et ta avaldab hääletades oma vaba tahet)?
7. Milline on näotuvastusteenus jõudlus?

- Kui palju tuvastuspäringuid ajaühikus jõuate teenindada?
- Kui palju kulub aega ühe näotuvastuse peale?
- Mitu paralleelset tuvastusseanssi jõuate teenindada?

8. Kuidas on paika pandud näotuvastusteenuse pakkuja vastutus? Valimiste puhul tähendavad nii valepositiivsed- kui negatiivsed tuvastused otsest vastuolu põhiseaduslike nõuetega. Kas sel juhul on võimalik esitada nõudeid tuvastusteenuse pakkuja vastu?
9. Kas näotuvastusseanssidest säilitatakse hilisemate vaiete lahendamise jaoks ka salvestusi? Kui jah, siis kuidas need salvestused valedesse kätesse sattumise vastu kaitstud on?
10. Kuidas on tagatud kaamerast paistva pildi privaatsus?
    - Missugust infot salvestatakse ja kui kaua seda säilitatakse?
    - Kas vastavat infot on võimalik GDPRi alusel välja nõuda?
    - Kas GDPRi alusel on võimalik nõuda salvestatud info kustutamist?
11. Kas näotuvastus saab olla interaktiivne ja inimese poolt juhitav?
12. Kas tuvastatav isik näeb, kes teda tuvastab? Kuidas on tagatud see, et nägu tuvastav isik ei teeks endale eraldi salvestust (näiteks salvestades nutitelefoniga ekraani)? Missugust infot omab nägu tuvastav isik tuvastatava kohta?
13. Kuidas toimub näotuvastusteenuse hinnastamine? Kuidas saaks valimise korraldaja prognoosida valimissündmusega seotud tuvastusteenuse kulu?
14. Millistes sektorites ning milliste kasutusjuhtumite jaoks teie teenust rakendatakse? Euroopa Liidus? Maailmas?
15. Millised näotuvastusteenuse kvaliteedile relevantsed sertifikaadid on teie ettevõttel / tootel?
16. Mida tõstaksite enda näotuvastusteenuse juures esile, mis eristab teid konkurentidest?

A.2 English questionnaire

1. Which architectural solutions do you support for interfacing facial recognition service and the main information system?
    - What is the protocol between the facial recognition service and the information system?
    - What prior information does the facial recognition service need about the persons and the information system?
    - What is the content and format of the reply given by the facial recognition service to the information system? Is the reply signed?
    - In what format does the service expect the dataset of persons and faces? How is this dataset updated (e.g. when the list of eligible voters changes during the elections)?
2. Do you use automatic recognition, human recognition, or both?
    - If you use both, then how is it decided which one to use at a particular case?
    - How does the switch from one mode to the other happen?
3. How does the recognition work in the user's view?
    - What are the requirements to the hardware?
    - What are the requirements to the software?
4. How high is the reliability of facial recognition?
    - How do you ensure that the client side does not use a recording for recognition?
    - What is the error rate (both false positives and false negatives) of your system?
    - What does this error rate depend on?
    - How is the error rate influenced by different conditions (camera quality, lighting, ageing, etc.)?
    - What are the requirements on the camera?
    - How do you distinguish between twins?
5. Can you support the workflow where the user has already been identified (say, using an eID mechanism), and the system needs to check whether the identified digital person matches the physical one?
    - Can such a use case be implemented so that the user would not need to show his/her ID into the camera (as the ID card can be in the reader at the same time)?
6. What are other aspects that you can detect using your system (say, is the person alone in the room, or whether he/she expresses his/her free will while voting)?
7. What is the performance of your system?
    - How many recognitions per time unit can you handle?
    - How much time do you need per one recognition?
    - How many parallel recognition sessions can you handle?
8. What is the responsibility of the facial recognition service provider? Note that in case of elections, both false positive and false negative recognitions mean direct conflict with constitutional requirements. In this case, is it possible to sue the facial recognition service provider?

