Tartu Ülikool

Sotsiaalteaduste valdkond

Johann Skytte poliitikauuringute instituut

Martin Reissar

PRIVAATSUS VS TURVALISUS: RIIGITEOORIATE KONFLIKT KÜBERKURITEGEVUSE JA TEHNOLOOGIAAJASTUL

Magistritöö

Juhendaja: Viljar Veebel, PhD

Kaasjuhendajad: Illimar Ploom, PhD & Hent-Raul Kalmo, MSc

Tartu 2021

Olen koostanud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, põhimõttelised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.
Olen nõus oma töö avaldamisega Tartu Ülikooli digitaalarhiivis DSpace.

.....

Martin Reissar

Sisukord

Abstrakt

Uurimistöö analüüsib privaatsuse ja turvalisuse kaasaegset vastandumist tehnoloogiaajastu kontekstis. Küberkuritegevuse kaudu on toimunud oluline paradigmaatiline muutus. Riigid on oma jõumonopoli ja kodanike turvalisuse tagamisel muutunud sõltuvaks nii erasektori ettevõtetest kui teistest riikidest. Tagantjärele seni anarhiliste ilmingutega küberruumi reguleerimine on toonud esile põhimõttelise probleemi riigivõimu liigsest sekkumisest inimeste vabadustesse. Samas akadeemiliselt on tagaplaanile jäänud asjaolu, et ulatuslikud vabadused ja privaatsus võib omakorda avalduda ohuna turvalisusele. Käesolev töö selgitab privaatsuse ja turvalisuse vastandumist Thomas Hobbesi ja Georg W. F. Hegeli riigiteooriate toel ning väidab, et viidatud konflikti aitab selgitada oluliselt erinev vabaduse defineerimine. Kui liigsed piirangud avalduvad autokraatlikena, siis piirangute puudumise tulemusel tekkiv hirm ja ebakindlus võivad piirata küberruumi vabadusi hoopis teistsugusel viisil. Uurimuse käigus selgus, et Eestis turvalisust kujundavad riigiametnikud on valdavalt seisukohal, et privaatsus ja turvalisus ei ole omavahel olemuslikult vastanduvad. Välistades olemusliku vastandumise momendi, on võimalik argumenteerida, et privaatsus ja turvalisus on kaks ajas muutuvat ning selgelt ja otseselt üksteist mõjutavat väärtust.

Sissejuhatus

Tehnoloogia kiiret arengut on valdavalt peetud ühiskonda positiivselt mõjutavaks nähtuseks. Ühest küljest on tehnoloogia tekitanud lugematul hulgal uuenduslikke majanduslikke, sotsiaalseid, meditsiinilisi jm võimalusi ühiskondliku heaolu ja elatustaseme suurendamiseks. Samas on positiivsete arengute taustal tehnoloogia soodustanud uute ja omanäoliste ühiskondlike ohtude teket. Tehnoloogia kiire areng, kättesaadavus, ulatuslik levik ning internetis võimalikuks saanud ulatuslik anonüümsus, on loonud soodsad tingimused ka kuritegevusele. Seetõttu on tehnoloogia kujunenud oluliseks ohuks inimeste turvalisusele ning riikide julgeolekule (vt nt Tabinsky 2012). Riikide püüded uute ohtudega kohaneda on omakorda tõstnud esile mure kodanlike vabaduste vähenemise ees. Ulatuslikult on levinud valdavalt ühemõtteline ühiskondlik ja akadeemiline seisukoht, mille kohaselt on riikidepoolne tehnoloogiakasutus turvalisuse ja julgeoleku tagamiseks muutunud suureks ohuks eelkõige inimeste privaatsusele (vt Drozdova 2003; Neocleous 2007; Friedewald et al. 2017). Seevastu antiteesina on väidetud, et ulatuslik privaatsus kujutab ohtu turvalisusele (Burgess 2008: 3). Kuna tegemist on seni vähest akadeemilist diskussiooni pälvinud vastuolulise argumendiga, on käesoleva magistritöö eesmärgiks mainitud puudujääki adresseerida.

Poliitilisel tasandil on küberkuritegevuse ohtlikkuse ja probleemsuse tõdemine pälvinud Euroopa Liidus (EL) aastatega üha enam tähelepanu ning küberturvalisust reguleerivad mitmed mahukad õigusaktid. Samuti on küberkuritegevus ning vajadus tulla toime tehnoloogia ulatusliku kasutamisega kuritegevuse toimepanemisel üheks prioriteediks Euroopa Komisjoni esitatud Euroopa julgeoleku tegevuskavas 2015-2020 kui selle jätkustrateegias aastateks 2020-2025 (Euroopa Komisjon 2015; 2020a). Võttes arvesse, et 2021. aastaks on küberrünnakud nii kodanike, ettevõtete kui riikide suunal muutunud igapäevasteks, on probleemi esiletoomine strateegiadokumentides asjakohane. Tervikuna on küberkuritegevuse tunnustamine olulise globaalse ja ühiskondliku probleemina nii teaduskirjanduses kui ekspertanalüüsides üsna ühemõtteline. Seevastu probleemi olemuse ja põhjuste kohta võib leida äärmiselt erinevaid argumente ja hinnanguid. Erimeelsused küberkuritegevuse probleemi kirjeldamisel on omakorda tekitanud olulise arutelu probleemi võimaliku lahendamise osas. Tehnoloogia järjepideva arenemise ja probleemide süvenemise

