

JAANIKA PUUSALU

ETTEMAKSTUD KÕNEKAARTIDE ISIKUSTAMINE:

ÜLEVAADE MAAILMATRENDIDEST NING
NÕUDE RAKENDAMISEGA KAASNEVATEST
OOTUSTEST JA OHTUDEST



ETTEMAKSTUD KÕNEKAARTIDE ISIKUSTAMINE:

**ÜLEVAADE MAAILMATRENDIDEST NING
NÕUDE RAKENDAMISEGA KAASNEVATEST
OOTUSTEST JA OHTUDEST**

JAANIKA PUUSALU



SISEKAITSEAKADEEMIA
ESTONIAN ACADEMY OF SECURITY SCIENCES

Autoriõigus: Sisekaitseakadeemia 2021

Esikaane foto: Shutterstock

Makett ja küljendus: Jan Garshnek

Keeletoimetaja: Siiri Soidro

ISBN 978-9985-67-340-9 (pdf)

www.sisekaitse.ee/kirjastus



SISUKORD

SISSEJUHATUS	5
1. SIM-KAARTIDE ISIKUSTAMISE NÕUE MAAILMAS	9
1.1. Kõnekaardi isikustamist nõudvad riigid	10
1.2. Isikustamist mitte nõudvad riigid	14
1.3. Isikustamise reeglid külastavatele välismaalastele	15
1.4. Isikustamisega kaasnevad probleemid	16
2. SIM-KAARTIDE ISIKUSTAMISE EESMÄRK: VÕIMALUSED JA TEGELIKKUS	20
2.1. Erinevad sideteenused	20
2.2. SIM-kaartide isikustamine ja uued kuriteoliigid	22
3. SIM-KAARTIDE ISIKUSTAMINE EESTIS	24
KOKKUVÕTE	26
KASUTATUD ALLIKAD	28

SISSEJUHATUS

Eestis kavandas 2020. aasta kevadsuvel Majandus- ja Kommunikatsiooniministeerium elektroonilise side seaduse muutmise eelnõu, mille eesmärk oli teha ettemakstud mobiilteenuste lõppkasutaja isiku tuvastamine sideteenuse pakkuja jaoks enne teenuse pakku- mist kohustuslikuks (Roosve, 2020a). Eelnõu vastuvõtmisel oleks kasutusel olevad isikus- tamata SIM-kaardid tulnud kasutajatel isikustada ning isikustamata kõnekaardid oleksid kaotanud pärast seadusemuudatuses fikseeritud üleminekuperioodi kehtivuse. Uute kõnekaartide ostul oleks ostja isiku aga juba tuvastama pidanud: kas kohe kõnekaarti ostes või hiljem, riiklikult tunnustatud keskkonna kaudu.¹ 3. detsembril 2020 kinnitasid nii Siseministeerium kui ka Majandus- ja Kommunikatsiooniministeerium aga, et Eesti riik loobub sellest plaanist ning seadusemuutusega seotud eelnõu ei ole enam töös (Mägi, 2020; Poom, 2020).

Eestis plaanitud seadusemuutus, mis oleks kohustanud teenusepakkujal kõik SIM-kaar- did, sealhulgas ettemakstud kõneaja ja andmemahuga² teenust tagavad kõnekaardid, enne teenuse osutamist isikustama, poleks olnud maailmas uudne. Riike, kus kõnekaartide isi- kustamist ei nõuta, on maailmas oluliselt vähem kui neid, kus see on vajalik.³ Esimesed nõuet rakendavad riigid võtsid meetme kasutusele juba 15–16 aastat tagasi ning ka isikus- tamise nõuded on järk-järgult detailsemaks muutunud. Eestiski on kõnekaartide isikusta- misest varem juttu olnud (Korpan, 2000) ning Euroopas toimunud terroriaktide tõttu on isikustamise nõude kehtestamist ka Euroopa Liidu üleselt kaalutud (GSMA, 2013, p. 10). Samas ei ole Eesti-sisesed ega Euroopa Liidu algatused seni seaduseks saanud.

Olgugi et kõnekaartide isikustamise plaaniga praegu edasi ei minda, tähendaks meetme rakendamine tulevikus Politsei- ja Piirivalveameti ning teiste korrakaitseasutuste menet- lustoimingutes lisavõimaluste teket. Samuti on isikustamismõue rahvusvaheliselt laialt levinud. Seetõttu vajab nõude tõhususe ja proportsionaalsuse küsimus tähelepanu.

Isikustamise mõue, mis on rahvusvaheliselt juba kasutuses, tähendaks Eesti sideteenuste pakkujale lisaandmete kogumise kohustust. Tavapäraselt koguvad sideteenuste pakkujad teenuse, sealhulgas kõnekaardi kasutajate (kasutus)andmeid oma ärihuvist lähtuvalt, et pakkuda atraktiivset ja konkurentsivõimelist teenust. Seega ei ole andmeid kogudes tee- nusepakkujatele oluline mitte see, kes on see isik, kes teenust kasutab, ja mida ta seda tehes teeb või ütleb, vaid millised on kasutusmustrid, mis on populaarsed tooted ning kui konkurentsivõimeline on teenus teiste teenusepakkujate toodetega võrreldes.

¹ Seaduseelnõu ettevalmistamise käigus ei tutvustatud viise, kuidas Eesti Vabariigi väljastatud isikutunnistuse- ta inimesed saaksid kõnekaarte soetada.

² Kõnekaardi abil mobiiltelefonis andmesideteenuse kasutamine on alternatiivne ja lihtsamini kättesaadav teenus kui lepinguline andmesideteenus ning turvalisem kui avalikud wifivõrgud.

³ Maailmas oli 2020. aastal 155 riiki, kus nõuti kõnekaartide isikustamist, ja 34 riiki, kus isikustamine pole kohus- tuslik (Yongo & Theodorou, 2020, p. 7).

Riiklikult SIM-kaartide isikustamise kohustuslikuks muutmise eesmärk on seevastu anonüümselt sideteenuste kasutamise piiramine ning parem võimalus vajaduse korral sideteenuste kasutamist ja kasutajaid kontrollida. Peamiselt nähakse isikustamises meedet võitluses organiseeritud kuritegevuse, terrorismi⁴ ja seksuaalkuritegude vastu (Kommussaar, 2020). Lisaks sideoperaatori enda andmekogumisele, mis võib sõltuvalt teenusepakkujast erineda, on Eestis praegu sideteenuse osutajal seadusega pandud kohustus aasta jooksul teenuse kasutamise andmeid koguda ja talletada, et vajaduse korral riiklikele päringutele andmeedastusega vastata. Samas on paljud kogutud andmed kõnekaardi kasutamise andmed. Isikustamata SIM-kaardi tõttu on need konkreetsete inimeste tegevuse jälgimise (või pigem tagasivaatavalt tegevuse kontrollimise) seisukohalt kasutud. Kõnekaartide kohustuslik isikustamine aitaks menetlustegevusele kaasa, sest kõik Eesti sideoperaatorite telefoni- ja andmesideteenuse kasutajad oleksid sellisel juhul identifitseeritavad, st iga sideteenuse kasutamise juhtumi eest vastutaks keegi.⁵

Samas ei ole SIM-kaartide isikustamine meede, mis võimaldaks ülevaadet kõikide teenuste kasutusmustrite kohta, kuna suhtluse sisu jääb jätkuvalt kaitstuks. Lisaks on internetiajastul, kui paljud suhtlusteenused toimivad andmeside alusel, teenuse kasutamismustrite aastapikkuse talletamise nõudmine kõikidelt teenuseosutajatelt, sh suhtlusrakendustepakkujatelt, suur kitsaskoht, mis võib oodatud efektiivsust pärssida. Mitmed suhtlusrakendused, näiteks Facebooki korporatsioonile kuuluv WhatsApp või Microsofti Skype, mis pakuvad andmeside alusel suhtlusvõimalust, on rahvusvaheliste firmade teenused-rakendused. Eesti seadused võivad neid firmasid küll teenuse osutamise viisi muutma kohustada, kuid kas teenuse pakkujad sellise muutuse sisseviimist ka sellise väikese turu jaoks vajalikuks peavad, on küsitav (Turk, 2020). Isegi kui teenusepakkujad kõnealuste muudatustega kaasa lähevad ning oma andmetalletamise ja andmete riigiasutustega jagamise praktikad muudavad, on siiski seadusega kaasnev kohustus kõigest suhtlusmustrite ja adressaatide avaldamine, mitte suhtluse sisu edastamine. Nii saab seadusemuutusega kaasnevat lisakohustust teenusepakkujatele pidada küll lisameetmeks, mis võib teatud olukordades menetlustegevust toetada, kuid mitte ennetavaks meetmeks, mille abil riigi kontroll kõigi kasutajate reaalajas toimuva suhtlustegevuse üle suureneks. Teenuse kasutamise andmetele ligipääs on jätkuvalt võimalik vaid menetlustegevuses loa alusel ja suhtluse sisu on vastavalt teenusepakkuja teenuse struktuurile kaitstud.⁶

Maaailmas ei ole kõnekaartide isikustamisega kaasnenud sellist kuritegevuse piiramist ja pidurdumist nagu on meetme abil loodetud saavutada. Kommunikatsioonitehnoloogia areng käib seadusandlusest ees ning kui isikustamise nõudega on reguleeritud suhtluse vormi, mis oli valdav 15 aastat tagasi, siis kõikide sideteenuse viiside kontrolliks pelgalt SIM-kaardi isikustamisest praegu enam ei piisa. Kuigi menetlustegevuses on kõnekaartide isikustamine aidanud isikuid tuvastada näiteks kõneeristuse puhul, on andmesideteenuse abil internetirakenduste kasutamise andmed keerukamad ning pelgalt teadmine, kes andmesidet millal ja millises mahus kasutab ning isegi, missugust rakendust andmeside abil kasutatakse, ei aita eristada näiteks seda, kellega sideteenust kasutades kontaktis oldi. Pealegi toimub mitmes veebirakenduses suhtlemine anonüümselt või pseudonüü-

⁴ Itaalias 2005. aastal vastu võetud seadus märgib isikustamise nõude põhjuseks just terrorismi (Stella, 2005; Turk, 2020).

⁵ Turk (2020) toob välja, et selline andmete talletamise nõue ei ole Euroopa Liidu seadustega kooskõlas ning Eesti lubas astuda samme nõuete parendamiseks, kuid pole seadusemuudatuse väljatöötamiseni veel jõudnud. Samas on oluline märkida, et kuigi Euroopa Kohus tunnistas Eesti seaduse aluseks oleva direktiivi kehtetuks, ei ole Euroopas uut direktiivi veel välja töötatud. Nii ei ole Eestilt nõutud uue seaduse väljatöötamiseks võimalik ka Euroopa direktiivist lähtuda.

⁶ Suhtluse sisu saab jälgida ilma lisaloata vastavalt suhtlusplatvormi avatusele ja kasutaja enda seadistatud turvasätetele avaandmete põhjal, näiteks avalik tekst Facebooki seinal.

mide abil või on suhtlusringkond rahvusvaheline. Seetõttu ei piisa sideteenuse kasutamise jälgimisest, et kõiki suhtluse osapooli tuvastada. Nii on kõnekaartide isikustamine kuritegevuse tuvastamiseks küll põhimõtteliselt tulemuslik, sest kõne või sõnumi puhul on osapoolte tuvastamine isikuandmete olemasolul lihtsustatud. Samas on isikustamine menetlustegevuses kvalitatiivset ja kvantitatiivset muutust ennustava meetmena olemuselt aegunud: muutunud on nii kommunikatsiooni viis (näiteks interneti suhtlusrakendused) kui ka mitmekesistunud saadetud sõnumite olemus (näiteks emotikonide kasutamine).

Lisaks sellele, et SIM-kaartide isikustamine ei ole toonud oodatud muutust või läbimurret kriminaalmenetluses, on kõnekaartide isikustamisega ilmnenud uued illegaalse tegevuse liigid, mis lõikavad kasu ja isikustamist kuritarvitavad, sh SIM-kaartide must turg.⁷ Nii ei tohiks ka Eesti kontekstis eeldada, et isikustamise nõude puhul ei muuda kuritegelikud organisatsiooni oma taktikat. Nõude rakendamisel tuleb valmis olla uut liiki kuritegude tuvastamiseks, kus teo keskmes on isikustatud SIM-kaardid ja nende võltsimine.

Kõnekaartide isikustamine võib samas plaanimatult kaasa tuua haavatavate ühiskonnaliikmete suhtlus- ja informatsiooni hankimise võimaluste piiramise ning takistada ajakirjandus- ja isikuvabadust, sh sõnavabadust ja demokraatlikke protsesse.⁸ Põhjusena, miks soovitakse kõnekaardid isikustada, on välja toodud kuritegude ennetamist ja kuritegelike organisatsioonide tuvastamist. Kuigi kõnekaarte kasutatakse ka kuritegelikel eesmärkidel, on kõnekaardid ühiskonnas laialdaselt levinud teenus, sest püsiva lepinguta sideteenus on kättesaadav ka majandilikult vähekindlustatud ja hinnatundlikele inimestele. Nõue võib tõsta teenuse hinda ja muuta selle lõpptarbijale raskemini kättesaadavaks; kuritahtlike kavatsustega kasutajad leiavad tänu tehnoloogia kiirele arengule aga uue viisi, kuidas varjatult suhelda.

Samuti ei tohi jätta tähelepanuta, et kõnekaarti kasutavast mobiiltelefonist on tänu internetiteenuste ja -rakenduste vahendamisele saanud informatsiooni hankimise, ühiskondlikus debatis osalemise ja oma vaadete edastamise vahend. Uuenenud kõnekaardi nõuded võivad aga piirata liikumiskesksete inimeste ligipääsu kõnekaartide soetamisele, suunata teenusepakkujad maakonnakeskustesse ja jätta keskusest kaugemal elajad kõnekaardi ostmise võimalusest ilma või ei võimalda sideteenust kasutada inimestel, kes ei soovi oma isikut teenusepakkujale avaldada (GSMA, 2013, p. 12).⁹ Lisaks ei saa suhtluse isikustamist võtta iseenesestmõistetava nõudena, sest kuigi õigust anonüümsele kommunikatsioonile ei ole, võib nõue riivata inimese õigust kaitsta oma andmeid (Roosve, 2020b).