9. In order to resolve possible disputes, are the recognition sessions recorded? If yes then how are the recordings protected from ending up in the wrong hands?
10. How is privacy of the images/stream coming from the camera protected?
    - What information is stored and for how long?
    - Is it possible to request this information based on GDPR?
    - Is it possible to demand deleting this information based on GDPR?
11. Can the recognition process be interactive and humanly controlled?
12. In case recognition is performed by a human operator, can the subject see who is recognising him/her? How is it ensured that the operator does not record the sessions on one's own (say, capturing the screen using his/her own smart phone)? What information does the operator have about the subject?
13. What is the pricing model of the facial recognition service? How can the Election Management Body predict the costs of recognition required for elections?
14. What are the main use cases your service is currently being used in Europe and in the World?
15. Has your service/company/product and its quality been certified?
16. What are the main points of difference between you and your competitors?

Kirjandus

[1] Article 29 Data Protection Working Party. Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is “likely to result in a high risk” for the purposes of Regulation 2016/679. Adopted on 4 April 2017. As last Revised and Adopted on 4 October 2017. 17/EN WP 248 rev.01. https://edpb.europa.eu/our-work-tools/our-documents/guidelines/data-protection-impact-assessments-high-risk-processing_en.

[2] Automaatse biomeetrilise isikutuvastuse süsteemi andmekogu ehk ABIS. https://www.siseministeerium.ee/et/eesmark-tegevused/automaatse-biomeetrilise-isikutuvastuse-susteemi-andmekogu-ehk-abis.

[3] Code of Good Practice of the European Commission for Democracy Through Law (Venice Commission). https://rm.coe.int/090000168092af01.

[4] Coop Pank võttis kasutusele uue isikutuvastuse süsteemi. https://www.cooppank.ee/coop-pank-vottis-kasutusele-uue-isikutuvastuse-susteemi.

[5] E-identimise ja e-tehingute usaldusteenuste seadus. https://www.riigiteataja.ee/akt/125102016001?leiaKehtiv.

[6] E-valimiste turvalisuse töörühma koondaruanne. 12.12.2019, https://www.mkm.ee/sites/default/files/e-valimiste_tooruhma_koondaruanne_12.12.2019.pdf.

[7] E-valimistel on pettuse kahtlus. Sakala, 12.10.2005, https://dea.digar.ee/cgi-bin/dea?a=d&d=sakala20051012.1.8.

[8] Eesti esimesed automatiseeritud piirikontrolli väravad said töökorda. Tallinna lennujaam. https://www.tallinn-airport.ee/uudised/eesti-esimesed-automatiseeritud-piirikontrolli-varavad-said-tookorda/.

[9] Eesti Vabariigi põhiseadus. https://www.riigiteataja.ee/akt/115052015002?leiaKehtiv.

[10] Euroopa Kohtu (suurkoda) 16. juuli 2020. aasta otsus (High Courti eelotsusetaotlus – Iirimaa). Data Protection Commissioner versus Facebook Ireland Limited, Maximillian Schrems. Kohtuasi C-311/18, ELT C 297, 7.9.2020, p. 4–5. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CA0311&qid=1622017812864.

[11] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[12] Euroopa Parlamendi ja Nõukogu määrus (EL) 2019/1157, 20. juuni 2019, liidu kodanike isikutunnistuste ning vaba liikumise õigust kasutavatele liidu kodanikele ja nende pereliikmetele väljaantavate elamislubade turvalisuse suurendamise kohta. PE/70/2019/REV/1, ELT L 188, 12.7.2019,. https://eur-lex.europa.eu/eli/reg/2019/1157/oj.

[13] Euroopa Parlamendi ja Nõukogu määrus (EL) nr 910/2014, 23. juuli 2014, e-identimise ja e-tehingute jaoks vajalike usaldusteenuste kohta siseturul ja millega tunnistatakse kehtetuks direktiiv 1999/93/EÜ. OJ L 257, 28.8.2014, p. 73–114. http://data.europa.eu/eli/reg/2014/910/oj.

