Dan Bogdanov, Triin Siil

Infotehnoloogilised võimalused põhiõiguste kaitsel

1. Sissejuhatus

Eesti Vabariigi põhiseaduse II peatükk sätestab põhiõigused, vabadused ja kohustused. Peatükk on mahukas ning annab põhiseadusliku jõu nii Eesti kodanike kui ka Eestis viibivate välisriikidest pärit isikute õigustele. Nende õiguste kaitse eest hoolitsevad ühelt poolt riik ning teisalt õigustatud ja kohustatud isikud ise. Eesti Vabariik on loonud õiguskaitseorganid nagu politsei, mis tegelevad nii ennetustöö kui ka väär- ja kuritegude menetlusega. Samal ajal paigaldavad paljud Eesti kodanikud oma kodudele tehnilisi lahendusi (nt lukustusmehhanisme), mis aitavad tagada kodu ja omandi puutumatust.

Tehnoloogia on oma loomuselt neutraalne ja seda saab kasutada nii õiguste kaitsel kui ka piiramisel. Lukk aitab ühes kohas kaitsta vara ja teises kohas võib õigusvastaselt võtta vabaduse. Suurendava objektiiviga fotoaparaat võib aidata luua tõendusmaterjali õigusrikkumise menetluses, aga võib ka rikkuda eraelu puutumatust. Viimased kaks võivad juhtuda ka ühekorraga, kas või üheainsa fotojäädvustuse tegemisel.

Infotehnoloogia kiire areng 20. sajandi teisel poolel tõi senisest suurema tähelepanu alla eraelu kaitse. Varasemast efektiivsem digitaalsete andmete kogumise, salvestamise, edastamise ja töötlemise tehnoloogia tegi võimalikuks paljude inimeste kohta käivate andmete kiire kopeerimise ja analüüsi. Sai selgeks, et kui mingeid andmeid on kerge kopeerida õiguslikel alustel, on neid andmeid sama kerge kopeerida ka õigusvastaselt, levitades nii eraelu puudutavat teavet või rikkudes autori õigusi tema loomingule.

Matemaatika ning arvutitehnika edasise arengu käigus kiirenes ka kaitsemeetmete areng. Salakirjade kirjutamise kunst viidi arvu- ja keerukusteoreetilistele alustele, mis andis meile tänapäevase krüptoloogia ning võimaldab turvalist ja autentset andmesidet arvutite vahel. On aga tähelepanuväärne, et Colossus, maailma esimene programmeeritav digitaalne elektronarvuti, loodi Teise maailmasõja ajal sakslaste kasutatava Lorenzi šifri murdmiseks ja seega saladuste rikkumiseks.[*1]

Selles keskkonnas on kujunenud välja tänane Euroopa andmekaitse regulatsioon ning praktika. Oleme teadlikumad digitaalse teabega seotud riskidest ning selle mõjust isikuandmete töötlemisele, samas teadmised privaatsuskaitse tehnoloogiatest ning nende rakendamisest on alles lapsekingades. Samuti on era- ja avalikus sektoris veel vähe praktikat süsteemide talitluse kavandamisel nii, et töödeldav andmehulk oleks võimalikult väike ning kataks vaid eesmärgi saavutamiseks vajaliku.

Artikli 2. peatükis selgitame isikute eraelu puudutava massandmetöötluse kasu ja riske ning toome näiteid Eestis 2020. aastal viiruse SARS-CoV-2 leviku tõkestamiseks kavandatud süsteemidest. Kolmandas peatükis räägime isikuandmete töötlemise minimeerimisest ja selle keerukusest, tuginedes Eesti avaliku sektori rakendustele, ning 4. peatükis tutvustame privaatsuskaitse tehnoloogiaid ja nende kasutust Eestis. Viiendas peatükis kirjeldame juhtumianalüüsina Eestis viirusega SARS-CoV-2 nakatunute lähikontaktide tuvastamiseks loodud rakenduse Hoia arendust. Viimaks pakume välja, kuidas võiks Eesti riik ja erasektor jõuda privaatsuskaitse tehnoloogiaid rakendavate ning andmetöötlust vähendavate infosüsteemideni.

[1] B. Jack Copeland. Colossus: The Secrets of Bletchley Park's Codebreaking Computers. Oxford: Oxford University Press 2006.

2. Põhiõigused ja massandmetöötlus

Põhiseadus näeb ette olukordi, kus põhiõiguste riive on põhjendatud. Näiteks on võimalik seaduses sätestatud korras rahva tervise tagamiseks piirata inimeste vaba liikumist (PS § 34 lg 2) või töödelda eraelulist teavet (PS § 26 lg 2). Oluline on mõista, et mõned vabadused saab pärast riivet taastada, teisi aga mitte.

Liikumispiirangute täies mahus lõppemise järel on võimalik isikul jätkata liikumist ning tema vabadus on taastatud piirangutele eelnevaga võrdsele tasemele. Eraelu puudutava teabe kolmandatele isikutele kättesaadavaks tegemist ei saa aga tagasi võtta: need isikud ei saa käsu peale teavet unustada. Näiteks võib tervishoiutöötajal olla raske unustada mõne tuntud isiku terviseseisundi teavet, mis talle teatavaks on saanud.