Antud analüüs tutvustab kõnekaartide isikustamise nõudeid rahvusvahelises kontekstis, selgitab isikustamismõiste keskseid argumente ja vastuargumente ning toob välja, mis on suhe SIM-kaardi isikustamise ootuste ja võimaluste vahel. Analüüs juhib tähelepanu, et kõnekaardi isikustamise nõue ei pruugi anda ajastul, kus sideteenuse pakkuja vahendab

⁷ Privacy Internationali andmetel (Privacy International, 2019a) kasvas SIM-kaartide isikustamisega must turg, nii toimus see näiteks Pakistanis (Vt ka Dawn Media Group, 2021). Samas oli Eestis plaanitud eelnõu seletuskirjas eeskujuks toodud just Pakistan.

⁸ Näiteks on nn vilepuhujate anonüümse tagamine demokraatlike protsesside toimimiseks oluline (Roosve, 2020b).

⁹ SIM-kaartide isikustamise debatis räägitakse isiku varjamise soovist kui pahatahtlike kavatsuste tunnusest. Samas on suurandmete ajastul mõistetav teenuse tarbijate soov jääda anonüümseks, kuna suur hulk kasutaja kohta kogutavaid andmeid ei ole vajalikud mitte teenuse pakumiseks, vaid lähtuvad teenusepakkuja (äri)huvist. Nagu The GSM Associationi 2020. aasta raport „Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages“ välja toob, on mitmed autoritaarsed riigid rakendanud kõnekaartide isikustamise nõuet, et omada suuremat ligipääsu ja kontrolli inimeste suhtlusmustrite ja suhtluse üle (Yongo & Theodorou, 2020).

nii telefoni- kui ka andmesideteenust, täit ülevaadet kõnekaardi kasutaja suhtluse sisust (mis võiks korraldada tagada kvalitatiivse muutuse). Kommunikatsiooniviisid on mobiiltelefonide tulekust alates kiiresti muutunud ja uusi võimalusi kasutatakse ka kuritegelikul eesmärgil; ainuüksi kõnekaartide kohalik isikustamine ei too rändlusteenuse, suhtlusrakenduste ja krüpteeritud sõnumite ajastul märkimisväärset edu. Samas võib isikustamise nõue lisada riigile ülesandeid ja muuta elanike ligipääsu teenusele keerulisemaks.

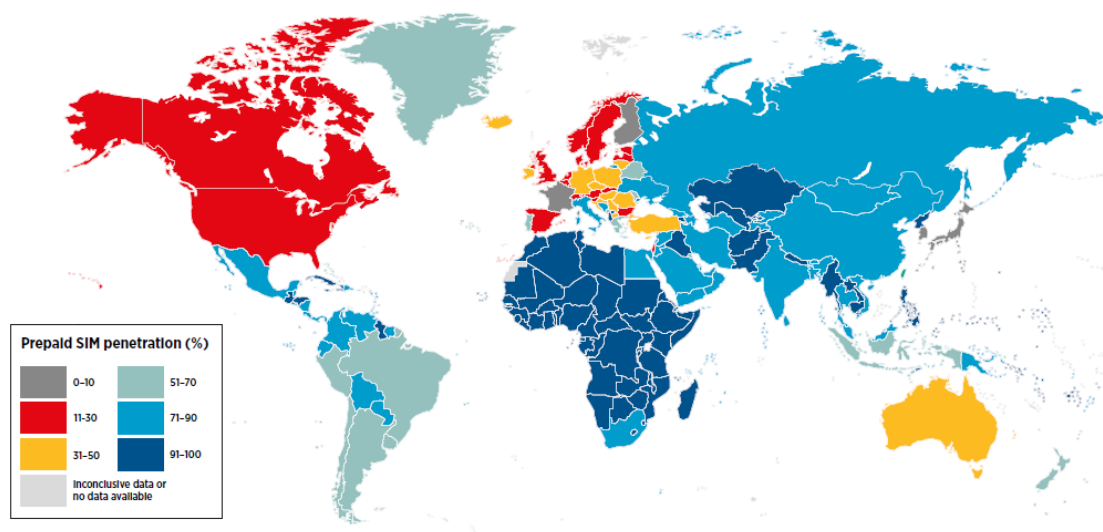
1. SIM-KAARTIDE ISIKUSTAMISE NÕUE MAAILMAS

Mobiiltelefonis kasutatavad SIM-kaardid jagunevad vastavalt telefoni- ja andmesideteenuse tarbimise eest tasumise viisile kaheks. Esmalt SIM-kaardid, mis on seotud lepingulise sideteenuse tarbimisega, st teenust tarbitakse sideteenuse operaatoriga sõlmitud lepinguga määratud mahus ja fikseeritud maksumuse ulatuses. Teiseks SIM-kaardid, mille puhul ostab tarbija krediiti, mille mahus saab telefoni- ja andmesideteenust kasutada, ehk nn kõnekaardid. Esimesel juhul on sideteenuse pakkuja ja tarbija vahel lepinguga fikseeritud, kes teenuse tarbimise eest vastutab ja tasub. Isegi kui teenuse lõppkasutaja on lepingulise kliendi leibkonna liige, on sideteenuse pakkuja teada inimene, kelle nimel teenust tarbitakse. Vastutava inimese isik on oluline, sest lepinguga võetakse finantskohustus. Kõnekaartide puhul aga sideteenuse pakkuja kaardi kasutaja isiku tuvastamise vajadus puudub, sest teenuse eest tasutakse enne teenuse tarbimist, kõneaeg või andme-maht lunastatakse kõneaaja ostmisega.

The GSM Associationi (edaspidi GSMA) 2020. aasta raporti „Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages“ alusel on 73% kasutusel olevatest SIM-kaartides ettemakstud kõnekaardid. Arvestades inimeste finantsvõimekust on kõnekaartide kasutamine enim levinud just arenevates maades, kus paljudel elanikel puudub sideteenuse lepinguliseks kliendiks saamiseks piisav ja/või püsiv sissetulek. Hinnanguliselt on 94% SIM-kaartides, mis Aafrikas kasutusel, ettemakstud kõnekaardid (Yongo & Theodorou, 2020, p. 6). See on olnud Aafrika mandri riikide jaoks oluline majanduse, sotsiaalse ja poliitilise arengu osa – tänu infrastruktuuri arengule on Aafrikas domineeriv „ainult mobiili“ (ingl *mobile only*) paradigma (Donovan & Martin, 2014). Blank ja Dutton (2014) juhivad tähelepanu tõsiasjale, et tänu telefonide arengule ja uutele tehnoloogilistele võimalustele jääb arenevates riikides (laual) arvuti omamine ühiskondlikust tehnoloogiaarengust välja ning telefonist saab paljudele esimene interneti kasutamise vahend. See tähendab, et sideteenusele ligipääs on oluline piirkonna majanduslikuks ja ühiskondlikuks arenguks. Aasias on kõnekaartide kasutuse protsent 79, Lõuna-Ameerikas 68, Euroopas 50 ja Põhja-Ameerikas 21 (Yongo & Theodorou, 2020, p. 6).

Eestis kasutatakse kõnekaarte teiste maailma riikidega võrreldes üsna vähe, GSMA 2020. aasta raporti andmetel on kuni 30% kasutatavatest SIM-kaartidest ettemakstud kõnekaardid. Sarnast (langus)trendi on Eesti sideteenuste turul märgitud mitmel korral (Korpan, 2002; Äripäev Kinnisvarauudised, 2008). Kõnekaarti peetakse Eestis pigem noortele mõeldud teenuseks ja sinna on ka turunduskampaaniad suunatud (Üürrike, 2014).

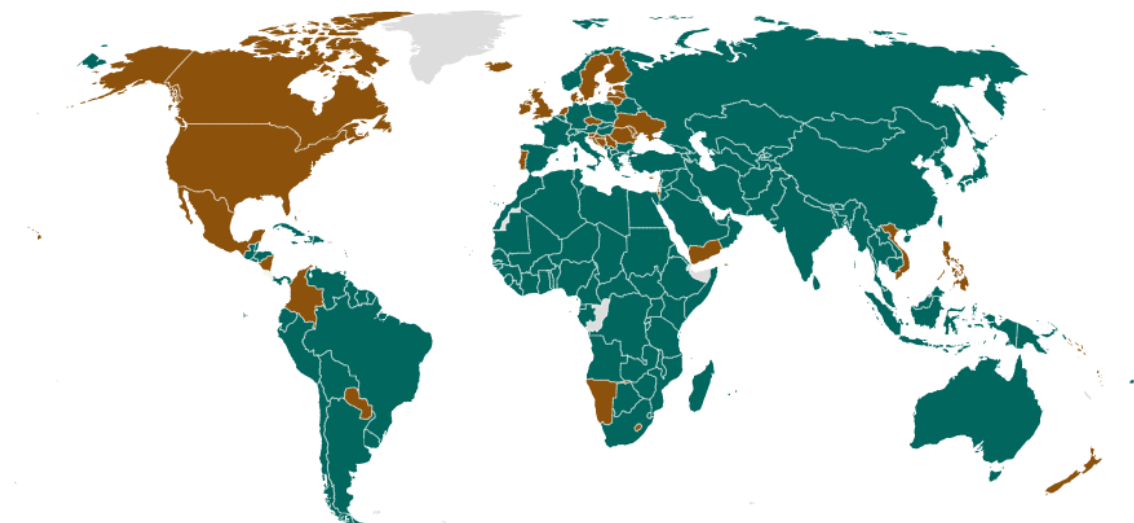
Kindlasti on kõnekaartide vähene hulk Eestis mingil määral seotud sellega, et lepingulise sideteenuse tarbimise puhul on võimalik hankida isikutuvastust võimaldav Mobiili-ID, mis ei vaja erinevalt teistest elektroonilistest isikutuvastuse teenustest andmeside olemasolu ja/või ID-kaarti. ID-kaardi turvariskiga seotud kaardiuuendused 2017. aastal näitasid ühiskonnale alternatiivsete isikustamisvõimaluste vajalikkust. Nii oli aastaks 2018 Eestis juba ligikaudu 200 000 Mobiili-ID-d aktiivselt kasutatavat SIM-kaardi omanikku (Sibold, 2018).



JONIS 1. KÕNEKAARTIDE KASUTUS MAAILMAS, PROTSENTUAALSELT. ALLIKAS: YONGO & THEODO-
ROU, 2020, P. 6

1.1. KÕNEKAARDI ISIKUSTAMIST NÕUDVAD RIIGID

2020. aasta märtsi seisuga on GSMA raporti andmetel 155 riiki, kus sideteenuse pakku-
jad küsivad kõnekaardi ostuks isikut tõendavat dokumenti ja isikustavad müüdava kõne-
kaardi. Kõnekaardi isikustamine on levinud kõigil kontinentidel ning peamised riigid,
kus selline nõue ei kehti, on lääneriigid, sh mitmed Euroopa riigid, Ameerika Ühendriigid
ja Kanada.



JONIS 2. KÕNEKAARDI ISIKUSTAMISE KOHUSTUSEGA RIIGID. ALLIKAS: BISCHOFF, 2020

Esimese riigina maailmas muutis 2002. aastal SIM-kaartide isikustamise kohustuslikuks Lõuna-Aafrika Vabariik, sellele järgnesid 2003. aastal Brasiilia ja 2005. aastal India. 2010-ndate algusaastatel kehtestasid esimeste seas isikustamisreeglid näiteks Sambia, Nigeeria, Kongo DRV ja Zimbabwe. Järgemööda on isikustamisreeglid kehtima hakanud paljudes riikides, kuigi ülemaailmne ühtne seisukoht isikustamisele endiselt puudub. Näiteks nõudis Euroopa Komisjon 2012. aastal põhjendust kõnekaartide isikustamise nõudele ning tões pärast uurimist, et nii kriminaalmenetluse läbiviimise kui ka ühisturu toimimise huvides puudub sellise meetme kasutuselevõtuks vajadus ning Euroopa Liidus ühtset meetme kehtestamist nõudma ei hakata (GSMA, 2013, p. 10).

Kõnekaartide isikustamist ei ole Euroopa Liidus seni kohustuslikuks tehtud ning isikuandmete talletamise seadusi on hoopis ühtlustatud ning talletusviise ja -põhjuseid piiratud.¹⁰ Ka on mitmed riigid, nagu Mehhiko, kes nõudis isikustamist juba üsna ammu, sellest nüüdseks kasu puudumise ja riigiaparaadi põhjendamatu koormamise tõttu loobunud. Üks viimaseid riike, kes tegi SIM-kaartide isikustamise kohustuslikuks, oli Austria, kus 1. jaanuaril 2019 jõustus nõue kõik uued kõnekaardid isikustada ning 1. septembril 2019 lõppes registreerimata kõnekaartide kasutusaeg.