taustal on prognoositud, et see arutelu jääb kaasaegse ühiskonna lahutamatuks osaks (Giacomello 2005). Nimelt seisneb arvamuste lahknevus probleemi lahendamiseks kasutatavates meetmetes. Üldistatult saab kuritegevust tõkestavaid poliitikaid ning tegevusi liigitada kahetiselt - kaitsvateks (ingl *protective*) ja reageerivateks (ingl *reactive*). Kui kaitsvad meetmed panustavad näiteks infosüsteemide turvalisusesse ja rünnakute ennetamisesse, siis reageerivad meetmed keskenduvad kuritegevuse menetluslikule ehk õiguskaitselisele poolele (Drozdova 2001: 186-187). Kuigi ennetustöö erinevates valdkondades on kahtlemata oluline ning vajalik, tuleb samal ajal silmas pidada kaasaegset demokraatlikku põhimõtet, mille kohaselt on riikidel kohustus tagada iga inimese põhiõiguste kaitse. Sealhulgas on inimestel õigus riigipoolsele kaitsele, mis avaldub näiteks riigipoolses kohustuses menetleda isikute vastu sooritatud kuritegusid ehk reageerivas funktsioonis.

Kuigi ennetustöö on oluline kõikides kuritegevust, turvalisust ja ohutust tagavates valdkondades, ei võimalda see ohte siiski kunagi lõplikult vältida. Ühtlasi on tehnoloogia areng kahetsusväärselt näidanud, et digitaalsete ohtude ja digitaalse kuritegevusega kohanemine on üleilmselt keeruline väljakutse (vt nt Peters & Jordan 2019). Ka Euroopa Liidu Õiguskaitsekoostöö Ameti (Europol) perioodilised ohuhinnangud ja statistika kinnitavad, et kuritegude toimepanemisel on tehnoloogia kasutamine muutunud aasta-aastalt üha ulatuslikumaks ning kuritegevusevastane võitlus seetõttu järjest komplitseeritumaks (vt nt Europol 2020). Kuivõrd riigil tuleb tagada inimeste õigused ja kaitse nii füüsilises kui virtuaalruumis, on jätkuvalt oluline ka reageeriva mudeli suutlikkus kurjategijaid vastutusele võtta. Siinkohal avaldubki tehnoloogia laialdasest levikust välja kasvanud keskne vastuolu (O'Neil 2001) – kuigi ühest küljest soovivad inimesed riigipoolset kaitset ja ohtudele reageerimist, siis kuidas tagada seda küberkuritegevuse ehk andmetel põhineva kuritegevuse kontekstis inimeste põhiõiguseid protsessi käigus võimalikult vähe riivates?

Eelneva kirjelduse pinnalt avaldub töö keskne uurimisobjekt ning probleem: turvalisust ja privaatsust mõistetakse üksteisele vastanduvatena. Tegemist on levinud thomashobbesiliku arusaamaga, mille kohaselt saab inimese turvalisuse suurenemine tuleneda üksnes tema isiklike vabaduste arvelt ja vastupidi. Seevastu alternatiivne, G.W.F. Hegeli käsitlus viitab, et seaduste ja reeglite kaudu riik mitte ei piira, vaid tagab inimeste vabadused ja õigused.

Antud küsimus on eriti aktuaalne Euroopas, kuivõrd EL regulatsioonide tulemusel on privaatsus (Balboni & Pelino 2013) ja isikuandmete kaitse (Gonzales Fuster & Gutwirth 2013) tagatud tugevamal määral kui mujal maailmas. Tugev orienteeritus isikuandmete kaitsele avaldub viimaste aastate märgilistes Euroopa Liidu Kohtu (ELK) otsustes. 2014. aastal tühistati ebaproportsionaalse põhiõiguste riive tõttu Euroopa Liidu sideandmete direktiiv (C-293/12 ja C-594/12). Kaks aastat hiljem, 2016. aastal, tunnistati põhiõigustega vastuolus olevaks riiklikud õigusaktid, mis kohustavad kuritegevuse tõkestamise eesmärgil sideteenuse osutajatel säilitada kõikide klientide sideandmeid (C-203/15 ja C-698/15). Seevastu on sideandmed küberkuritegude lahendamise väga oluline komponent, mis on omakorda tekitanud turvalisuse tagamise vaatest olulise probleemi.