Probleem säilib ka siis, kui teavet on sellises mahus, et seda meelde jätta ei ole võimalik – näiteks kui see puudutab märkimisväärset hulka rahvastikust. Selliste massandmete töötlemiseks peab kasutama infotehnoloogilisi vahendeid, mis artikli kirjutamise ajal levinud lahenduste puhul tähendab, et andmeid ei ole raske kopeerida ning kasutada ka otstarbeks, milleks neid algselt ei kogutud.

Sellest järeldub, et eraelu puutumatuse taastamine on, osaliselt tehnoloogilistel põhjustel, keerukam kui muude põhiõiguste taastamine. Sellest lähtudes peame eraelu puutumatuse riivega ka ettevaatlikumad olema. Me võime usaldada neid, kellele täna riive raames massandmeid jagame. Aga kui meil pole kontrolli andmete tulevase töötlemise üle või me pole kindlad, et andmed kaotavad tulevikus oma aktuaalsuse, ei saa me ka tagada, et ühel otstarbel eraellu tungimine ei vii tulevikus uute riiveteni, kui samu andmeid kasutatakse mõnel ette nägemata moel.

2019. aastal aktiivsemalt levima hakanud koroonaviiruste perekonda kuuluv SARS-CoV-2 on nii Eestis kui ka mujal maailmas põhjustanud tõsiseid tervisekahjustusi. Eesti Vabariigis kehtestati viiruse leviku tõttu eriolukord, mis tõi kaasa mitmeid piiranguid, sealhulgas vaba liikumise piirangud.[*2] Viiruse leviku tõkestamiseks või selle paremaks mõistmiseks pakuti välja mitu laialdast andmetöötlust nõudvat lahendust. Näiteks tehti ettepanek analüüsida, kus nakatunud elavad, millisesse demograafilisse gruppi nad kuuluvad ning kus nad on liikunud.[*3] Andmete avaldamisega viivitamist nimetasid teadlased ka mänguks inimeludega ning põhjendasid jõulist retoorikat vajadusega kiiresti andmeid analüüsida ja õigel ajal otsuseid teha.[*4] Kaaluti ettepanekut jälgida karantiini jääjate mobiiltelefoni asukohta.[*5]

Rohkem tähelepanu sai valitsuse kriisikomisjoni korraldus Eesti Statistikaametile hinnata mobiiltelefonide asukohaandmete põhjal populatsiooni üldist liikumist, mille abil oleks Eesti Vabariigi valitsusel võimalik hinnata piirangute toimimist.[*6] „Ei viida läbi jälitustegevusega, tegemist ei ole isikustatud andmetega. Need on anonümiseeritud andmed. Eesmärk on anda pilt Eestis toimuvast liikumisest. Suuresti see töö toimub operaatorite majades, et tagada täielik anonüümsus. See ei ole reaalaja andmestik, see on võrdlus enne eriolukorda ja pärast," kirjeldas Eesti Rahvusringhäälingule töötlust Eesti Statistikaameti peadirektor Mart Mägi.[*7] Eraelu kaitse seisukohalt on väga tervitatav, et kirjeldatud analüüs korraldati lõpuks nii, et võimalikult suure osa andmetöötlusest tegid ära Eesti Vabariigi mobiilsideoperaatorid ning Statistikaametile liikusid vaid eeltöötluse tulemused, mida siis koondati ning asetati kaardile koostöös andmeteadlastega ettevõttest Positium.[*8] Tegemist oli kiiduväärt näitega andmetöötluse vähendamisest

---

2 P. K. Tupay. Riigivõimu otsused koroonaviiruse ohjeldamiseks: kas garantiikiri Eesti riigi püsimiseks või demokraatia lõpp? – Juridica 2020/3, lk 163–179.

3 M. Laine, H. Roonemaa, O. Kund. Teadlased ja eksperdid ei saa koroonakriisis riiki aidata: meile ei anta andmeid. – Eesti Päevaleht, 17.03.2020. Arvutivõrgus: https://epl.delfi.ee/uudised/teadlased-ja-eksperdid-ei-saa-koroonakriisis-riiki-aidata-meile-ei-anta-andmeid?id=89249689 (23.07.2020).

4 Postimehe ja akadeemikute nõukoda: andmetega viivitamine on mäng inimeludega. – Postimees, 01.04.2020. Arvutivõrgus: https://heureka.postimees.ee/6939107/postimehe-ja-akadeemikute-noukoda-andmetega-viivitamine-on-mang-inimeludega (23.07.2020).

5 R. Liive. Minister Karu: me ei soovi saavutada politseiriiki, kus paljude inimeste detailset liikumist jälgitakse. – Digigeenius, 19.03.2020. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/minister-karu-me-ei-soovi-saavutada-politseiriiki-kus-paljude-inimeste-detailset-liikumist-jalgitakse/ (23.07.2020).

6 Statistikaamet hakkab viiruse leviku piiramiseks inimeste liikumist jälgima. – ERR uudised, 24.03.2020. Arvutivõrgus: https://www.err.ee/1068185/statistikaamet-hakkab-viiruse-leviku-piiramiseks-inimeste-liikumist-jalgima (23.07.2020).

7 Statistikaamet loodab inimeste liikuvusanalüüsi valmis saada järgmisel nädalal. – ERR uudised, 27.03.2020. Arvutivõrgus: https://www.err.ee/1069748/statistikaamet-loodab-inimeste-liikuvusanaluusi-valmis-saada-jargmisel-nadalal (23.07.2020).