Isikustamata kõnekaartide kasutusaaja lõppemise mõju on riigiti väga erinev ning kindlasti on küsimus ka selles, kui suur osa teenusekasutajatest kõnekaarti kasutab. Belgias jõustus kõnekaartide isikustamise seadus 2016. aasta detsembris ja 2017. aasta 7. juunil lõppenud üleminekuperioodi ajal isikustati 85% kõnekaartidest. Myanmar, kus isikustamata kõnekaardid muutusid aastal 2020 kehtetuks, raporteeris Telenor Myanmar aga, et jäi ilma 6,3 miljonist kasutajast.¹¹

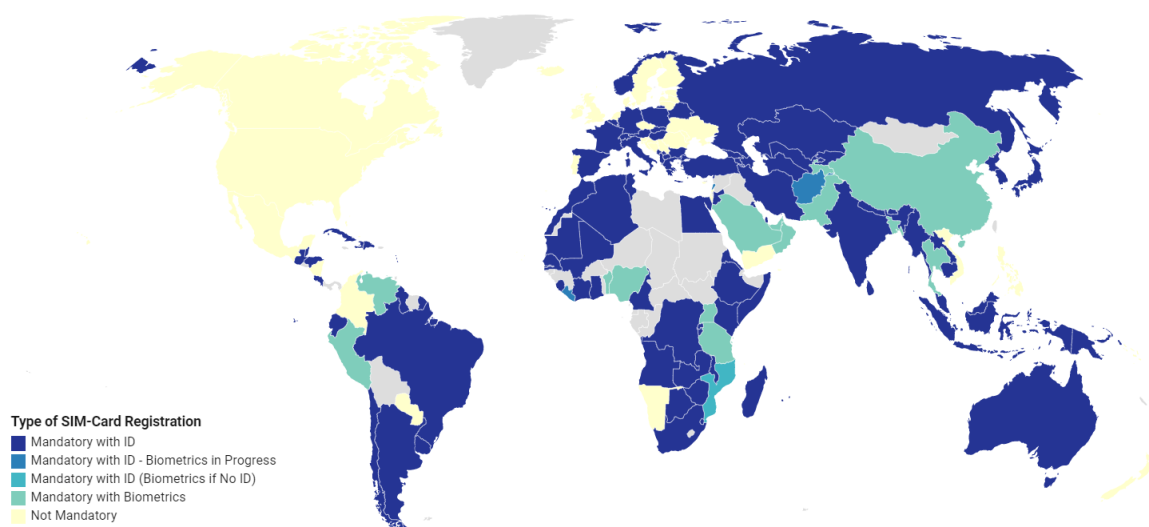
Missugust dokumenti isikustamiseks täpsemalt küsitakse ja missugused on isikustamise reeglid, on samuti riigiti väga erinev ning sõltub ka sellest, kas ja missugused on riigis väljastatud ja kehtivad isikut tõendavad dokumendid. Enim on levinud nõue, et kaardi isikustamiseks on vaja esitada isikut tõendav pildiga dokument, näiteks pass või isikutunnistus. Levinud on ka praktika, kus küsitakse inimese elukohta. Mõnel puhul piisab aga ühiskonna silmis väärika inimese, näiteks külavanema kirjalikust kinnitusest, et tegemist on kõnealuse isikuga.

Samas on mitmes riigis – Bahrein, Bangladesh, Hiina, Nigeeria, Pakistan, Peruu, Saudi Araabia, Tansaania, Uganda, Araabia Ühendemiraadid ja Sambia – SIM-kaardi soetamiseks ja isikustamiseks kohustuslik biomeetriline isikutuvastus. Ka Jordaania, Liibanon ja Libeeria plaanivad biomeetrilise isikutuvastuse kasutuselevõttu. Esimesena kehtestas biomeetriliste andmete kogumise nõude 2009. aastal Mehhiko, kus hiljem selline isikuandmete kogumine aga lõpetati. Enim levinud biomeetrilise isikutuvastuse meetod on seni sõrmejälje võtmine, mõnel puhul ka näo skaneerimine. Näiteks peavad Hiinas kõik uue telefoninumbri saajad oma näo skaneerida laskma. Sarnane tendents on ka Singapuris, kus Singtel, kelle käes on 50% turust, laseb kasutajatel näo telefonirakenduse kaudu skaneerida (Privacy International, 2019a).

SIM-kaartide isikustamise märkimisväärse uuendusena hakkas Uganda 2020. aastal arendama koostöös FSD Uganda ja CryptoSavannahga plokiahela tehnoloogiat, et täiendada Uganda SIM-kaartide registreerimise ja verifitseerimise protsessi (Privacy International, 2019b).

¹⁰ 2018. aastal jõustunud Euroopa Liidu isikuandmete kaitse üldmäärus (GDPR) seab andmete kogumisele ja talletamisele Euroopa Liidus ranged piirangud.

¹¹ Myanmaris rahvaarv on umbkaudu 51 miljonit inimest, 2019. aasta andmetel oli kasutusel 61,14 miljonit telefonibonenti ehk umbes 114 telefonikasutajat iga 100 elaniku kohta (Statista, 2020).



Joonis 3. Kõnekaardi isikustamise nõuded isikustamiseks vajalike dokumentide alusel. Allikas: Bischoff, 2020

Riigiti on erinev kõnekaardi isikustamise viis. On riike, kus kõnekaarte saab osta ainult sideteenuse pakkuja esindustest, on kohti, kus ka volitatud edasimüüjatel on õigus kaarte müüa, ning on riike, kus kõnekaardid on laialdaselt kättesaadavad nii sideteenuse esindustes kui ka edasimüüjate juures. Tihti nõutakse, et kaart isikustatakse juba soetamise hetkel.¹²

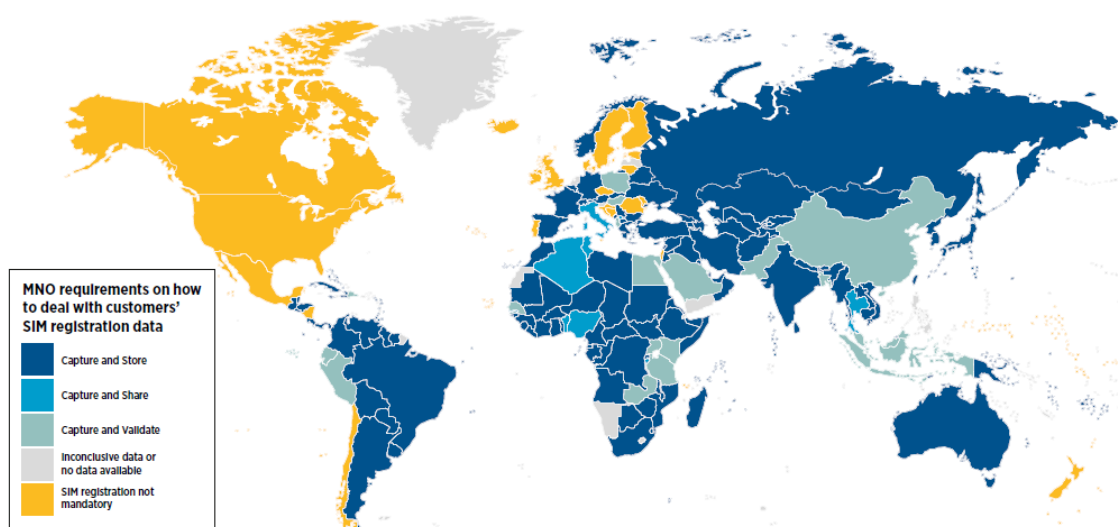
Hinnates kõnekaartide isikustamise ülemaailmset levikut, näib, et kõnekaardi isikustamise nõude kehtestamisel mängivad rolli nii see, milleks riigis sideoperaatori teenust peamiselt kasutatakse, kui ka see, kuidas kõnekaartide isikustamine kuritegevuse ennetamisele, piiramisele ja tõkestamisele kaasa aitab. Mitmes riigis on väga levinud just telefonikõnedel põhinevad pettused ja väljapressimised (Omandi Gumba & Wanyonyi, 2020). Nii on ka SIM-kaartide isikustamisest kuritegevuse piiramisel ja kuritegude lahendamisel suur abi. Samuti on isikustatud kõnekaardid meede terrorismivastases võitluses.

Samas puuduvad põhistavad andmed, et kõnekaartide isikustamise abil õnnestuks kuritegevuse ja terrorismiga edukalt võidelda. Näiteks Keenia, kus kõnekaartide isikustamise kohustus kehtib juba 5–6 aastat, on ikka samade probleemidega hädas (Omandi Gumba & Wanyonyi, 2020). Sedalaadi probleem on ka Tansaania, kus juriidiliselt ja praktiliselt ollakse pealegi silmitsi küsimusega, kuidas nõude vastu eksijaid karistada (Xinhua, 2019). Austraalia uurimus toob aga kõnekaartide info kasutamise keerukusena välja, et näiteks narkogrupeeriingud vahetavad kõnekaarte keskmiselt kuus korda päevas (Markson, 2007).

Kuigi andmete kogumise põhjuseks tuuakse välja turvalisuse tagamine ehk võimalus kõnekaardi omaniku isikut kontrollida, on kõnekaartide isikustamise puhul oluline ka see, kas ja millisel määral on inimeste sideteenuste kasutamise andmed seadusega kaitsitud ehk missugused nõuded on riik sideteenuse pakkujale isikuandmete ja sideteenuse kasutamise statistika kohta esitanud. GSMA raport (Yongo & Theodorou, 2020, p. 8) teeb siin vahet kolme liiki isikuandmete, sh kasutusandmete jagamise süsteemil ja grupeerib vastavalt riigid, mis antud praktikaid kasutavad

¹² Selline nõue kehtib Euroopa kultuuriruumis, näiteks Prantsusmaal, Kreekas, Itaalias, Luksemburgis, Montenegros, Põhja-Makedoonias, Šveitsis ja Türgis (Prepaid Data SIM Card Wiki, 2020).

- Kogu ja talleta (ingl *Capture and Store*) – sellises süsteemis peavad sideteenuse pakkujad koguma ja talletama SIM-kaardi kasutaja isikuandmeid. Konkreetse nõude alusel on võimalik ametkondadel kasutaja andmed sideteenuse pakkujalt välja nõuda. Sarnased nõuded on kehtestatud umbes 81% riikides, kus on SIM-kaartide isikustamine kohustuslik.
- Kogu ja jaga (ingl *Capture and Share*) – sellises süsteemis peavad sideteenuse pakkujad koguma ja jagama SIM-kaardi kasutaja isikuandmeid riigi ametkondadega süsteemselt, mitte konkreetse nõude alusel. Sarnased nõuded on kehtestatud umbes 6% riikides, kus on SIM-kaartide isikustamine kohustuslik.
- Kogu ja valideerid (ingl *Capture and Validate*) – sellises süsteemis peavad sideteenuse pakkujad valideerima kasutajate andmed riiklike andmebaaside alusel või kasutaja dokumendi alusel (näiteks elektroonilise ID-kaardi alusel). Sarnased nõuded on kehtestatud umbes 12% riikides, kus on SIM-kaartide isikustamine kohustuslik.



JONIS 4. SIM-KAARTIDE REGISTREERIMISEL ANDMEKOGUMISE NÕUDED SIDETEENUSE PAKKUJALE.
ALLIKAS: YONGO & THEODOROU, 2020, P. 9

Andmekasutusvõimaluste neutraalse näitena võib tuua Hispaanias 2019. aastal tehtud uuringu, mis hõlmas kõigi elanike telefonide seireandmete töötlemist. Andmeid kasutati riigis kehtivatele seadustele vastavalt ja volitusi ei ületatud. Olgugi et uuringu eesmärk oli täiustada avaliku sektori teenuseid, tekitas see üldsuses suurt pahameelt, kui rakendatud meetodist teada saadi. Vaatamata sellele, et andmed olid anonüümsed, joonistus andmekasutuse praktikast hästi välja, mida saab valitsus telefonisideandmetega teha (Jimenez Arandia, 2019; Biscoff, 2020).

SIM-kõnekaartide isikustamise puhul on seega oluline hinnata, mis on isikustamise nõude põhjus ning riigiasutuste volitused ja ligipääs kogutud isikuandmetele. Kuna üha rohkem on sideteenus seotud mitte telefoniteenusega, vaid andmeside abil internetiteenuste tarbimisega, siis ei ole kindlasti motivatsiooniks mitte ainult kasutajate tuvastamine, vaid ka jälgimine, kes ja missuguseid rakendusi ja teenuseid andmeside vahendusel tarbib.

Kui SIM-kaardi andmete käitlus ei ole seadustega reguleeritud, siis on võimalus, et andmeid jagatakse kolmanda osapoolega. Tegemist võib olla reklaamiagentuuride, teiste ri-

kide valitsuste, laenu sissenõudmisega tegelevate firmade ja teiste huvitatud osapooltega. Kolmandatele osapooltele kättesaadavaks muutunud informatsioon teeb kogu andmes-
tiku haavatavaks nii võimaliku varguse kui ka andmete kuritarvitamise osas.

Kuna mitmes riigis on sisse seatud range kontroll informatsiooni üle, mida riigi elanikud
tarbida võivad (näiteks Venemaa ja Hiina, aga ka mitmed Aafrika riigid), siis on sideteen-
nuse pidajatele seatud reeglid ja range kontroll elanikkonna sideteenuste tarbimise üle
osa viisist, kuidas ühiskonnas valitsevat meelsust ohjata ja võimul olemiseks *status quo*
tagada.

Veebitegevusi – külastatud veebisaidid, veebiotsingud (otsingusõnad), ostud jne – saab
seostada konkreetse seadmega. Nii saavad interneti üle kontrolli omavate riikide ametni-
kud vajaduse korral näiteks blokeerida teatud inimeste ja gruppide internetiühendust ja
-suhtlust. Inimeste identifitseerimine veebitegevuse alusel võib omakorda viia ahistamise
ja tagakiusamiseni.

Ekstreemne näide sellisest praktikast on Hiina. Hiinas on oma pärisnimega veebikon-
tode loomine, veebirakendustesse registreerimine ja SIM-kaartide isikustamine omava-
hel seotud, suhtlusrakendus või sotsiaalmeediakonto loomine nõuab ametliku nime ja
telefoninumbri esitamist. Sellega on piiratud või takistatud liba- ja varikontode tegemine
või salajane suhtlus.

Kuigi kõnekaartide isikustamise eesmärkides nimetatakse nii elanikele turvalisuse taga-
mist kui ka võitlust organiseeritud kuritegevusega, toetavad andmete kogumise ja kasu-
tamise praktika paljudes riikides pigem kontrolli elanikkonna üle ning võimaldavad
jälgida nende meelsust (Vt Amnesty International, 2011; Bischoff, 2019; Hiina teemal:
Beaucar Vlahos, 2019; Kobie, 2019).¹³ Samas põhistavaid andmeid meetme märkimis-
väärsest kasulikkusest kuritegevuse ennetamisel ja terrorismi tõkestamisel avalikkusele
kättesaadavad ei ole ning intsidentide jätkuv toimumine ja uute kuriteoliikide ilmnemine
lubab eeldada, et need meetmed ei ole seatud ootusi täitnud.