[14] Isikut tõendavate dokumentide seadus. https://www.riigiteataja.ee/akt/131012020015?leiaKehtiv.

[15] Karistusseadustik. https://www.riigiteataja.ee/akt/103032021003?leiaKehtiv.

[16] Kohtuotsus kriminaalasjas number 1-10-17400. https://www.riigiteataja.ee/kohtulahendid/fail.html?id=40465800.

[17] Notarite Koda. Kaugtõestamine. Näotuvastus. https://www.notar.ee/et/teabekeskus/kaugtoestus.

[18] Riigikogu valimise seadus. https://www.riigiteataja.ee/akt/103012020013?leiaKehtiv.

[19] Riigikohtu põhiseaduslikkuse järelevalve kohtuotsus asjas nr 3-4-1-13-05, 01.09.2005, p 24. https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-13-05.

[20] Riigikohtu üldkogu kohtuotsus asjas nr 3-4-1-33-09, 1.07.2010, p 30. https://www.riigikohus.ee/et/lahendid?asjaNr=3-4-1-33-09.

[21] Sõrmejälg ja näotuvastus: biomeetrilised tuvastusvõtted jõudsid netipanka. Ärileht 12.11.2020. https://arileht.delfi.ee/artikkel/91647055/sormejalg-ja-naotuvastus-biomeetrilised-tuvastusvotted-joudsid-netipanka.

[22] The European Data Protection Board. Endorsement 1/2018. https://edpb.europa.eu/sites/default/files/files/news/endorsement_of_wp29_documents_en_0.pdf.

[23] Toomas Pauri kaebuse läbivaatamine. Vabariigi Valimiskomisjoni otsus 11.03.2015, https://www.riigiteataja.ee/akt/313032015014.

[24] Vihje: Hummuli vallas pandi hooldekodu kliendid vallavanema poolt hääletama. Vallavanem: esimest korda kuulen. Lõunaeestlane, 23.10.2017, https://lounaeestlane.ee/vihje-hummuli-vallas-pandi-hooldekodu-kliendid-vallavanema-poolt-haaletama-vallavanem-esimest-korda-kuulen/.

[25] 14 misunderstandings with regard to biometric identification and authentication, June 2020. https://edps.europa.eu/data-protection/our-work/publications/papers/14-misunderstandings-regard-biometric-identification_en.

[26] Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne, 2020. https://pohiseadus.ee/.

[27] Shadnaz Asgari, Jelena Trajkovic, Mehran Rahmani, Wenlu Zhang, Roger C. Lo, and Antonella Sciortino. An observational study of engineering online education during the COVID-19 pandemic. *PLOS ONE*, 16(4):1–17, 04 2021.

[28] Ahto Buldas, Sven Heiberg, Kristjan Krips, and Jan Willemson. Mobile voting feasibility study and risk analysis, 2020. Cybernetica report T-184-5, https://www.valimised.ee/sites/default/files/uploads/eng/2020_m-voting-report.pdf.

[29] European Data Protection Supervisor. The EDPS Strategy 2020-2024. Shaping a Safer Digital Future, 2020. https://edps.europa.eu/sites/default/files/publication/20-06-30_edps_shaping_safer_digital_future_en.pdf.

[30] Sven Heiberg, Kristjan Krips, and Jan Willemson. Planning the next steps for Estonian Internet voting. pages 82–97, 2020. Fifth International Joint Conference on Electronic Voting E-Vote-ID 2020: 6-9 October 2020: Proceedings, TalTech Press.

[31] Sven Heiberg, Tarvi Martens, Priit Vinkel, and Jan Willemson. Improving the Verifiability of the Estonian Internet Voting Scheme. In Robert Krimmer, Melanie Volkamer, Jordi Barrat, Josh Benaloh, Nicole J. Goodman, Peter Y. A. Ryan, and Vanessa Teague, editors, *Electronic Voting - First International Joint Conference, E-Vote-ID 2016, Bregenz, Austria, October 18-21, 2016, Proceedings*, volume 10141 of *Lecture Notes in Computer Science*, pages 92–107. Springer, 2016.