8 K. Aarma. Amet: liikumisandmed aitavad otsustada, kuidas ja millal piiranguid leevendada. – ERR uudised, 31.03.2020. Arvutivõrgus: https://www.err.ee/1071067/amet-liikumisandmed-aitavad-otsustada-kuidas-ja-millal-piiranguid-leevendada (23.07.2020).

ning hajutatud analüüsist, mis vältis tsentraalse andmebaasi loomist, kuid andis valitsuse kriisikomisjonile kasulikku teavet eriolukorra juhtimisel.[*9]

3. Massandmete töötluse minimeerimise keerukus

Tihti kutsutakse meedias andmepõhiseid teenuseid kirjeldades andmeid anonüümseteks. Heaks näiteks on eelmise peatüki lõpus toodud tsitaat mobiiltelefonide asukohaandmete kohta. Erinevus tuleneb sellest, et andmeteaduses ja andmekaitseõiguses on „anonüümimise" terminil erinev tähendus. Andmeteaduse mõistes tähendab andmestiku anonüümimine selle teisendamist nii, et sealt isiku tuvastamine on keerukam. Samas on tihti võimalik nii töödeldud andmestikust isikut tuvastada keerukate andmeteaduse meetoditega või seda mõne teise kättesaadava andmestikuga sidudes.

Juriidiliselt saab anonüümimist defineerida Euroopa Liidu isikuandmete kaitse üldmääruse[*10] põhjenduspunktist 26 tuletatud lihtsustatud selgituse järgi. Selle sõnastuses tähendab anonüümimine andmestiku muutmist nii, et sellest ei ole võimalik mõistlike pingutustega tuvastada ühtegi isikut.

Seega, kui keegi väidab, et andmed on anonüümsed, tuleb küsida, et kelle jaoks ja milline on see vähim pingutus, millega saaks andmestikust kedagi tuvastada. Kui leidub isik, kes suudab andmestikust analüütilist meetodit või lisaandmestikku kasutades mõistliku pingutusega kas või ühe isiku tuvastada, siis võis andmestik olla anonüümimismeetodiga töödeldud, kuid mitte õiguslikult anonüümne.

Näitena, inimeste liikumisandmete anonüümimine on ääretult keerukas. 2013. aastal avaldatud pooleteise miljoni inimese mobiiltelefonide 15 kuu liikumisandmestiku põhjal tehtud teadusuuring näitas, et 95% isikutest on võimalik unikaalselt eristada nelja ruumipunkti abil.[*11] Sellest lähtudes peame arvestama riskiga, et asukohaandmete andmebaasi anonüümimiseks ei piisa vaid isikustatud kirjete (nt kasutaja isikukood, telefoninumber, telefoni IMEI-kood) eemaldamisest. Nii töödeldud andmeid peaks ennekõike nimetama pseudonüümseks (ehk isikustatavaks „võtit" omavale isikule), sest Montjoye jt kohaselt[*12] ei ole isikuil sellistes andmestikes anonüümsust, vaid nad on selgesti eristatavad. Kui konkreetse andmestiku põhjal ei õnnestu pseudonüümset kirjet taasisikustada, siis seda saab teha suure tõenäosusega lisateabe, näiteks elukoha ja töökoha andmete lisamisel.

Massandmete töötlusel põhinevaid suuri süsteeme on Eesti Vabariigis kavandatud ka väljaspool kriisiolukordi. Isikuandmete laialdane töötlemine on olnud kavas näiteks e-majutuskaardi loomise algatuses. Majutuskaartidel olevat teavet on Eestis seni kogutud paberkujul. Üldjuhul seda ei teisendata ühtsele elektroonilisele kujule ning ei laadita ühtsesse kesksesse süsteemi. 2019. aastal jõudis testimisse riiklik e-majutuskaardi lahendus. „Iseenesest on plaanis teha selline andmetöötlus, et see on automatiseeritud ja inimeste nimesid tuvastatud kujul ei liigu. Andmed anonümatiseeritakse, ainult tabamuse saanud registreerunud jõuavad politsei töölauale, kui tegu on tagaotsitava inimesega. Sellist asja ei saa olla, et tekib ülevaade, millises hotellis ja kellega me käime, selliseid päringuid ei saa ega tohi sealt teha," ütles Majandus- ja Kommunikatsiooniministeeriumi kaubanduse ja teenuste talituse nõunik Kati Kikas seda algatust kommenteerides.[*13] Kirjelduse järgi edastataks majutuskaardid riigile, kellel tekiks sellest andmekogu, mida oleks võimalik ühendada tagaotsitavate loeteluga ning leida kattuvused, mille põhjal oleks võimalik algatada õiguskaitsetoiminguid. Samas oleks sellise andmekoguga võimalik teha ka teisi tegevusi, mis ei oleks tingimata seotud enam õiguskaitsega. Näiteks oleks andmestikust tehniliselt võimalik tuvastada inimeste omavahelisi isiklikke kontakte, mis võib viia laialdase eraelu riiveni.