1.2. ISIKUSTAMIST MITTE NÕUDVAD RIIGID

2020. aasta märtsi seisuga ei ole kõnekaardi isikustamine kohustuslik 34 riigis, sh kõik
Balti riigid, Soome, Rootsi, Sloveenia, Moldova, Suurbritannia, Kanada ja Ameerika
Ühendriigid.¹⁴ SIM-kaartide registreerimine on praegu arutlusel näiteks Küprosel, Mal-
tas, Namiibias ja Vietnamis.

Põhjuseid, miks SIM-kaartide isikustamist kehtestatud ei ole või on isikustamine lõpetat-
ud, on erinevaid. Kesksed põhjused, mis kõnekaardid ei ole kõikides riikides kohustusli-
kud, on ühest küljest oht demokraatlike isikuvabaduste piiramisele ning teisalt puuduvad
andmed ja tõestus, et isikustamise süsteem suudaks lubatud eesmäärke täita. Lisaks näi-
tavad uuringud, mis keskenduvad Aafrika riikidele, kus peaaegu kõikjal on isikustamine
kohustuslik, et nõue pärsib vabaturumajandust, sest inimesed ei liigu enam sama vabalt
eri teenusepakkujate vahel soodsamat valides (Sumbwanyambe ja Nel, 2013) ning tarbi-
vad suurema tõenäosusega sama operaatori teisi teenuseid, sh finantsteenuseid (Jentzsch,

¹³ Bischoff (2019) toob oma uurimuses välja, et paljudes riikides, sh Tadžikistan, Araabia Ühendemiraadid, Saudi Araabia, Singapur ja Hiina, on riigivõimul piiramatu ligipääs sideteenuse pakkuja kogutavatele andmetele ning andmete talletamise periood ei ole seadusega määratud. The Human Freedom Index 2020 andemetele on kõnealu-
sed riigid isikuvabaduste poolest nimekirja viimase paarikümne hulgas (Vasquez & McMachon, 2020, p. 7–8).

¹⁴ Ameerika Ühendriikides on vastavasisuline diskussioon toimunud juba kümnekond aastat, kuid ühest seadust
pole seni vastu võetud. (Vaata: Stankey, Frappier & Guyton, 2010)

2012). Sarnase käitumismustri tuvastasid eurooplaste privaatsusharjumusi hindavas raportis ka Jentzsch jt (2012): kui ühele sideoperaatorile oma andmed esitatakse, siis jäädakse pikaks ajaks selle teenusepakkuja kliendiks.

SIM-kaartide isikustamise kohustuse kehtestamisele on mitmed riigid lähedal olnud, sh Eesti, kus 2020. aastal toimusid ettevalmistused seaduse muutmise eelnõuks. Iirimaa toimus 2017. aastal kõnekaartide isikustamise teemal diskussioon, kuid kuna otsest põhjust teenusepakkujatel isikustamist nõuda ei ole ning kõnekaartide puhul on kasutajatel võimalus kaart isikustada, siis nõue seaduseks ei saanud.

Mehhikos jõustus juba 2009. aastal seadus, mille alusel pidid kõik SIM-kaardi ostjad oma isiku tuvastamiseks ja SIM-kaardi isikustamiseks andma sõrmejäljed. Sama seadus muutus 2012. aastal kehtetuks ja kõik andmed hävitati, sest süsteemil puudus rakendus ja kasutegur (Privacy International, 2019a). Ka Liibanon loobus 2014. aastal rahvusvaheliste mobiiliseadmete registreerimisest, kuna leiti, et protsess on nii aja- kui ka ressursimahukas ega too suurt tulu.

Kuid Rumeenia on loonud pretsedendi, kus pärast mitmendat korda seaduse vastuvõtmist ja kehtetuks tunnistamist võeti sama isikustamise seadus taas vastu ning see jõustus 2020. aasta 1. jaanuaril (EDRi, 2019). Kuigi seaduse pooldajad väitsid, et isikustamise puhul saab paremini jälgida hädaabikõnede tegijaid ja libakõnede autoreid karistada, on kohus seda pidanud ebaproportsionaalseks meetmeks, sest isikustamisel kogutakse suures hulgal isikuandmeid ja see piirab eraelu vabadust. Pealegi on siit näha suhtumine, et kõik hädaabikõnede tegijad on juba eos süüdi valekõnes. Viimasel korral seadust vastu võttes riigikohtu varasemaid argumente aga arvesse ei võetud. Näib, et seadusega nõude kehtestamine oli olulisem kui juriidiline hinnang meetme vajalikkusele.

Ka isikustamisega kaasnevas terrorismi ja/või organiseeritud kuritegevust takistavas mõjus ei ole põhistavaid andmeid, sest isikustamisega saab tuvastamisel kergemini jälgida kuritegelikel organisatsioonidel ja võrgustikel, mitte aga jälgida või jälitada üksikuid inimesi, kes on radikaliseerumas või kuritegu toime panemas. Tõendite puudumine või vähesus ongi üks peamine põhjus, miks on seni puudunud poliitiline tahe isikustamine üleilmselt kohustuslikuks teha.

Vaba turumajanduse puhul saab hinnateadlik ja -tundlik klient lihtsasti teenusepakkujat vahetada ja soodsama pakkumise valida. Isikustamata ettemakstud kõnekaardid annavad selleks hea võimaluse. Kõnekaartide isikustamine ja kaartide omamisega kaasnevad piirangud, mis on mõnes riigis kehtestatud¹⁵, pärsivad aga sellist võimalust. Pealegi on uuringud kinnitanud, et isikuandmete edastamisega sideoperaatorile on inimesed ka sellele lojaalsemad.

1.3. ISIKUSTAMISE REEGLID KÜLASTAVATELE VÄLISMAALASTELE

Kõnekaartidele kehtestatud isikustamise reeglid võivad muuta kaardi hankimise keeruliseks riigi elanikele, kuid riiki külastavatel välismaalastel võib see lausa võimatuks osutuda. Kuigi riiki külastavate välismaalaste telefonisuhtluse ja internetiteenuste tarbimise piiramine isikustamise nõudega võib olla sihipäraseks heidutusmeetmeks ja mõeldud pahatahtlike kavatsuste ennetamiseks, on anonüümne suhtlus võimalik ka alternatiivsete sõnumi- ja kõnerakenduste kaudu, milleks on vaja kõigest ligipääsu wifi võrku.

¹⁵ Näiteks tohib Bulgaarias ja Ungaris ühe inimese nimel olla kuni kümme SIM-kõnekaarti, Myanmaris ainult kaks (Prepaid Data SIM Card Wiki, 2020).

Kuid kõnekaarti soetada püüdnud välismaalasel on vaja anda enda kohta väga detailseid andmeid. Esiteks on ranged nõuded isikut tõendava dokumendi kohta. Kuigi Euroopa Liidus on võimalus teisi riike külastada ka isikutunnistuse, sh Eesti ID-kaardi abil, aktiveeritakse näiteks Poolas kõnekaarti ostva välismaalase isikutunnistusena ainult passi. Sama nõue on ka Norras, mis ei ole küll Euroopa Liidu liige, kuid kuulub Euroopa Majanduspiirkonda.

Teiseks nõutakse isikustamise puhul mõnikord kohaliku aadressi olemasolu. Näiteks Albaanias ja Saksamaal on kõnekaardi soetamisel selline nõue. Saksamaal sobib aadressiks ka majutusasutuse aadress, kus peatutakse. Samas on üha levinumad ka reisimise vormid, kus konkreetne aadress puudub, näiteks loodusturism või reisimine haagissuvilaga. Niisugusel juhul ei ole inimesel aadressi ette näidata. Vastavalt riigis kehtestatud reeglitele ei saa sellisel juhul kõnekaarti osta. Kuigi rändlusteenus, millest tuleb hiljem juttu, on Euroopa-sisest kõnekaartide ostmise vajadus vähendanud, on teenuse kättesaadavuse tagamine siiski oluline näiteks elutähtsate teenuste tarbimiseks sihtriigis ja kohaliku aadressi olemasolu nõue võib seda märkimisväärselt pärssida. Arvestades, et inimene võib nii riigi elanikuna kui ka külalisena oma elu- ja peatuspaika küsimusteta vahetada, pole selliste andmete nõue tarvilik ega proportsionaalne isegi isikutunnistust nõudes.

Kolmandaks, kõnekaartide müügi süsteem ja isikustamise protsess on riigiti väga erinev ning tihti pärsib see teenuse kättesaadavust ja kasutamise võimalust. Näiteks Austrias on kõnekaardi isikustamine laialt levinud teenus, mida saab teha nii sideteenuse esinduses kui ka veebi vahendusel, kaardi registreerimisel lisandub teenustasu. Türgis saab SIM-kaardi hankida ainult 120 päevaks ja ühele telefonile vaid ühe kaardi – pikema visiidi puhul muutub see probleemiks. India nõuab kõnekaardi soetamiseks kohaliku isikukoodi olemasolu (Prepaid Data SIM Card Wiki, 2020).

Globaliseerivas maailmas, kus inimesed reisivad järjest rohkem, on kohalikud kõnekaardireeglid tihti takistuseks kohalike sideoperaatorite teenuste kasutamisel. Lisaks on nõuded esitatavatele isikuandmetele tihti päris ranged, eriti väljaspool Euroopa Liitu, kus ühised isikutunnistuse reeglid puuduvad. Mõnikord kogutakse välismaalaselt lausa bio-meetrilisi andmeid.

Samas ei ole kehtestatud isikustamise nõuded aga alati seatud eesmärgiga proportsioonis. Näiteks kohaliku aadressi esitamisest hoolimata ei ole teenusepakkujal võimalust ega volitust isiku elu- või peatumiskohta kontrollida. Lisaks erineb riikide andmekasutuspraktika ja sideteenuste pakkujal ei ole alati kontrolli enda kogutud andmete üle. Sellisel juhul võib välismaalaste isikuandmete jõudmine teiste riikide sideteenuse pakkujate käsutusse olla probleemne (suureneb identiteedivarguse võimalus või ebaproportsionaalse jälitustegevuse oht sihtriigis).

1.4. ISIKUSTAMISEGA KAASNEVAD PROBLEEMID

Kuigi eeltoodud statistika näitab, et SIM-kaartide isikustamine on rahvusvaheliselt levinud praktika ja isikustamiseks vajalike andmete hulk kasvab, on kõnekaartide isikustamisele ka vastuargumente, mis toovad välja, et kõnekaartide isikustamine võib õõnestada ühiskondlikku võrdsust ning demokraatlikke väärtusi, k.a. sõna- ja kogunemisvabadust. Kolm keskset teemat, mis isikustamisega kaasnevad, on sideteenuse ligipääsetavus, sideteenuse olemasolu nõudvate teenuste ligipääsetavus ning võimalus ohutult, ilma jälgimise ja repressioonideta sideteenuse võimalusi kasutada. Selleks et mõista, kuidas ühis-

kondliku turvalisuse eesmärgil või ettekäändel kõnekaartide isikustamine võib ühiskonna kihistumisele ja ebademokraatlikele praktikatele kaasa aidata, tuleb vaadata, missuguseid arenguid võib isikustamine endaga kaasa tuua.

Üks keskne argument, mis kõnekaartide isikustamise nõude vastu tõstatatakse, väidab, et isikustamisnõudega võivad haavatavad ühiskonnagrupid jääda ilma sideteenuse võimalusest. Haavatavaid grupe on selles kontekstis mitmeid ja nii on ka sideteenusele ligipääsu tagamise teema mitmetahuline.

Privacy Internationali andmetel oli 2019. aastal maailmas 1 miljard inimest, kellel puudub kehtiv isikut tõendav dokument.¹⁶ SIM-kaartide isikustamise nõude puhul, kus inimesel tuleb kohale minnes isikutunnistust näidata, tähendab see teenusele ligipääsu puudumist. Samal ajal kui rahvusvahelised organisatsioonid teevad jõupingutusi arenevate riikide aitamiseks, et elanikele saaks väljastatud isikut tõendavad dokumendid¹⁷, on mitmed riigid võtnud SIM-kaartide isikustamiseks vajaliku isikutuvastamise jaoks kasutusele alternatiivseid meetodeid. Mitmes Aafrika riigis sobib isikutunnistuse puudumisel kinnituseks näiteks külavanema kirjalik kinnitus elaniku isiku kohta. Selline praktika on kasutusel näiteks Nigeerias (Yongo & Theodorou, 2020, p. 8). Tihti tuleb sobiliku isikutunnistuse puudumisel aga end kaardi kasutajaks registreerida kas kolmandate isikute kaudu või leida endale käendajad. Üha enam levib ka biomeetriliste andmete kogumine kas ainsa või täiendava isikustamise meetmena – ka see võimaldab isikutunnistuse puudumisest hoolimata ligipääsu sideteenustele.

Teine haavatav grupp, kes võivad jääda kõnekaardita, on põgenikud. Neil puudub tihti isikutunnistus ja riigis, kuhu on põgenetud, põgenikelaagris või asüüli taotlemise protsessi käigus (sideteenuste ostmiseks sobilikke) isikutunnistusi ei väljastata. Nii on sellele inimgrupile sideteenused tihti kättesaamatud – nende võimalus ja õigus vabale suhtlusele on piiratud.

Samas pole dokumentide olemasolu ainus aspekt, mis sideteenuse tarbimise võimaluse määrab. Ka füüsiline mobiilsus on oluline teenuse kättesaamiseks. Kui inimesel on raskusi liikumisega, ei pruugi ta pääseda kõnekaardi registreerimiseks füüsiliselt teenusepakkuja juurde isikut tõendama. Liikumispuudega inimese puhul on tõenäoline, et isikustamise nõue tähendab teenusele ligipääsu puudumist või eeldab teise inimese abi. Kuigi Eestis on riiklikult tunnustatud isikustamise teenuseid mitmeid ning plaaniti võimaldada ka kaardi isikustamine-aktiveerimine pärast kaardi ostmist, tuleb teenusele ligipääsetavusele tähelepanu pöörata. Elanike digipädevus on erinev ja uute nõuete kehtestamisel tuleb tagada abi teenuse edasiseks tarbimiseks.

Samuti on oluline tähelepanu pöörata sellele, et ka isikustamise nõude järel oleks kõigile soovijatele SIM-kaardid endiselt kergesti kättesaadavad nii tarbijate majanduslikku olukorda kui ka teenuse füüsilist asukohta silmas pidades.