[32] Sven Heiberg, Arnis Parsovs, and Jan Willemson. Log Analysis of Estonian Internet Voting 2013-2014. In Rolf Haenni, Reto E. Koenig, and Douglas Wikström, editors, *E-Voting and Identity - 5th International Conference, VoteID 2015, Bern, Switzerland, September 2-4, 2015, Proceedings*, volume 9269 of *Lecture Notes in Computer Science*, pages 19–34. Springer, 2015.

[33] Sven Heiberg and Jan Willemson. Verifiable internet voting in Estonia. In Robert Krimmer and Melanie Volkamer, editors, *6th International Conference on Electronic Voting: Verifying the Vote, EVOTE 2014, Lochau / Bregenz, Austria, October 29-31, 2014*, pages 1–8. IEEE, 2014.

[34] Kert Kingo. Miks ERKE e-valimiste pärast nii palju muretseb? Kert Kingo: sest need tekitavad usaldamatust. Uued Uudised, 21.07.2020, https://uueduudised.ee/uudis/eesti/miks-erke-e-valimiste-parast-nii-palju-muretseb-kert-kingo-sest-need-tekitavad-usaldamatust/.

[35] Robert Krimmer, David Duenas-Cid, Iuliia Krivonosova, Priit Vinkel, and Arne Koitmae. How Much Does an e-Vote Cost? Cost Comparison per Vote in Multichannel Elections in Estonia. In Robert Krimmer, Melanie Volkamer, Véronique Cortier, Rajeev Goré, Manik Hapsara, Uwe Serdült, and David Duenas-Cid, editors, *Electronic Voting - Third International Joint Conference, E-Vote-ID 2018, Bregenz, Austria, October 2-5, 2018, Proceedings*, volume 11143 of *Lecture Notes in Computer Science*, pages 117–131. Springer, 2018.

[36] Kristjan Krips and Jan Willemson. On Practical Aspects of Coercion-Resistant Remote Voting Systems. In Robert Krimmer, Melanie Volkamer, Véronique Cortier, Bernhard Beckert, Ralf Küsters, Uwe Serdült, and David Duenas-Cid, editors, *Electronic Voting - 4th International Joint Conference, E-Vote-ID 2019, Bregenz, Austria, October 1-4, 2019, Proceedings*, volume 11759 of *Lecture Notes in Computer Science*, pages 216–232. Springer, 2019.

[37] Ülle Madise and Priit Vinkel. Internet Voting in Estonia: From Constitutional Debate to Evaluation of Experience over Six Elections. In Tanel Kerikmäe, editor, *Regulating eTechnologies in the European Union: Normative Realities and Trends*, pages 53–72. Springer International Publishing, 2014.

[38] Claire Poirson. The Legal Regulation of Facial Recognition. In Katharina Miller and Karen Wendt, editors, *The Fourth Industrial Revolution and Its Impact on Ethics: Solving the Challenges of the Agenda 2030*, pages 283–302. Springer International Publishing, 2021.

[39] Riigi Valimisteenistus. Elektroonilise hääletamise üldraamistik ja selle kasutamine Eesti riiklikel valimistel, 2017. IVXV-ÜK-1.0, https://www.valimised.ee/sites/default/files/uploads/eh/IVXV_raamistiku_yldkirjeldus_29052017.pdf.

[40] Wojciech Wiewiórowski. The State of Biometrics. Update from the European Data Protection Supervisor, 2020. https://edps.europa.eu/sites/edp/files/publication/20-10-07_edps_biometrics_speech_en.pdf.

[41] Ülle Madise. Interneti teel hääletamise õiguslikke ja poliitilisi aspekte. *Juridica*, (10):663–672, 2006.