Ei ole kahtlust, et sellist süsteemi ehitades juurutataks nii organisatoorseid kui ka tehnilisi infoturbemeetmeid, mis kahandavad mitte-eesmärgipärase andmetöötluse tõenäosust. Samas peaksime alati

9 Statistikaameti andmetel püsivad inimesed rohkem kodus. – ERR uudised, 09.04.2020. Arvutivõrgus: https://www.err.ee/1075441/statistikaameti-andmetel-pusivad-inimesed-rohkem-kodus (23.07.2020).

10 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), põhjenduspunkt 26. – ELT L 119, 04.05.2016, lk 1–88.

11 Y. de Montjoye, C. Hidalgo, M. Verleysen et al. Unique in the Crowd: The privacy bounds of human mobility. – Scientific Reports 2013/3, article No 1376. Arvutivõrgus: https://doi.org/10.1038/srep01376.

12 Samas.

13 R. Liive. Testimisse jõuab riiklik e-majutuskaart, mis informeerib politseid tagaotsitavatest. – Digigeenius, 29.10.2019. Arvutivõrgus: https://digi.geenius.ee/rubriik/uudis/testimisse-jouab-riiklik-e-majutuskaart-mis-informeerib-politseid-tagaotsitavatest/ (24.07.2020).

mõtlema, kas on veel mingeid võimalusi vaikimisi privaatse (lõimprivaatse) infosüsteemi ehitamiseks, nagu nõuab isikuandmete kaitse üldmääruse artikli 25 lõige 2.*[14] Majutatute nimekirja võrdlus tagaotsitavate nimekirjaga on tavatehnoloogiaid kasutades lihtne toiming ning selle negatiivseid mõjusid privaatsusele ei saa vähendada. Võrdluse enda turvalisemaks teostamiseks saame abi otsida privaatsuskaitse tehnoloogiatest.

4. Privaatsuskaitse tehnoloogiad

Privaatsuskaitse tehnoloogiad on info- ja sidetehnoloogilised lahendused, mis väldivad või vähendavad infosüsteemis isikut tuvastava teabe töötlemist nii, et süsteem säilitab oma võimed. Siin saab tõmmata paralleeli keskkonnahoiuga ning öelda, et privaatsuskaitse tehnoloogiatega ehitatud süsteem käib isikuandmetega säästlikumalt ringi ja töötleb neid väiksemas mahus kui süsteem, mis privaatsuskaitse tehnoloogiaid ei rakenda.

Privaatsuskaitse tehnoloogiaid saame klassifitseerida selle järgi, millistes toimingutes nad andmete isikustamist takistavad. Esimese grupi moodustavad sides kasutatavad privaatsuskaitse tehnoloogiad, mis takistavad üle sidevõrgu suhtlevate isikute tuvastamist või isegi raskendavad sideakti enese tuvastamist. Selliseid privaatsuskaitse tehnoloogiaid kasutatakse näiteks pealtkuulamise ja tsensuuri vältimiseks, aga ka delikaatsete teemade aruteluks.

Teise grupi moodustavad isiku tuvastamise käigus kasutatavad privaatsuskaitse tehnoloogiad, mis vähendavad seda teabe hulka, mis tuvastamise käigus avaldatakse. Näiteks mõnes müügikohas kasutatakse elektroonilist isikutunnistust, mis asub füüsilisel andmekandjal, s.o kiibiga varustatud plastikkaardil: kui viibata kaarti sobiva lugeva seadme juures, saaks süsteem teada vaid seda, et oleme täisealised, aga mitte meie nime või sünnikuupäeva.

Kolmandasse gruppi kuuluvad andmetöötluses rakendatavad privaatsuskaitse tehnoloogiad, mis vähendavad isikuandmete leket kõikvõimaliku andmeanalüüsi käigus, kus kasutatakse näiteks statistika või masinõppe meetodeid. Sellised privaatsuskaitse tehnoloogiad aitaksid privaatsemalt lahendada siin artiklis näidetena kirjeldatud ülesandeid, kus uuritakse inimeste liikumise mustreid või kuulumist tagaotsitavate nimekirja. Privaatsuskaitse tehnoloogiate abil saaks vältida nendes süsteemides isikute tuvastamist juhtudel, kus talitluse reeglid seda ette ei näe.

Privaatsuskaitse tehnoloogiatega saab infosüsteemides isikuandmete töötlemist vähendada, kuid see peab käima käsikäes süsteemi talitluse muutmisega. Ilma selleta oleks võimalik privaatsuskaitse tehnoloogiaid kasutada näiteks nii, et see kaitseb isikuandmeid töötlemise ajal perfektselt, kuid seejärel avalikustab tulemused kõigile. Parima kaitse saavutame, kui analüüsime kõigepealt isikuandmeid töötleva süsteemi talitlust ning leiame üles kõik kohad, kus esineb risk andmete lekkeks. Seejärel saame otsustada, kas muudame süsteemi talitlust, et kasutataks vähem andmeid, või kasutame privaatsuskaitse tehnoloogiaid, et töötlust paremini kaitsta. Selleks on välja töötatud ka tarkvaratehnilisi metoodikaid, näiteks *Privacy-Enhanced Business Process Modelling Notation* (PE-BPMN).*[15]

Privaatsuskaitse tehnoloogiatel on kõigil ka jääkrisk ehk tõenäosus, et sellega kaitstud andmeid saab siiski isikustada. Näiteks eespool kirjeldatud mobiiltelefonide asukohaandmete pseudonüümimise rakendamisel suudaks andmeteadlane ilmselt andmestikust leida iseenda ning eristada end teistest andmestikus olevatest isikutest. Mõne teise privaatsuskaitse tehnoloogia (nt turvalise arvutamise) rakendamisel poleks see võimalik, kuid sellisel juhul tuleks arvestada tehnoloogia muude nõrkustega (nt turvalise arvutamise puhul võib töötluse paindlikkus väheneda).