Hinnast tingitud kättesaadavuse tagamise puhul on oluline teenuse lõpphind. Uuringud on välja toonud, et SIM-kaartide isikustamise seaduse kehtima hakkamisel on teenusepakkujad tihti sunnitud kinni maksma kaasnevad muutused, sh isikustamiseks vajaliku

¹⁶ Maailmas on need tihti vaesemate piirkondade ja riikide elanikud, kus isikutunnistuste väljastamine on ühel või teisel põhjusel piiratud. Samas on isikutunnistuse omamised reeglid ka arenenud maailmas erinevad, näiteks Suurbritanniast ei nõuta, et elanikel oleks ametlik isikutunnistus (pass on reisidokument, juhuluba on vaid sõiduõigusega kodanikel). Ameerika Ühendriikides, kus isikutunnistuse väljastamise reeglid on eri osariikides erinevad, on isikutunnistuse puudumine teatud ühiskonnagruppidel näiteks valimiste puhul suur probleem, sest elanikel pole võimalus oma demokraatlikke õigusi kasutada (vt ka Ameerika Ühendriikides on riikliku ID kaardi puudumine suur probleem ka valimiste kontekstis (NPR, 2012)).

¹⁷ ÜRO eesmärk on, et aastaks 2030 on kõikidel inimestel isikutunnistus (UN LIEG Technical Secretariat, 2019).

infrastruktuuri ja personali koolitamise. Sellised lisakulutused võivad muuta teenuse nii edasimüüjale kui ka lõpptarbijale kallimaks ning seetõttu väheneb elanikkonna võimalus sideteenuseid kasutada.

Lisaks on suhteliselt hõredalt asustatud Eestis oluline, et ka pärast SIM-kaartide isikustamise seaduse jõustumist oleks kõnekaartide edasimüüjatel endiselt võimalus ja huvi kõnekaarte müüa. Kui kõnekaartide edasimüümise võimalust ei ole (nt kohalikus külapoes pole enam võimalust kõnekaarti soetada, sest teenuse pakkuja peab teenuse tarbija isikustama) või puudub edasimüüjal motivatsioon, sest kõnekaartide edasimüümisest ei saa tulu, siis koonduvad sideteenuste tarbimise võimalused suurematesse maakonnakeskustesse. Ligipääs keskustele on leibkonniti aga väga erinev ja nii võib ka ligipääs teenustele senisega võrreldes halveneda.

Pealegi on kõnekaardita mobiiltelefon nii maailmas kui ka Eestis mõnel juhul ainus võimalus sideteenust kasutada, näiteks puudub paljudel inimestel piisav sissetulek, et sideteenuse pakkujaga lepingut sõlmida. Seega tuleb seadusmuudatuse planeerimisel hinnata ka seda, kui palju SIM-kaartide isikustamise nõue kõnekaarti kasutavate inimeste elu raskendab ehk kui paljusid inimesi uus nõue mõjutab ja kuidas kaasnevaid probleeme ennetada.

Teenuse kättesaadavuse võimalik kitsenemine mõjutab eelkõige vähekindlustatud ühiskonnaliikmeid. Sideteenuse kättesaadavus on oluline kõikidele inimestele, sest võimaldab suhtlemist nii kogukonnas kui ka riigiasutustega. Nii tuleb kõnekaartide isikustamisega kaasnevate nõuete puhul arvestada, et need ei lisaks probleeme.

Kuigi riigiti on kohustus sideteenuse pakkujate ees erinev ning näiteks Eestis peaks riik sideteenuse pakkujaid uute nõuete sisseseadmisel majanduslikult abistama, ei tähenda see, et meetme saaks ilma ühiskondlikku ja majanduslikku kulu põhjalikult hindamata rakendada – riigi võetav finantskohustus peab olema põhjendatud ning siinkohal tähendaks see seatud eesmärkide saavutamist ehk kuritegevuse ennetamist, terrorismiohu tõkestamist ja seksuaalkuritegude vähenemist. Samas ei ole meetme kasulikkus sellisel kujul rahvusvahelises praktikas kinnitust leidnud.

Teine oluline aspekt sideteenuste ahenemisel on teiseste teenuste kättesaadavus. Sellele on suurt tähelepanu pööratud just arenevates maades, kus sideteenustega kaasnevate hüvede hulk on võib-olla kõige lihtsamini eristuv, sh finantsteenuste kättesaadavus, ise teenuse pakkumise võimalus ja ligipääsetavus informatsioonile. Sideteenustele juurdepääsu piiramine võib peale suhtluse piiramise nõrgestada majanduslikult haavatavate inimeste ühiskondlikku positsiooni: haavatavad ühiskonnagrupid võivad jääda ilma võimalusest tarbida edasisi teenuseid, sh finantsteenuseid, mida telefoni- ja/või internetiteenuse omamine võimaldab.

Teiseste teenuste ligipääsetavuse kitsenemisega kaasnevast ühiskonna kihistumisest ja sellest tulenevast ühiskonna gruppide üksteisest kaugenemisest räägitakse pigem arenevate riikide puhul. Isikustatud kõnekaardi puudumisel (või vastava seaduse jõustumisega kaasneval kõnekaardi kasutamise võimaluse kadumisel) kaob inimestel ligipääs nii raha ja kõneaja saatmise võimalusele kui ka internetis leiduvale informatsioonile. See tähendab, et osa ühiskonnaliikmeid jääb ilma võimalusest omaste või oma elujärge parandada, sh teadmisi hankida.

Kuigi Eesti kontekstis ei pea teiseste teenuste kasutamise puhul rääkima finantsteenustele ligipääsu puudumisest, sest teenuse kasutamiseks vajaliku isikustamise jaoks kasutatakse igal juhul teisi riigis tunnustatud isikustamise meetodeid (sh Mobiili-ID), on ka siin oluline mõelda, missugustele teenustele ja teadmistele telefoni- ja internetiteenuse kasuta-

misvõimaluseta inimene ligipääsu kaotab. Kui ühiskond toetub üha rohkem e-teenustele ja ametlik informatsioon on üha rohkem elektrooniliselt edastatud, siis nendele ligipääsu puudumisega võib inimene jääda infosulgu ja hätta eluks vajalike toimingute tegemisel.

Kolmas keskne teemadering, mis kõnekaartide isikustamise puhul tähelepanu all on, on inimeste õigus anonüümsusele ja võimalus anonüümselt suhelda, mis muutub kõnekaardi isikustamisega võimatuks. Kuigi anonüümsusest räägitakse SIM-kaartide isikustamist planeerides ja selgitades kui võimalusest kriminaalset või kõlbeliselt probleemset tegevus varjata, on oma isiku varjamiseks, ka demokraatlikus ühiskonnas, põhjuseid rohkem (Privacy International, 2019a).

Kuna kõnekaartidega kaasnevad nii telefoni- kui ka andmeside kasutamise andmed ning nagu eespool välja toodud, on eri riikide sideteenuste kasutamise jälgimise ja kontrollimise praktikad erinevad ning mõtte-, sõna-, usu- ja teiste vabaduste lubamine varieerub, siis on inimeste anonüümsuse tagamine ja selle vabaduse säilimine vajalik. Nii kodu- kui ka välisriigis kõnekaardi isikustamise puhul võivad teatud inimgrupid, näiteks inimõiguste eest võitlejad, ajakirjanikud ja marginaliseeritud gruppide või vähemuste liikmed, sattuda ahistamise, tagakiusamise ja vägivalda ohvriks. Kuna internetirakendustega on avaliku suhtluse piirid nihkunud ning paljud sotsiaalmeedia postitused on avalikult kättesaadavad, siis on kõigil inimestel oht sattuda oma sõnade eest mittedemokraatlikus režiimis tagakiusatuks (Amnesty International, 2011).

Mõned kõnekaardi isikustamise debatis esitatud vastuargumendid ja murekohad ei ole üheselt ülekantavad kõikidele riikidele. Eestis on riiklikult väljastatud isikutunnistuse omamine riigi elanikele, ka ajutistele elanikele, kohustuslik. Samas on mitmed teemad väga ajakohased ka Eestis, kus kasvab ääremaastumine (Plüschke-Altof, Loewen ja Leetmaa, 2019; Riigikontroll, 2020) ning ajakirjandus- ja sõnavabaduse indeks on viimastel aastatel kahanenud. Viimase puhul mängivad Eestis olulist rolli nii riigi väiksusest soodustatud üksikute meediakanalite monopoolne roll kui ka üha polariseerunumad vaated, mis nõuavad sõnavabadusele viidates suuremat kõlapinda ja proportsionaalset esitamist (Reporters Without Borders, 2020). Samuti tehakse süsteemset kriitikat ajakirjanike erapooletuse ja nende esitatud väidete õigsuse teemal (Reisenbuk, 2019). Sellises avalikult polariseeritud arvamusruumis on uuriva ajakirjanduse jaoks anonüümse suhtluse tagamine hädavajalik. Lisaks on oma identiteedi varjamise võimalus oluline, et inimesed saaksid abi otsida, näiteks usaldustelefoni teenuse kasutamine, ning juhtida tähelepanu ebademokraatlikele või lausa kriminaalsetele protsessidele, näiteks anda anonüümse telefonivihje. Nii ei ole ka Eestis võimalik kõnekaartide isikustamise vastuargumente ja isikustamisega kaasnevaid probleeme tähelepanuta jätta ning nõuete kehtestamisel tuleb teenuse ligipääsetavus ja demokraatlike väärtuste toimimine tagada.

Kuna andmesideteenus annab tänapäeval ligipääsu demokraatlikule debatile, siis on võimalus, et kõnekaartide isikustamisel ei saa kõik ühiskonnaliikmed enam sama lihtsalt sellele debatile ligi: e-riigis, kus üha rohkem teenuseid pakutakse veebipõhisena, peab sellise võimaluse piiramisele olulist tähelepanu pöörama ning plaanitud muutuste mõju hindama ja vajaduse korral abimeetmed kasutusele võtma.

Viimaks ei tohi tähelepanuta jätta tõsiasja, et isikustamise nõude kehtestamisel võib tekkida olukord, kus eri- või kriisiolukorras pole riigi elanikel teenust võimalik saada. Ekstreemsete ilmastikuoludega riikides on selliseid olukordi sageli tekkinud. Näiteks Indias jäid mudalaviinide tõttu inimesed ilma nii oma varast kui ka isikut tõendavatest dokumentides, mis oleksid uue kõnekaardi hankimist võimaldanud. Nii tuli kasutusele anda ajutised isikustamata kõnekaardid (Press Trust of India, 2014). Kuid ka ilmastikuoludest sõltumata tuleb valmis olla erandite tegemiseks ning see ka seadustesse ja süsteemi integreerida.

2. SIM-KAARTIDE ISIKUSTAMISE EESMÄRK: VÕIMALUSED JA TEGELIKKUS

2.1. ERINEVAD SIDETEENUSED

Kuna tehnoloogiline areng võimaldab telefone lisaks kõneteenustele kasutada ka internetiteenuste jaoks, siis vahendab SIM-kaart vastavalt telefoni tehnoloogilisele võimekusele ja kõnekaardi omaniku teenusepakatile kaht liiki sideteenust: telefoniteenust ja andmeside- ehk internetiteenust.

Telefoniteenus hõlmab nn traditsioonilisi teenuseid ehk telefonikõnesid ja tekstisõnumite saatmist. Mõlemal puhul on tegemist teenusega, kus on vajalik telefoniteenuse olemasolu ehk side, kõne või teksti saatmine toimub kahe telefoninumbri vahel. Sellised otsesed kontaktid telefoninumbrite vahel on lihtsasti tuvastatavad. Samas sõltub nende telefoninumbritega seotud isikute tuvastamine teenuse olemusest. Lauatelefoni puhul on tegemist lepingulise teenusega ja igal numbril on kas vastutav institutsioon või eraisik; (väheste) avalike telefonide puhul jääb kasutaja isik anonüümseks. Mobiiltelefoni puhul on kõneteenuse kasutamine aga võimalik nii lepingulise SIM-kaardi abil kui ka ettemakstud kõnekaarti kasutades. Viimased on vastavalt riigis kehtivatele seadustele kas isikustatud või isikustamata. Juhul kui kõik riigis müüdavad SIM-kaardid on isikustatud, on ka telefoniteenuse tarbimine jälgitav.

Andmesideteenus, mida vastava võimekusega telefoni olemasolul teenusepakkujalt osta saab, annab mobiiltelefoni vahendusel võimaluse kasutada internetti ja internetti kasutavaid rakendusi, näiteks sirvida veebilehti, kasutada sotsiaalmeedia teenuseid ja suhtlusrakendusi. Internetiteenuse puhul annab sideteenuse pakkuja kasutajale ligipääsu internetile – kuidas ja milleks kasutaja internetti kasutab, seda teenuse pakkuja ei määra.¹⁸ Internetiteenuse kasutamise maht oleneb teenuse paketist ja teenuse maksumusest konkreetses riigis.¹⁹ Teenusepakkujal on lihtne jälgida teenuse kasutamist, sest andmeside aktiveerimine ja kasutamine jätab operaatorile logi. Seda logi talletatakse vastavalt riiklikult kehtestatud reeglitele. See, kas andmesideteenuse kasutaja isik on tuvastatav,

¹⁸ Oluline on täheldada, et kuigi internetivabadus on valdav, on mõnes riigis kehtestatud riiklikud piirangud veebilehtede külastamisele ja veebirakenduste kasutamisele. Näiteks on Hiinas blokeeritud mitmed läänemaailma veebiplatvormid, sh Facebook.

¹⁹ Vastavalt kõnepaketile või kõnekaardiga lunastatud internetiteenusele on võimalik kasutada kas teatud mahus andmesideteenust või teha seda lausa piiramatult. Erinevate internetiteenuste kasutamiseks on vaja erinevat andmesidemahtu, näiteks videote vaatamine nõuab suurt andmesidemahtu, tavalise tekstipõhise internetilehe lehitsemine aga oluliselt väiksemat.

sõltub sellest, kuidas ta teenust kasutab ja missugused on riiklikud reeglid. Juhul kui andmeside on osa lepingulisest teenusepaketest, on teenuse kasutaja isik teada; kõnekaartide kaudu andmesideteenuse ostmise puhul on teenusekasutus aga isikustatav vastavalt sellele, missugused on kõnekaartide isikustamise reeglid riigis.