Privaatsuskaitse tehnoloogiate rakendamisel tuleb hinnata, kas süsteemi tegelikus juurutuses on tehniliste ja organisatoorsete kaitsemeetmete kombinatsioon andmete kaitseks piisav. Kui andmed on ühe süsteemi osalise jaoks mitteisikustatud, ei tarvitse nad seda olla teise jaoks.

14 Isikuandmete kaitse üldmääruse art 25.

15 P. Pullonen. R. Matulevičius, D. Bogdanov. PE-BPMN: Privacy-Enhanced Business Process Model and Notation. – Business Process Management. Lecture Notes in Computer Science 10445. J. Carmona, G. Engels, A. Kumar (eds.). BPM 2017.

5. Juhtumianalüüs: lähikontaktsete tuvastamine

Nakkushaiguste leviku tõkestamisel on lähikontaktide tuvastamine tavapärane praktika. Selle käigus küsitakse positiivse diagnoosiga isiku käest, kellega ta on hiljuti kokku puutunud. Seejärel teavitatakse lähikontaktis olnuid ning antakse neile haiguse iseloomust lähtudes nõu. Näiteks SARS-CoV-2 puhul on põhjendatud vabatahtlik eneseisolatsioon.

„Käsitsi" lähikontaktide tuvastamise peamine nõrkus on inimeste mälu ning teadmatus sellest, kellega nad avalikes kohtades kokku puutunud on. Viiruse laia leviku tõttu on otsitud tehnoloogilisi võimalusi, mis muudaksid tuvastamist efektiivsemaks. On tehtud ettepanekuid nii eriotstarbeliste käevõrude[*16] kui ka mobiiltelefonide kasutamiseks. Põhjusel, et nutitelefonidel on sobiv tehniline võimekus ning need on ühiskonnas levinud, valisid mitmed riigid[*17], sealhulgas Eesti[*18], nutitelefonil põhineva lahenduse.

Kuidas teha selgeks, et kaks nutitelefoni kasutajat on olnud omavahel kontaktis, mis võis viia viiruse levikuni inimeselt inimesele? Selleks tuvastatakse, kas telefonid, mida omanikud eeldatavasti kaasas kannavad, on olnud mingi aja (nt 10 minuti) jooksul teineteise läheduses. Selleks ei saa kasutada mobiiltelefonide asukohaandmeid operaatorite poolt mõõdetuna, sest need on liiga ebatäpsed.

Enamlevinud nutitelefonides saab lähikontaktide tuvastamiseks kasutada positsioneerimisteenust (GPS) või näiteks Bluetooth Low Energy raadiosignaale, mille abil mõõta telefonide kaugust signaalide tugevuse järgi.[*19] Kui võrdleme nende kahe meetodi põhjustatud võimalikku perekonna- ja eraelu puutumatuse põhiõiguse riivet, siis näeme, et iga kasutaja positsioneerimine töötleks rohkem isikuandmeid kui telefonide vahel raadiosignaalide vahetamine. Esimesel juhul töödeldaks kõigi kasutajate asukohainfot igal ajahetkel, teisel juhul vaid seda, millised muud nutitelefonid on olnud selle telefoni läheduses. Ehk siis täieliku asukohainfo töötlemise (mis on võrreldav jälitustegevusega) asemel töödeldaks suhtlusvõrgu infot. Seega antud juhul oleks teine meetod – Bluetooth Low Energy raadiosignaalide vahetamine – privaatsem ja seega eelistatum valikuvariant.

Järgmine küsimus on, kuidas seda teavet töödelda: kas tsentraalselt või hajutatult? Tsentraalse töötlemise puhul luuakse üks teenusepakkuja, kes teab, kes kellega pidevalt suhtleb. Alternatiiviks on hajus lahendus, kus telefonid teevad võimalikult suure osa töötlusest ise ning keskset osalist kasutatakse vaid selleks, et teavitada isikut võimalikust lähikontaktist haigega. Samas on soovitav, et ka telefonides ei töödeldaks teiste telefonide andmeid kergesti isikustataval kujul, sest seeläbi on võimalik ennetada diskrimineerimist terviseandmete põhjal (nakatunu või selle kahtlusega isiku kohta info lekkimise korral võidakse teda taga kiusata).

Selline ülesandepüstitus näib vastuoluline: kuidas on võimalik, et ei ole keskset osalist, mis töötleks isikustatud andmeid ning ka nutitelefonid ise seda ei tee? Selliste ülesannete lahendamine on võimalik, kui privaatsuskaitse tehnoloogiaid osavalt kombineerida. Teadlased pakkusid välja mitmeid erinevaid skeeme, millest üheks tuntumaks sai *Distributed Privacy-Preserving Proximity Tracing* ehk lühendatult DP-3T.[*20] Selle väljatöötajate seas on mitu tunnustatud krüptograafi ning privaatsuskaitse tehnoloogi. Kui kaks suurimat nutitelefonide tarkvara tootjat Apple ja Google otsustasid oma telefonide operatsioonisüsteemidesse (vastavalt iOS ja Android) ehitada sisse lähikontaktide tuvastamist toetavad funktsioonid, siis ehitati need just DP-3T baasil.[*21]

Singapuri TraceTogether oli üks esimestest lähikontaktsete tuvastamise rakendustest.[*22] Rakendus kasutas Bluetooth Low Energy raadiosignaale, kuid võimaldas siiski kesksel teenusepakkujal tuvastada,

16 Coronavirus: People-tracking wristbands tested to enforce lockdown. – BBC News, 24.04.2020. Arvutivõrgus: https://www.bbc.com/news/technology-52409893 (13.08.2020).

17 A. Holmes. Singapore is using a high-tech surveillance app to track the coronavirus, keeping schools and businesses open. Here's how it works. – Business Insider, 23.03.2020. Arvutivõrgus: https://www.businessinsider.com/singapore-coronavirus-app-tracking-testing-no-shutdown-how-it-works-2020-3 (13.08.2020).

18 M. Hindre. Riik loob koroonakontaktsete tuvastamise mobiilirakendust. – ERR uudised, 13.04.2020. Arvutivõrgus: https://www.err.ee/1076792/riik-loob-koroonakontaktsete-tuvastamise-mobiilirakendust (13.08.2020).

19 L. Ferretti, C. Wymant, M. Kendall, L. Zhao, A. Nurtay, L. Abeler-Dörner, M. Parker, D. Bonsall, C. Fraser. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. – Science, 08.05.2020, Vol. 368, No. 6491.

20 DP-3T – Decentralized Privacy-Preserving Proximity Tracing. GitHub. Arvutivõrgus: https://dp-3t.github.io (13.08.2020).

21 D. Etherington, N. Lomas. Apple and Google update joint coronavirus tracing tech to improve user privacy and developer flexibility. – TechCrunch, 24.04.2020. Arvutivõrgus: https://techcrunch.com/2020/04/24/apple-and-google-update-joint-coronavirus-tracing-tech-to-improve-user-privacy-and-developer-flexibility (13.08.2020).

22 TraceTogether. A Singapore Government Agency Website. Arvutivõrgus: https://www.tracetogether.gov.sg (13.08.2020).

kes on kellega kontaktis olnud. Sellise kontaktivõrgu kogumine aitab kindlasti teha epidemioloogilist statistikat, kuid võimaldaks näiteks jõustruktuuridel teha ka mitmeid teisi analüüse, mis ei ole rahva tervisega seotud. Ehk siis: pandeemia ajal loodud taristut on pärast pandeemia loodetavat lõppu võimalik kasutada ka muul otstarbel ja seega tuleb küsida, kas sellise taristu ehitamine on mõistlik.

Norra kasutas oma rakenduse ehitamiseks globaalseid positsioneerimisandmeid ning võimaldas need koguda kesksesse serverisse. Amnesty International hindas Norra rakenduse koos Bahreini ja Kuveidi omaga kõige rohkem privaatsust riivavaks.[*23] Norra andmekaitse lõpuks keelas rakenduse kasutamise ja nõudis andmete kustutamist.[*24]

Eesti lähikontaktsete tuvastamise rakenduse Hoia arendus algas aprillis 2020. Eesti Majandus- ja Kommunikatsiooniministeeriumi, Sotsiaalministeeriumi ja infotehnoloogiaettevõtjate kohtumisel 9. aprillil 2020 esitles artikli üks autoritest DP-3T-protokolli kui privaatsust säilitavat lahendust, mille abil lähikontaktsete tuvastamist korraldada. Sotsiaalministeeriumi koordineerimisel leiti ettevõtjad, kes olid nõus tasuta panustama Eesti rakenduse arendusse ning selle riigile üle andma. Sõlmiti vastastikuse mõistmise memorandum ning töö algas. Sotsiaalministeerium tegi Eesti lähikontaktsete tuvastamise rakenduse nimega Hoia avalikkusele kättesaadavaks 20. augustil 2020.[*25]

6. Kuidas jõuda eraelu kaitsvate infosüsteemide ajastusse?

Isikuandmeid sisaldavate massandmete töötlusele lisab keerukust vajadus tagada selle õiguspärasus. Seejuures mängivad üha kasvavat rolli tehnoloogilised vahendid. 25. mail 2018 jõustunud isikuandmete kaitse üldmääruse artikliga 25[*26] kehtestati Euroopa Liidu andmekaitseõiguses vastutavatele töötlejatele sõnaselgelt lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete järgimise kohustus. Neid norme peetakse liidu andmekaitsereformi ühtedeks innovatiivseimateks ja ambitsioonikaimateks sammudeks – tegemist on sisuliselt infosüsteemide arendusele mõeldud nõuetega, mis sunnivad arvestama privaatsusega seotud huve läbi kogu arendusprotsessi. Kui andmekaitsepõhimõtted on IT-süsteemidesse sisse ehitatud, peaks vastavad tehnilised meetmed suunama isikuid andmekaitseõigusega rohkem kooskõlas käitumisele kui pelk õigusaktide kehtestamine või lepingute sõlmimine.[*27]