Andmeside puhul ei ole aga teenuse tarbimine iseenesest see, mille puhul oleks kõnekaartide isikustamisest suurt abi ning mis tooks suure läbimurde kuritegevuse ja terrorismiga võitluses. Andmeside üldisest kasutamisest hoopis tähtsam on sel juhul võimalus isikustada konkreetsete teenuste kasutamine, näiteks sotsiaalmeediaplattformide ja suhtlusrakenduste kasutamine. Sarnaselt telefoniteenuse otsestele kontaktidele loodetakse, et saab jälgida ka andmesideteenuseid kasutavate inimeste kontakte. Juhul kui kõnekaardid on isikustatud, on teoreetiliselt võimalik tuvastada, kes mis ajahetkel missugust internetilehte külastab või suhtlusrakendust kasutab.

Suhtlusrakenduste, veebiportaalide ja internetikommentaariumide kasutamise puhul on sarnaselt telefoniteenusele kasutajate isikustamise ning teenuste kasutamise jälgimise puhul huviks see, et oleks võimalik tuvastada suhtlusvõrgustikud. Teisisõnu, kui telefoniteenuse puhul on korrakaitseasutustel vastava loa olemasolul võimalik tuvastada, missuguste (isikustatud või isikustamata) telefoninumbritega konkreetne inimene suhelnud on, ehk tuvastada suhteseosed, siis kuritegevuse tõkestamiseks on vaja sarnast ligipääsu ja tuvastatavust ka andmesideteenuse kaudu kasutatavate teenuste puhul.

Nõuded isikute tegevuse talletamiseks andmesideteenuse kaudu kasutatavate teenuste ehk internetirakenduste ja veebilehtede kasutamise puhul on vaja kehtestada teenuse pakkujale. Kui sideoperaatorid on igas riigis registreeritud ning nad peavad kehtivaid seaduseid järgima, siis internetirakendused on tihti globaalsete firmade tooted ning nende isikuandmete, talletamise ja kasutamise reeglid on universaalsed. Ühes riigis toimuv seadusemuutus ei pruugi globaalset teenusepakkujat oma teenust muutma panna, vaid võib teenuse pakkumise selles riigis sootuks lõpetada (Turk, 2020).

Lisaks toob Turk (2020) välja, et praegu Eestis kehtiv nõue sideoperaatoritel andmeid talletada ei ole kooskõlas Euroopa Liidu seadustega. Kui Euroopa Liit pöörab üha suuremat tähelepanu elektroonilise side konfidentsiaalsusele, siis Eestis kavandatud seadusega oleks seda just piiranud. Olgugi et riikliku julgeoleku huvides on ka Euroopa Liidus lubatud internetiplattformide sisu talletamine, on tegemist erandliku meetmega, mis peab olema proportsionaalne. Radikaliseerumisele ja terrorismile ohutavad sõnumid ja veebisisu on üks keskne teemadering, mille puhul on Euroopa Liidu ja liikmesriikide sideteenuste kontekstis erandlikke meetmeid rakendatud, näiteks Radicalisation Awareness Networki (RAN) loomine Euroopa Liidus. RAN võrgustiku eesmärk on radikaliseerumisele viitavate ja terrorismi ohutavate sõnumite tuvastamine, vajalike spetsialistide koolitamine ning riikide vahel teadmiste ja infovahetus. Konkreetsetest ohtudest, nagu terrorism, lähtuvate meetmete rakendamine on aga erinev Eestis plaanitud nõudest, millega sooviti, et teenuse pakkuja talletaks kogu kasutuse. Viimast ei saa pidada proportsionaalseks nõudeks, vaid meetmeks, mis ohustaks sideteenuse kasutajate side konfidentsiaalsust.

Lisaks on oluline tähelepanu pöörata sellele, et nõue kasutusinformatsiooni talletada ei tähenda seda, et teenuse pakkuja kasutajate tegevusi ja vestlusi talletaks ja/või nende vestluste sisu hindaks ja edastaks vajaduse korral korrakaitseasutustele. Teenuse sisu jääb ka teenuse kasutamise talletamise nõude jõustudes puutumatuks. Pealegi ei ole mitmel teenusepakkujal, nagu WhatsApp või Signal, ligipääsu krüpteeritud tekstile. Nii ei ole ka kõnekaartide isikustamise kohustuslikuks muutmisel korrakaitseasutustel lihtsat ligipääsu sideteenuste, eriti internetiteenuste sisule – ligipääs tuleb saada seadusega kehtestatud viisil ja oma vahendeid, sh küberkriminalistikavahendeid kasutades. Küberkri-

minalistika abil internetirakenduse andmetele ligipääsemiseks on mõned väljatöötatud meetmed juba olemas ja neid arendatakse pidevalt.²⁰

2.2. SIM-KAARTIDE ISIKUSTAMINE JA UUED KURITEOLIIGID

Kuigi isikustamisega üritatakse organiseeritud kuritegevust ja terrorismi takistada, on uusi kuritegevuse vorme, mis võimaldavad kehtestatud reeglite eiramist. Toon siinkohal välja kolm kõige levinumat viisi, kuidas kõnekaartide isikustamisest on võimalik ebaseaduslikke meetodeid kasutades kõrvale hiilida.

Identiteedivargus ehk olukord, kus teenuse saamiseks kasutatakse teise inimese identiteeti. Kõige lihtsamad näited on laenatud, varastatud või võltsitud dokumentide esitamine enda isiku varjamise eesmärgil, kuid põhjalikum identiteedivargus hõlmab näiteks nii pangakontode kui ka kinnisvara omastamist. Olgugi et formaalselt on isikustamise reeglid maailmas ranged, sh kehtiva isikutunnistuse olemasolu nõue, tõi eelmine peatükk välja, et tihti on sideteenuse pakkuja valmis isikutunnistuse puudumisel piirduma pelgalt kolmanda isiku tunnistusega identiteedi õigsuse kohta. Lisaks, kuigi ükski riik ei nimeta ametlikult kehtivaks isikutunnistuseks originaali koopiasid, on empiiriliste kogemuste varal võimalik kinnitada, et tihti piisab oma isiku tõendamisest, eriti välisriigis viibides, kõigest dokumendi koopia esitamisest. Dokumentidele kehtivad toepeltstandardid soodustavad aga identiteedivargust veelgi. Vastavalt kehtestatud nõuetele isikustatakse kuritahtlikul eesmärgil kõnekaart siis kellegi teise nimele, kuid teenuseid tarbitakse ise.²¹ Seega viitavad kasutusandmed valele inimesele.²²

Näiteks on telefoniga maksmine rahvusvaheliselt üha levinum, kuid sellega kaasnevad ka kõrgendatud küberturberisk, näiteks Aafrikas laialdaselt levivad SIM-kaardi pettused, eriti SIM-kaartide vahetamine (ingl *SIM swap*).²³ SIM-i vahetamise juhtumeid on tuvastatud ka Euroopas (Tims, 2015) ja Ameerika Ühendriikides (Cranor, 2016). See tähendab, et teenusepakkuja veendakse vahetama teenusega seni seotud SIM mõne teise SIM-kaardi vastu ehk mõni teine kurjategijate käes olev SIM-kaart isikustatakse selle sama inimese nimel.²⁴ Suunates SMS-id uuele SIM-kaardile, on kelmidel võimalik hõlpsasti kuritarvitada kahetasemelist autentimist, kus isikutuvastus käib tekstisõnumi abil. Sel-line kahetasemeline autentimine on kasutusel nii finantstoimingute puhul, sotsiaalmeediakontode, meilikontode kui ka sõnumiteenuste (ingl *instant messages*) puhul. Tihti on

²⁰ Näiteks on WhatsAppi suhtlusteenuste puhul järelevalve olemasolul ja tavapäraseid küberkriminalistikavahendeid kasutades ligipääs suhtluse sisule võimalik, kuid seda ligipääsu ei anna mitte teenuse pakkuja (kellel seda kasutajalt kasutajale krüpteerimise tõttu ei ole), vaid see on võimalik läbi andmesalvestamise pilveteenusesse. Vt Angalo, 2014; Anwar & Supriyanto, 2019; Nada, *et al.* 2016; Onovakupri, 2018.

²¹ Siin on kindlasti Eesti kontekstis haavatavad toimetulekuraskustesse sattunud elanikud, kes võivad majandusliku kasu eesmärgil oma identiteeti müüa ehk oma isikutunnistust kasutades kolmandatele isikutele tasu eest kõnekaarte isikustada.

²² Rahvusvahelist statistikat selle kohta, kui suur osa kriminaalsete eesmärkidega sideteenuse kasutajaid kasutab SIM-kaardi omandamiseks valeidentiteeti või võltsitud dokumente, pole avalikustatud. Küll on viiteid sellele väiksemal skaalal. Näiteks on Indias Bangalore piirkonnas lausa 90% kurjategijate kasutatavatest SIM-kaartidest valenime alt ostetud (Mendonsa, 2016).

²³ South African Banking Risk Information Centre (SABRIC) esitatud SIM-kaardi pettuste statistika aasta 2017 ja 2018 võrdluses näitab märkimisväärtset intsidentide hulga suurenemist kahe aasta esimese kuue kuu lõikes nii veebiteenuste kasutamisel (44%), mobiilirakenduse kasutamisel (20%) kui ka SIM-kaartide vahetuse näol (104%) (The South African Banking Risk Information Centre, 2018).

²⁴ Selliste pettuste puhul on tegemist olnud ka kokkumänguga teenusepakkuja juures töötava inimese ja kriminaalse rühmituse vahel (PTI, 2015).

selline autentimine kasutusel ka telefonimaksete puhul.²⁵ 2017. aastal oli näiteks Sahara-taguses Aafrikas 135 mobiilset rahateenust ja 122 miljonit aktiivset kontot. SIM-vahe-tuse tõttu on hulk inimesi kaotanud raha kas otseste (ligipääs pangakontole) või kaudsete (näiteks WhatsAppi sõnumite kopeerimine ja kontaktidelt raha välja petmine) rünnakute kaudu (APOGroup, 2019; Robertson, 2013).

Teiseks levinud viisiks on isikustatud SIM-kaartidega telefonide vargus ja/või nendega hangeldamine.²⁶ Nagu teiste varastatud kaupade puhul, on ka isikustatud SIM-kaardid saanud musta turu toodete oluliseks osaks. Varastatud kaardid ja kaartidega seadmed, mis kellegi teise identiteeti kannavad, on kergesti kättesaadavad inimestele, kes soovivad mingil põhjusel oma identiteeti varjata.²⁷

Kolmandaks on levinud SIM-kaartide kopeerimine ehk kloonimine (Ansari, 2020). Kui kunagi peeti SIM-kaardi tehnoloogiat turvaliseks, siis nüüd on häkkerid leidnud viisi, kuidas kaarte lahti muukida (Olson, 2013). Kuigi sellest identiteedi varjamise meetmest pole laialdaselt juttu olnud, on võimalus nii füüsiliselt kui ka kaude SIM-kaarte kopee-rida. Viimase puhul on tegemist situatsiooniga, kus ühe telefoni sees olevast ja toimivast SIM-kaardist on samal ajal võimalik teha identne koopia ning seda paralleelselt originaa-liga kasutada. Ka sellisel juhul ei ole koopia kasutaja identiteet kusagile salvestatud ning teenuse kasutamise puhul viitavad andmed originaalse SIM-kaardi omanikule.

Kõigi kolme isikustamist eirava meetme puhul on SIM-kaardi kasutajatel võimalus oma isikut varjata. Kui esimesed kaks isikustamise nõude eiramise viisi on uus tahk juba toi-mivate illegaalsete ja kuritahtlike võrgustike meetoditest, siis viimane on seotud tehnoloogia arenguga ja vajab tuvastamiseks uut kompetentsi. Kõigi kolme olemasolu peab aga kõnekaartide isikustamise puhul arvesse võtma ja uute kuriteoliikidega arvestama. Nii võib juhtuda, et plaanitud lisavõimaluste tagamiseks, mida kõnekaartide isikustamisest loodetakse, toob süsteemi seaduslik toimimises hoidmine kaasa hoopis lisakulu nii ini-meste töömahu, väljaõppe kui ka vajaliku tehnika näol.

²⁵ Vt nt Rajendran, 2014.

²⁶ Kindlasti on selliste isikustatud seadmete edasimüügil oluline ära märkida tõik, et paljudes riikides, sh Eestis, ei sulgeta inimese surma korral tema telefoninumbrit automaatselt. Nii tekib võimalus juba isikustatud vahendeid edasi müüa.

²⁷ Lõuna-Aafrika Vabariigis tehtud katse näitas, et mitmed mobiilioperaatorid registreerivad oma SIM-kaardid vajalikku süsteemi suurtes kogustes korraga enne edasimüüjateni jõudmist. Nii ei ole ka edasimüüjatel tarvis kaarti eraldi süsteemi registreerida ja ostjate andmeid koguda ning SIM-kaardi ostjal ei ole vaja SIM-kaart osta spetsiaalselt isikustamiseks verifitseeritud edasimüüjalt. Ilma andmete kogumiseta ei ole aga hiljem võimalik politseil SIM-kaarti kasutanud inimese identiteeti tuvastada (MyBroadband, 2020).

3. SIM-KAARTIDE ISIKUSTAMINE EESTIS

Kõnekaartide isikustamist esitatakse Eestis, sarnaselt maailmas levinud argumentidele, võimalusena takistada tõhusamalt organiseeritud kuritegevust, seksuaalkuritegusid ja terrorismi tänu täpsematele jälgimisvõimalustele (või õigemini, suhtlusmuustrite ja võrgustike täpsemale tuvastamisele). Kuigi põhimõtteliselt on nii isikustamata kui ka isikustatud SIM-kaartide kasutajate sideteenuste kasutamine jälgitav, sest teenuse osutajatel on Eestis kohustus teenuse kasutamise andmeid koguda ja aasta jagu talletada, on nii telefonide riistvara arengu kui ka telefoniga kasutatavate teenuste ja rakenduste erineva olemuse tõttu teenuse kasutamise jälgimine nii praktiliselt kui ka juriidiliselt raskendatud.

Esimene oluline muutus, mis võib lubatud mõju vähendada, on üha kasvav rändlusteenuse kasutamine. Maailmas ühtset sideteenuste kasutamise hinnakirja veel kehtestatud ei ole ning maailmajaoti erineb teenuste hind, olemus ja kättesaadavus märkimisväärselt. Samuti on rändlusteenuse kasutamise võimalused riigiti erinevad. Samas on mitme sideteenusefirma puhul tegemist rahvusvahelise teenusepakkujaga, mistõttu laienevad nende firma klientidele mõeldud teenused ka teistesse riikidesse ja sealsetesse sidevõrkudesse.

Euroopas kehtestatud kõne- ja internetiteenuste rändlustasude ühtlustamine tähendab, et inimestel on sama SIM-kaarti kasutades eri Euroopa riikides sideteenuste kasutamine senisest soodsam ning nii on ka vajadus eri riikide teenuste tarbimiseks uus kõnekaart osta väiksem. Ühtlustatud tasud tähendavad, et Euroopa sideteenuse klientidel puudub ka reisides või kolides otsene vajadus kõnekaarti vahetada. Seega võib rändlusteenuse vahendusel riigi sideoperaatorite teenuseid kasutavate inimeste hulk kasvada. Nii võib rändlusteenuse kasutamisel uue seaduse plaanitud mõju pisendada.

Isegi kui Eestis muutub uute kõnekaartide ostmisel SIM-kaardi isikustamine kohustuslikuks, siis ei saa kuidagi piirata teisest riigist pärit kõnekaartide kasutamist. Rändlusteenuse ühtlustatud hinnakiri soodustab seda. Nii on isikustamise seadustamisel edaspidi Eestis põhjendatult võimalik teiste riikide isikustamata kõnekaarte kasutada – seda mitte pelgalt sooviga anonüümsust tagada, vaid ka inimlikust mugavusest telefoninumbrit mitte vahetada. Kas teisest riigist pärit isikustamata kõnekaart on kasutusel pelgalt mugavusest või kuritahtlikel kaalutlustel, ei ole aga ilma kasutusandmete analüüsita võimalik kindlaks määrata. Viimastele on ligipääs vaid juhul, kui korrakaitseasutustel on andmete jälgimiseks luba juba saadud.

Kui tegemist on rändlusteenusega, siis kasutab teenuse tarbija seade küll teenuse tagamiseks kohaliku võrgu tuge ehk kohalik võrk vahendab teenust, kuid kuna tegemist on kõigest vahendamisega, võib sideteenuse kasutamise andmetele ligipääs olla juriidiliselt kee-

rukam. Rändlusteenust kasutades korjatakse kliendi kasutusandmete talletamise puhul põhimõtteliselt teise riigi teenusepakkuja ja kliendi andmeid.

Kuigi rakendust kasutatakse telefonis, ei ole rakenduse kasutamiseks vaja sideoperaatori andmesideteenust kasutada. Avalikud wifivõrgud, näiteks kaubanduskeskustes või avalikus linnaruumis, pakuvad võimaluse kasutada rakendusi anonüümselt. Isegi kui internetirakenduse teenuse pakkujale panna kohustus jälgida suhtlus- ja kasutusandmeid, siis ilma andmesideteenust kasutamata ehk kindla SIM-kaardiga sidumata ei ole internetirakenduse kasutamise andmeid võimalik sama lihtsalt konkreetse isikuga siduda. Ilma seoseta aga ei ole teenuse pakkujal põhjust andmeid esitada.

Lisaks on paljudel nutitelefonidel võimalus oma andmesidevõrgu teenust kasutada telefon ka kaasaskantavaks internetiruuteriks muuta ehk kasutada *hotspot*-teenust. Sellisel juhul saavad ühe andmesideteenuse kaudu ligipääsu internetile teised seadmed. Ühest küljest on sellise vahendatud interneti puhul taas andmesideteenuse kasutuse eest vastutuse panemine keerulisem. Teisalt aga ei ole ka sellised andmesidevõrgud lõplikult turvalised ja on võimalus, et kasutatakse pahatahtlikult teise inimese andmesideteenust.

Viimaks on oluline välja tuua ka see, et kõnekaartide peamiseks kasutajaskonnaks on Eestis noored (Üürike, 2014, lk 21). Isikustamata kõnekaardi puhul ei tekkinud küsimust noorte, sh alaealiste suhtlusandmete kogumises ja talletamises, isikustatud SIM-kaardi puhul tuleb aga ka see läbi mõelda, kuidas noored kõnekaardi kasutajad teenuse isikustada saavad ja mis on nende vastutus sideteenuse kasutamisel, sh internetirakendusi kasutades. Aja jooksul on see küsimus üha aktuaalsemaks muutunud, sest mobiiltelefonide arenguga on telefoniside asendunud andmesidega ning internetiruumis toimuva eest, mis on hiljem tuvastatav, on kõigil kasutajatel vastutus eemaldatud. Kuidas internetitegevuse eest vastutust proportsionaalselt ka alaealistele asetada, vajab ühiskonnas laialdasemat arutelu.

Kuigi SIM-kaartide isikustamine võimaldab vastava loa olemasolul sideteenuse kasutustreid jälgida, on isikustamisel kitsaskohti, mille puhul pole ilma edasise analüüsita võimalik hinnata, kas plaanitav kasutegur on vastavuses juriidiliste muutuste ja praktiliste ümberkorraldustega, mida kõnekaartide isikustamise meede eeldab. Arvestades üha mitmekülgsemat andmesidekasutust, lihtsamini kättesaadavaid ja võimekamaid mobiiltelefone ja globaliseeruvat kasutajaskonda, on enne nõude kehtestamist vaja avalikku arutelu, mis toetuks meetmete hindamisel rahvusvahelistele parimatele praktikatele ning võtaks arvesse ka kohalikku eripära, et töötada välja Eesti jaoks jätkusuutlik ja rakendamiseks optimaalne lahendus.

KOKKUVÕTE

Tehnoloogia arengu tõttu on viimase kümmekonna aastaga sideteenuste kasutamine märkimisväärselt muutunud: telefoniteenusele on lisandunud andmesideteenus ning mobiiltelefoni kasutatakse üha enam internetirakenduste puhul ning vähem otsekontaktiks kõnede ja tekstisõnumitena. Mitmekesistunud suhtlusvõimalused on kaasa toonud organiseeritud kuritegevuse, terrorismi ja seksuaalkuritegevuse laienemise sellesse andmesideteenuste toetatud suhtlusruumi. Uute suhtlusvõimaluste pahatahtliku kasutamise tõkestamiseks otsitakse mooduseid rahvusvaheliselt ja ühe levinud meetmena sideteenuse kasutaja isiku tuvastamiseks on laialdaselt kasutusele võetud kõnekaartide isikustamise nõue.

Kuigi nõue sideteenuse pakkujatele kõikide kasutajate kohta infot koguda ja kasutust talletada on tõhus telefoniteenuse puhul kuritegelike organisatsioonide tuvastamiseks suhtemustrite alusel, on sarnane jälitustegevus andmesideteenuse vahendusel internetirakenduste kasutamise andmeid vaadeldes oluliselt keerulisem. Muutunud kommunikatsioonivorme silmas pidades on meede aegunud: isiku saab otseselt siduda telefoni-teenusega, aga internetikasutus on komplekssem. Pelgalt kõnekaardi isikustamine ei ava internetikasutuse sisu, vaid annab ainult infot andmeside tarbimise kohta. Suhtemustrite tuvastamine demokraatlikus riigis ja legaalse vahenditega sõltub internetirakenduse teenusepakkuja paindlikkusest alluda riigis kehtestatud reeglitele ning jagada infot korrakaitseasutustega. Selline andmeajamine on klientide konfidentsiaalsust ja lojaalsust tähtsustavatele teenusepakkujatele aga erandlik.

Internetirakenduste kasutusandmete raske kättesaadavus ja andmesideteenuste andmete vähese informatiivsuses tõttu ei vasta rahvusvaheliselt kõnekaartide isikustamise meetme põhjenduseks esitatud kasutegurid reaalsele tulemusele. Kuritegude arv ja tuvastamine pole nimelt märkimisväärselt kahanenud. Pigem on isikustamine iganenud süsteemi uuendus, mis ei saa oma ülesannet teenuse muutunud olemuse tõttu täita – tegemist ei ole innovatiivse lahendusega, mis hõlbustaks korrakaitse tööd, vaid meetmega, mis eeldab, et kuritegelike kavatsustega suhtlus pole kommunikatsioonitehnoloogia arengust hoolimata oma olemust muutnud. Kui demokraatlikke väärtusi tähtsustavates riikides ei ole isikustamise nõue olukorda märkimisväärselt muutnud, siis autoritaarsed riigid on saanud isikustatud kõnekaartide näol juurde meetme elanike ja välismaalaste tegevuse valvsaks jälgimiseks. Lisaks on riike, kus isikustamise nõue on ahendanud inimeste ligipääsu suhtlus- ja informatsiooni hankimise võimalustele ja süvendanud ühiskonnas valitsevat ebavõrdsust.

Arvestades selle meetme vähest kinnitatud tõhusust ja võimalikke kaasnevaid komplikatsioone, sh uut liiki kuritegevuse kasv, riigil lasuv kohustus aidata sideteenuse operaatoritel nõuetekohast teenust pakkuda ning võimalik sideteenusele ligipääsu raskendamine, on kõnekaardi isikustamist planeerides vaja hästi läbi mõelda, kas tulemus on pingu-

tusega kooskõlas. Ka kuritegude ennetamiseks ja menetlemiseks kasutatav meede peab olema proportsionaalne ja selle vajalikkus elanike põhjendatud: isegi suurandmete ajastul ei tohi inimeste põhiõigusi ebavajaliku isikustamisega riivata, sest siis kaob kergesti usaldus nii meetme kui ka seda rakendava riigi vastu. Tehnoloogilist arengut arvesse võttes võib andmeside ja internetirakenduste kasutusandmete uurimiseks korraldada eesmärgil olla sobivamaid lahendusi kui suuremahuline isikuandmete kogumine sideoperaatorite poolt. Arvestades muukimatutena esitatud SIM-kaartide turvariske, otsivad arendajad ebaturvalisele tehnoloogiale juba uut alternatiivi. Kui aga kulutada ressursse vananenud meetodi juurutamisele, võivad jääda märkamata olulised arengud, mis vajavad kiiret reageerimist ja paradigma muutust.

KASUTATUD ALLIKAD

- Amnesty International, 2011. 5 countries where your online comments could land you in jail. [Võrgumaterjal] Leitav: <https://www.amnestyusa.org/5-countries-where-your-online-comments-could-land-you-in-jail/> [Kasutatud: 11.01.2021].
- Angalo, C., 2014. Forensic analysis of WhatsApp Messenger on Android smartphones. *Digitla Investigation*, 11 (13), p. 201–213.
- Ansari, W., 2020. How To Clone SIM Card Under 15 Minutes. *Tech2Hack*, [Võrgumaterjal] Leitav: <https://www.tech2hack.com/how-to-clone-sim-card-easily/> [Kasutatud: 11.01.2021].
- Ansuar, N. & Supriyanto, M.T., 2019. Forensic Authentication of WhatsApp Messenger Using the Information Retrieval Approach. *International Journal of Cyber-Security and Digital Forensics*, 8(3), p. 206–212.
- APOGroup, 2019. SIM swap fraud: A New Wave of Attacks Targeting Financial Services and online services in Africa. *Africanews.com*, [Võrgumaterjal] Leitav: <https://www.africanews.com/2019/05/06/sim-swap-fraud-a-new-wave-of-attacks-targeting-financial-services-and-online-services-in-africa/> [Kasutatud: 11.01.2021].
- Beaucar Vlahos, K., 2019. Orwell Goes to China. Thanks to the social credit system and total surveillance there, 1984 is now. *The American Coservative*. July-August, pp. 21–25.
- Biscoff, P., 2020. Which governments impose SIM-card registration laws to collect data on their citizens? [Võrgumaterjal] Leitav: <https://www.comparitech.com/blog/vpn-privacy/sim-card-registration-laws/> [Kasutatud: 11.01.2021].
- Blank, G. & Dutton, W. H., 2014. Next Generation Users: A New Digital Divide. Rmt: M. Graham & W. H. Dutton, toim-d. *Society & the Internet. How Networks of Information and Communication are Changig Our Lives*. Oxford: Oxford Univeristy Press, p. 36–52.
- Cranor, L., 2016. Your mobile phone account could be hijacked by an identity thief. *Federal Trade Commission*, [Võrgumaterjal] Leitav: Your mobile phone account could be hijacked by an identity thief | Federal Trade Commission (ftc.gov) [Kasutatud: 15.01.2021].
- Dawn Media Group, 2021. Mobile company's worker held with fake SIM cards. *Dawn.com*, [Võrgumaterjal] Leitav: <https://www.dawn.com/news/1599919/mobile-companys-worker-held-with-fake-sim-cards> [Kasutatud: 15.01.2021].