Üldmääruse artiklist 25 tulenevad lõimitud ja vaikimisi andmekaitse kohustused laienevad automaatselt ka eelmistes peatükkides kirjeldatud juhtumitele, kus on arendatud erinevaid isikuandmete masstöötluse lahendusi. Avalikkuseni pole jõudnud täpsemat infot, kuidas neid põhimõtteid on konkreetse lahenduse puhul rakendatud. Üksikisiku tasandil tuleb info isikuandmeid töötlevate rakenduste kasutamise kohta edastada andmesubjektile üldmääruse artiklites 12–14 sätestatud teavitamiskohustuste raames, v.a kui töödeldakse anonüümseid andmeid (sellisel juhul üldmäärus ei kohaldu, sest töötluse käigus isikuid ei tuvastata)[*28] või kui andmesubjekti tuvastamine vastutava töötleja poolt ei ole töötlemise eesmärkide jaoks (enam) nõutav.[*29] Võib eeldada, et viimati kirjeldatud olukorraga oli tegemist Eesti Statistikaameti poolt mobiiltelefonide asukohaandmete põhjal populatsiooni üldise liikumise hindamiseks loodud rakenduse, e-majutuskaartide lahenduse ja ka Eesti lähikontaktsete tuvastamise rakenduse Hoia puhul. Neist

23 Bahrain, Kuwait and Norway contact tracing apps among most dangerous for privacy. Amnesty International, 16.06.2020. Arvutivõrgus: https://www.amnesty.org/en/latest/news/2020/06/bahrain-kuwait-norway-contact-tracing-apps-danger-for-privacy/ (13.08.2020).

24 L. Kelion. Coronavirus: Contact-tracing apps face further hitches. – BBC News, 15.06.2020. Arvutivõrgus: https://www.bbc.co.uk/news/technology-53051783 (13.08.2020).

25 Hoia ennast ja oma lähedasi. Terviseamet. Arvutivõrgus: https://hoia.me (13.08.2020).

26 Samasugune kohustus on kehtestatud ka politseile ja kriminaaluurimisasutustele suunatud isikuandmete kaitse ja õiguskaitse direktiivi art-s 20. Vt Euroopa Parlamendi ja nõukogu direktiiv (EL) 2016/680, 27. aprill 2016, mis käsitleb füüsiliste isikute kaitset seoses pädevates asutustes isikuandmete töötlemisega süütegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise või kriminaalkaristuste täitmisele pööramise eesmärgil ning selliste andmete vaba liikumist ning millega tunnistatakse kehtetuks nõukogu raamotsus 2008/977/JSK. – ELT L 119, 04.05.2016, p 89–131.

27 L. A. Bygrave. Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. – Oslo Law Review 2017 (4) 2, p 1. Arvutivõrgus: https://www.idunn.no/oslo_law_review/2017/02/data_protection_by_design_and_by_default_deciphering_the_#xfn_15 (16.08.2020).

28 Isikuandmete kaitse üldmääruse põhjenduspunkt 26.

29 Isikuandmete kaitse üldmääruse art 11 ja art 12 lg 2.

ühelgi juhul ei ole avalikkusele teadaolevalt tehtud üldmääruse artiklis 32 nõutud andmekaitsealast mõjuhinnangut ega täpsemalt kirjeldatud üldmääruse artiklis 25 nõutud lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete rakendamise viise. Küsimus on, kas me ühiskonnana tahame, et selline info jõuaks avalikkuse ette?

Üldmääruse kohaselt ei pea isikuandmete töötlemise IT-lahenduste arendamisele eelnevaid andmekaitse mõjuhinnangu dokumente, järelevalvega konsulteerimisi ega üldisemalt lõimitud andmekaitse ja vaikimisi andmekaitse põhimõtete juurutamist avalikustama. Küll aga on nn artikkel 29 andmekaitse töögrupp soovitanud vastutaval töötlejal andmekaitse mõjuhinnang osaliselt avaldada, kas või kokkuvõttena.[*30] Ka erialakirjanduses on leitud, et andmekaitse mõjuhinnangu avalikustamine vähemalt riigi IT-lahenduste kohta on oluline, tagamaks huvipoolte õiguste kaitse.[*31] Ühtpidi on üldmäärusega loodud vajalikud mehhanismid selleks, et riik töötleks massisikuandmeid vastutustundlikult. Teisalt on nende reaalne täitmine läbipaistmatu ja sestap raskesti hinnatav. Isegi kui riik on andmetöötluse vallas olnud väga tubli, siis info puudumise tõttu me alati seda ei tea. Ka juhul, kui riigi tegevuses on puudujääke, ei saa me sellele reageerida parandusettepanekutega, sest puudub info vajakajäämiste kohta. Niisiis, esimese sammuna tuleks riigisisese andmekaitsealase õigusruumi arendamisel kaaluda, kas ja mis tingimustel tuleb riigil avaldada informatsiooni riiklike IT-lahendustega isikute põhiõigustele kaasnevate riskide ja nende maandamise viiside kohta.

Üks võimalus selleks on kehtestada nõue, et enne IT-lahenduse arendamiseks vajaliku riigihanke korraldamist tuleb selle nõuete väljatöötamiseks teha andmekaitsealane mõjuhinnang, mille tulemused avaldatakse vähemalt arendatava IT-lahenduse hankedokumentatsioonis. Ideaalis võiks riigil olla nii tava-, häda- kui ka eriolukorras käepärast varem kokkulepitud ja läbitestitud valik lahendusi, mis võimaldavad massandmete töötlemist kooskõlas põhiseadusega. Arendusele eelneva mõjuhinnangu raames saaks valida igaks konkreetseks juhtumiks neist sobivaima.