- Donovan, K. & Martin, A., 2014. The Rise of African SIM Registration: The Emerging Dynamics of Regulatory Change. *First Monday*, 19, 2–3, [Võrgumaterjal] Leitav: <https://firstmonday.org/ojs/index.php/fm/article/view/4351/3820> [Kasutatud: 29.12.2020].
- EDRI. 2019. The sixth attempt to introduce mandatory SIM registration in Romania. [Võrgumaterjal] Leitav: <https://edri.org/our-work/the-sixth-attempt-to-introduce-mandatory-sim-registration-in-romania/> [Kasutatud: 11.01.2021].
- GSMA, 2013. *The Mandatory Registration of Prepaid SIM Card Users. A White Paper*. [Võrgumaterjal] Leitav: https://www.gsma.com/publicpolicy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf [Kasutatud: 26.11.2020].
- Jentzsch, N., 2012. *Implications of Mandatory Registration of Mobile Phone Users in Africa*. Discussion Paper of DIW Berlin 1192. DIW Berlin. German Institute for Economic Research. [Võrgumaterjal] Leitav: https://www.diw.de/documents/publikationen/73/diw_01.c.394079.de/dp1192.pdf [Kasutatud: 11.01.2021].
- Jentzsch, N., Preibusch, S. & Harasser, A., 2012. Study on monetising privacy. An economic model for pricing personal information. European Network and Information Security Agency (enisa). [Võrgumaterjal] Leitav: <https://www.enisa.europa.eu/publications/monetising-privacy> [Kasutatud: 11.01.2021].
- Jimenez Arandia, P., 2019. Spain gathers anonymised phone tracking data to shape public services., *Global Government Forum*. [Võrgumaterjal] Leitav: <https://www.globalgovernmentforum.com/spain-gathers-anonymised-phone-tracking-data-to-shape-public-services/> [Kasutatud: 11.01.2021].
- Kobie, N., 2019. The complicated truth about China's social credit system. *Wired*, [Võrgumaterjal] Leitav: <https://www.wired.co.uk/article/china-social-credit-system-explained> [Kasutatud: 26.11.2020].
- Kommusaar, V., 2020. Veiko Kommusaar: politsei vajab õigeid tööriistu. *Postimees*, [Võrgumaterjal] Leitav: <https://leht.postimees.ee/7099704/veiko-kommusaar-politsei-vajab-oigeid-tooriistu> [Kasutatud: 26.11.2020].
- Korpan, V., 2000. Siseminister tahab keelata kõnekaardid. Äripäev, [Võrgumaterjal] Leitav: <https://www.aripaev.ee/uudised/2000/06/18/siseminister-tahab-keelata-konekaardid> [Kasutatud: 26.11.2020].
- Korpan, V., 2002. Eestis jääb kõnekaardi kasutus Põhjalale alla. Äripäev, [Võrgumaterjal] Leitav: <https://www.aripaev.ee/uudised/2002/02/27/eestis-jaab-konekaardi-kasutus-pohjalale-alla> [Kasutatud: 26.11.2020].
- Markson, S., 2007. SIM card identity check to beat terrorists. The (Sydney) Sunday Telegraph. 22 juuli 2007. lk. 4.
- Mendonsa, K., 2016. Majority of criminals procure sim cards using fake ID proofs, *The Times of India*, [Võrgumaterjal] Leitav: http://timesofindia.indiatimes.com/articleshow/54373021.cms?utm_source=contentofinterest&utm_medium=-text&utm_campaign=cppst [Kasutatud: 11.01.2021].
- Mägi, K. A., 2020. Siseministeerium kinnitab: anonüümseid kõnekaarte ei keelata, sellist plaani pole ka teistel ministeeriumitel. *digigeenius*, [Võrgumaterjal]

- Leitav: <https://digi.geenius.ee/rubriik/uudis/siseministeerium-kinnitab-anonuumseid-konekaarte-ei-keelata-sellist-plaani-pole-ka-teistel-ministeeriumitel/> [Kasutatud: 04.12.2020].
- MyBroadband, 2020. Here is how easy it is to buy an illegal SIM in South Africa. [Võrgumaterjal] Leitav: <https://mybroadband.co.za/news/cellular/357547-here-is-how-easy-it-is-to-buy-an-illegal-sim-in-south-africa.html> [Kasutatud: 11.01.2021].
- Nada, I., Al Naqbi, N., Iqbal, F. & AldFadi, O., 2016. Foresing Investigation of SIM card. *CDFSL Proceedings*, p. 219–234.
- NPR, 2012. *Why Millions of Americans Have No Government ID*. [Võrgumaterjal] Leitav: <https://www.npr.org/2012/02/01/146204308/why-millions-of-americans-have-no-government-id?t=1605097144479&t=1610362698497> [Kasutatud: 11.01.2021].
- Olson, P., 2013. SIM Cards Have Finally Been Hacked, And The Flaw Could Affect Millions Of Phones. *Forbes.com*, [Võrgumaterjal] Leitav: <https://www.forbes.com/sites/parmyolson/2013/07/21/sim-cards-have-finally-been-hacked-and-the-flaw-could-affect-millions-of-phones/?sh=2fd66efa17b8> [Kasutatud: 11.01.2021].
- Omandi Gumba, D.E. & Wanyonyi, E., 2020. More questions than answers: Tanzania's mandatory SIM card registration. [Võrgumaterjal] Leitav: <https://issafrica.org/iss-today/more-questions-than-answers-tanzanias-mandatory-sim-card-registration> [Kasutatud: 11.01.2021].
- Onovakpuri, P. E., 2018. Forensics Analysis of Skype, Viber and WhatsApp Messenger on Android Platform. *International Journal of Cyber-Security and Digital Forensics*, 7(2), p. 119–131.
- Plüschke-Altof, B., Loewen, B. ja Leetmaa, K., 2019. Keskuse ja ääremaa lõhe Eestis. *Eesti inimarengu aruanne 2019/2020*. lk 44-55. Leitav: <https://inimareng.ee/print/EIA-2019-1.2.pdf> [Kasutatud: 11.01.2021].
- Poom, R., 2020. IT-minister Siem tõmbab nuhkimisele pidurit: Eesti inimeste vestlusi suhtlusäppides ei hakata talletama. *Eesti Päevaleht*, [Võrgumaterjal] Leitav: <https://epl.delfi.ee/uudised/it-minister-siem-tombab-nuhkimisele-pidurit-ees-ti-inimeste-vestlusi-suhtlusappides-ei-hakata-talletama?id=91855031> [Kasutatud: 04.12.2020].
- Prepaid Data SIM Card Wiki, 2020. *Registration Policies Per Country*. [Võrgumaterjal] Leitav: https://prepaid-data-sim-card.fandom.com/wiki/Registration_Policies_Per_Country#Europe [Kasutatud: 26.11.2020].
- Press Trust of India, 2014. BSNL issues 5,000 SIMs in flood hit Kashmir without ID proof. *Business Standard*, [Võrgumaterjal] Leitav: BSNL issues 5,000 SIMs in flood hit Kashmir without ID proof | Business Standard News (business-standard.com) [Kasutatud: 15.01.2021].
- Privacy International, 2019a. *101: SIM Card Registration*. [Võrgumaterjal] Leitav: <https://privacyinternational.org/explainer/2654/101-sim-card-registration> [Kasutatud: 29.12.2020].

- Privacy International, 2019b. *Timeline of SIM Card Registration Laws*. [Võrgumaterjal] Leitav: <https://privacyinternational.org/long-read/3018/timeline-sim-card-registration-laws> [Kasutatud: 29.12.2020].
- PTI, 2015. Two telecom managers among three held in SIM card racket. *ET Telecom.com*, [Võrgumaterjal] Leitav: Two telecom managers among three held in SIM card racket, Telecom News, ET Telecom (indiatimes.com) [Kasutatud: 15.01.2021].
- Rajendra, M., 2014. Security alert: Frauds can clone your SIM, use your credit card. *The Hindustan Times*, [Võrgumaterjal] Leitav: Security alert: Frauds can clone your SIM, use your credit card | Hindustan Times [Kasutatud: 15.01.2021].
- Reisenbuk, K., 2019. Mart Helmele jäi ette järjekordne ERRi ajakirjanik, AK astus kolleegi kaitseks välja, *Postimees*, [Võrgumaterjal] Leitav: <https://www.postimees.ee/6683722/mart-helmele-jai-ette-jarjekordne-erri-ajakirjanik-ak-as-tus-kolleegi-kaitseks-valja> [Kasutatud: 11.01.2021].
- Reporters Without Borders, 2020. Estonia. [Võrgumaterjal] Leitav: <https://rsf.org/en/estonia> [Kasutatud: 11.01.2021].
- Riigikontroll, 2020. Esmatähtsate avalike teenuste tulevik. Riigikontrolli aruanne Riigikogule. Tallinn. [Võrgumaterjal] Leitav: https://www.riigikontroll.ee/Portals/0/Upload/RVKS2020/RVKS_06.11.2020_TRYKKI_LOPP.pdf [Kasutatud: 11.01.2021].
- Robertson, J., 2013. SIM-Card Hackers' Phone Fraud Is Costing Mobile Carriers a Fortune. *Bloomberg*, [Võrgumaterjal] Leitav: <https://www.bloomberg.com/news/articles/2013-10-17/sim-card-hackers-phone-fraud-is-costing-mobile-carriers-a-fortune> [Kasutatud: 11.01.2021].
- Roosve, G.-L., 2020a. MKM tahaks turvakaalutlustel keelata isikustamata kõnekaardid. *ERR.ee*, [Võrgumaterjal] Leitav: <https://www.err.ee/1149441/mkm-tahaks-turvakaalutlustel-keelata-isikustamata-konekaardid> [Kasutatud: 13.01.2021].
- Roosve, G.-L., 2020b. Tupay: kõnekaartide keelustamine riivab õigusi, kuid pole õigusvastane. *ERR.ee*, [Võrgumaterjal] Leitav: <https://www.err.ee/1149581/tupay-konekaartide-keelustamine-riivab-oigusi-kuid-pole-oigusvastane> [Kasutatud: 13.01.2021].
- Sibold, G., 2018. Eestis on nüüd 200 000 Mobiil-ID kasutajat. *digigeenius*, [Võrgumaterjal] Leitav: <https://digi.geenius.ee/rubriik/uudis/eestis-on-nuud-200-000-mobiil-id-kasutajat/> [Kasutatud: 26.11.2020].
- Stankey, R., Frappier, D. & Guyton, B.W., 2010. *Prepaid registration: will US consumers be required to show photo ID when buying a cell phone?* [Võrgumaterjal] Leitav: <https://www.lexology.com/library/detail.aspx?g=16683847-6b51-4954-8a01-a2d91a3c2bde> [Kasutatud: 11.01.2021].
- Statista, 2020. *Number of mobile cellular subscriptions per 100 inhabitants in Myanmar from 2000 to 2019*. [Võrgumaterjal] Leitav: <https://www.statista.com/statistics/509591/mobile-cellular-subscriptions-per-100-inhabitants-in-myanmar/> [Kasutatud: 26.11.2020].

- Stella, D., 2005. *Antiterrorism measures*. [Võrgumaterjal] Leitav: <https://www.twobirds.com/en/news/articles/2005/antiterrorism-measures> [Kasutatud: 29.12.2020].
- Sumbwanyambe, M. & Nel, A., 2013. Assessing the implications of SIM card registration policy in the SADC region. *IST-Africa 2013 Conference Proceedings*, p.1-9.
- The South African Banking Risk Information Centre, 2018. *Digital banking crime statistics*. [Võrgumaterjal] Leitav: <https://sabric.co.za/media-and-news/press-releases/digital-banking-crime-statistics/> [Kasutatud: 11.01.2021].
- Tims, A., 2015. 'Sim swap' gives fraudsters access-all-areas via your mobile phone. *The Guardian*, [Võrgumaterjal] Leitav: 'Sim swap' gives fraudsters access-all-areas via your mobile phone | Scams | The Guardian [Kasutatud: 11.01.2021].
- Turk, K., 2020. Karmen Turk: andmete säilitamiskohustus ja anonüümsete kõnekaartide keelamine eeldab, et meie enda seadused on õiguspärased. *Eesti Päevaleht*, [Võrgumaterjal] Leitav: <https://epl.delfi.ee/arvamus/karmen-turk-andmete-sailitamiskohustus-ja-anonuumsete-konekaartide-keelamine-eeldab-et-meie-enda-seadused-on-oigusparased?id=91718213> [Kasutatud: 30.11.2020].
- UN LIEG Technical Secretariat, 2019. *United Nations Strategy for Legal Identity for All. Concept note developed by the United Nations Legal Identity Expert Group*. [Võrgumaterjal] Leitav: <https://unstats.un.org/legal-identity-agenda/documents/UN-Strategy-for-LIA.pdf> [Kasutatud: 11.01.2021].
- Vasquez, I. & McMahon, F., 2020. *The Human Freedom Index 2020. A Global Measurement of Personal, Civil, and Economic Freedom*. [Võrgumaterjal] Leitav: <https://www.cato.org/sites/cato.org/files/2020-12/human-freedom-index-2020.pdf> [Kasutatud: 4.12.2020].
- Äripäev Kinnisvarauudised, 2008. *EMT: kõnekaardid on populaarsust kaotamas*. [Võrgumaterjal] Leitav: <https://www.kinnisvarauudised.ee/uudised/2008/04/25/emt-konekaardid-on-populaarsust-kaotamas> [Kasutatud: 26.11.2020].
- Üürike, M.-L., 2014. *Kõnekaartide kasutusharjumused 9.-12. klasside õpilaste seas. Lõputöö*. Tallinn: Tallinna Tehnikaülikool.
- Xinhua, 2019. *News Analysis: Mobile money on spot as Kenya links service to terrorism funding*. [Võrgumaterjal] Leitav: http://www.xinhuanet.com/english/africa/2019-01/30/c_137787614.htm [Kasutatud: 11.01.2021].
- Yongo, E. & Theodorou, Y., 2020. *Access to Mobile Services and Proof of Identity 2020: The Undisputed Linkages*. [Võrgumaterjal] Leitav: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2020/03/Access_to_mobile_services_2020_Singles.pdf [Kasutatud: 04.12.2020].

EESTIS 2020. AASTAL KAVANDATUD KÕNEKAARTIDE ISIKUSTAMISE NÕUDE VALGUSES UURIB ANALÜÜS NÕUDE VÕIMALIKKU TÕHUSUST JA PROPORTSIONAALSUST.

Analüüs tutvustab kõnekaartide isikustamise nõudeid rahvusvahelises kontekstis, selgitab isikustamishõude keskseid argumente ja vastuargumente ning toob välja, mis on suhe SIM-kaardi isikustamise ootuste ja võimaluste vahel. Analüüs juhib tähelepanu, et nõue ei pruugi anda ajastul, kus sideteenuse pakkuja vahendab nii telefoni- kui ka andmesideteenust, täit ülevaadet kõnekaardi kasutaja suhtlusest. Samas võib see tuua riigile lisakohustusi ja muuta elanike ligipääsu teenusele keerulisemaks.