Teiseks tuleks selgelt dokumenteerida ja avalikustada teave, millistel juhtudel riigi infosüsteemides isikuandmeid masstöödeldakse. Isegi kui andmeid ei ole võimalik üksikisiku tasandil tuvastada ning seetõttu ei jõua inimeseni info tema andmete kasutamise kohta riigi infosüsteemides, on avalikkusel huvi aru saada, kuidas kasutatakse massandmeid kui üksikisikute kohta koondatud andmeid ja kas selline kasutusviis on ühiskonnas vastuvõetav.

Kolmandaks: Eestis juurutatud *once only* põhimõtte[*32] valguses peaks olema avalikkusele läbipaistev, millistel teisese kasutuse eesmärkidel ühtesid ja samu isikuandmeid töödeldakse. Õigusteadlastele on tuttav elektroonilise side andmete säilitamise saaga[*33], kus mobiilsideoperaatoritele Euroopa Liidu õigusega pandud kohustust säilitada liiklus- ja asukohaandmeid õigustati algselt võitlusega terrorismi ja raske kuritegevuse vastu avaliku julgeoleku tagamiseks.[*34] Tegelikkuses hakkasid liikmesriigid, sealhulgas Eesti, tekkinud uut andmeallikat ära kasutama ja teostama töötlust riigisisese õiguse alusel ka muudel eesmärkidel. Abstraktse põhiseaduslikkuse analüüsi käigus ei leidnud Eesti õiguskantsler selles olukorras vastuolu põhiseadusega, kuid tõdes, et andmete töötlemise süsteem pole täiuslik ning konkreetsete töötlemisjuhtude puhul võiks siiski esineda menetluslikke probleeme ja küsitavusi.[*35] Sama võib juhtuda muudes valdkondades, kus isikuandmete koondamine ja säilitamine on kallis või keeruline, nii et riik soovib neid andmeid kasutada võimalikult mitmel otstarbel ja kuluefektiivselt. Kodaniku vaatest on oluline jälgida, et andmetele juurdepääs oleks eesmärgipärane ja piisavalt kontrollitud ega väljuks põhiseadusega kehtestatud raamidest.

30 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. 17/EN WP 248 rev.01. Adoptect on 4 April 2017. As last Revised and Adopted on 4 October 2017, p 18. Arvutivõrgus: https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236 (15.09.2020).

31 S. L. Harris. Data Protection Impact Assessments as rule of law governance mechanisms. – Data & Policy 2020 (2) e2, p e2-18. Arvutivõrgus: https://www.cambridge.org/core/journals/data-and-policy/article/data-protection-impact-assessments-as-rule-of-law-governance-mechanisms/3968B2FBFE796AA4DB0F886D0DBC165D (16.08.2020).

32 Printsiip, mille järgi peaks kodanik või ettevõte riigile standardset teavet andma üle vaid üks kord. Kui riigil seda edaspidi vaja on, saaks ta seda teavet riigisiseselt taaskasutada ning vältida näiteks seda, et mitmes asutuses on ühe isiku kohta erinev, sageli väär teave.

33 U. Lõhmus. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. – Juridica 2016/10, lk 704.

34 EKo (suurkoda) 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform, Commissioner of the Garda Síochána, Iirimaa, ja The Attorney General*, p 42.

35 Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus. Õiguskantsleri 22.04.2016 seisukoht nr 6-1/140621/1601788, lk 12.

Neljas võimalus on seada prioriteediks riigi infosüsteemidega ühilduvate privaatsuskaitse tehnoloogiatega seotud teadus- ja arendustegevus ning tagada selle läbipaistvus avalikkusega jagatavate teaduspublikatsioonide ning analüüsi-, arhitektuuri- ja arendusdokumentide kaudu. Nii peaks olema kontrollitav, kuidas algoritme isikuandmete töötlemisel rakendatakse ja kas see on kooskõlas põhiseadusega.

Nimetatud neli võimalust on vaid esmaseks mõtteaineks ja diskussiooni käivitamiseks isikuandmete masstöötluse õiguslike piiride ja tehniliste võimaluste teemal. Põhiseaduse juubeliaastal on paslik püüda heita pilk tulevikku ning kujutleda, mismoodi võiks digitaalse ühiskonna tingimustes isikuandmeid rohkem väärindada nii, et hundid söönud ja lambad terved. Kutsume üles selles diskussioonis kaasa lööma nii õigusteadlasi kui ka andmekaitse- ja infoturbespetsialiste ning eetikuid, sest üksnes valdkonnaüleses interdistsiplinaarses koostöös on võimalik leida sobivaid lahendusi andmekaitseõigusest mõjutatud põhiõiguste ja -vabaduste riivete omavaheliseks tasakaalustamiseks.

Autoritest: Dan Bogdanov on Cybernetica AS juhatuse liige ja infoturbeosakonna juht.
Triin Siil on Cybernetica AS infoturbesüsteemide osakonna privaatsustehnoloogiate üksuse õigusanalüütik.