Turvalisust ja riiklikku julgeolekut on nii eraldiseisvalt kui koostoimes privaatsuse ja turvalisusega analüüsinud paljud autorid. Eraldiseisvalt on analüüsitud Euroopa Liidu õiguslikke probleeme ja vastuolusid. Samuti on põhjalikult analüüsitud nii küberkuritegevuse teooriaid, praktikaid, motivatsioone, ajendeid kui ka tehnilisi menetluslikke detaile. Paraku puuduvad käsitlused, mis seoks omavahel ühtseks tervikuks privaatsuse, turvalisuse ja hiljutiste kohtulahendite ehk EL õiguse mõju küberkuritegevuse menetlemisele kaasaegses infoühiskonnas. Tegemist on huvitava nähtusega, kuivõrd oma olemuselt on õigus keskne privaatsust ja turvalisust tasakaalustav faktor – õigus defineerib, mida ja kuidas riik teha tohib ning maandab kaitsemeetmete kaudu riigi omavoli. Seega on just õigusnorm ning õigusnormide tõlgendatavus dilemma keskne komponent, mis tasakaalustatuse mõtestab.

Magistritöö eesmärgiks on esitada olemasoleva kirjanduse põhjal filosoofiline argumentatsioon privaatsuse ja turvalisuse olemusliku vastandlikkuse üle tehnoloogiaajastule omases kontekstis. Kui väärtuseid iseloomustatakse vastandlikena, siis milles see „vastandlikkus“ konkreetsemalt seisneb või mida vastandlikkus eeldab? Kas vastandlik suhe vajab küberkuritegevuse, tehnoloogia- ning massandmeajastul laiemat, teadlikumat ning mitmekülgsemat mõtestamist? Uurimistöö eesmärgiks ei ole esitada ammendavaid tõendeid ja ettepanekuid probleemide lahendamiseks, vaid peegeldatakse kaasaegse ühiskonna mitmeid põhimõttelisi paradokse, mis omamoodi huvitaval moel kajastavad jätkuvalt esmaste ühiskonnateooriate primitiivseid baasküsimusi.

Filosoofilist argumentatsiooni toetab Eesti turvalisust kujundavate ametnike hulgas läbi viidud ankeetküsitlus. Kui Euroopa Liidu supranatsionaalset ja siseriiklikke õigusruume suunavad üldjoontes poliitilised jõud, siis õigusloome kujundamisel on kandev roll riigiametnikel. Sellest lähtuvalt on uurimistöö peamiseks uurimisküsimuseks: mil määral peegeldub Eesti turvalisust kujundavate ametnike arusaamades küberruumi õiguste kaitsel vastuoluline riigikäsitlus, kus turvalisuse pakkujana on riik ühtaegu nii vabaduste kaitsja kui piiraja? Keskset uurimisküsimust toetavad töö teoreetilise osa lõpus esitatud alaküsimused.

Magistritöö teoreetilises osas avatakse esmalt kasutatavad mõisted ning privaatsuse ja turvalisuse vastanduse kontseptsioon. Väärtuste omavahelist suhet selgitatakse Hobbesi ja Hegeli riigiteooriate põhjal ning mõtestatakse üldisemalt angloameerikaliku *New Public Managementi* (NPM, eesti keeles uus haldusjuhtimine) ja traditsioonilise avaliku halduse vastandumisena. Uurimuse teises peatükis käsitletakse privaatsuse ja turvalisuse vastandumist 21. sajandi kontekstis ning esitatakse põhjalik ülevaade küberkuritegevuse kujunemisest oluliseks globaalseks probleemiks. Töö kolmas osa selgitab esmalt uurimistöö analüüsimiseks kasutatavaid meetodeid ning keskendub seejärel uurimisküsimustele vastamisele. Argumentatsiooni käigus esitatakse ka ankeetküsitluste tulemused. Uurimistöö neljas peatükk mõtestab uurimisküsimuste vastuste ja ankeetküsitluste järelduste kontekstis privaatsuse ja turvalisuse paradoksaalset suhet. Kokkuvõtvas osas esitatakse peamised tulemused ja uurimisküsimuste vastused ning tuuakse välja täiendavaid analüüsimist vajavaid uurimisvaldkondi.

1. Teoreetiline raamistik: privaatsuse ja turvalisuse omavaheline suhe Hobbesi ja Hegeli riigiteooriates

Uurimistöö teoreetiline peatükk analüüsib privaatsuse ja turvalisuse kui kahe fundamentaalse inimõiguse omavahelise vastandumise loogikat, selle teoreetilist käsitlust ning mudeli olulisust uurimisteema ja laiemalt Euroopa Liidu kontekstis. Selgitatakse mõistete „privaatsus“, „turvalisus“ ning „privaatsuse riive“ tähendust. Seejärel kontseptualiseeritakse Mandri-Euroopa avaliku halduse ja angloameerikaliku uue haldusjuhtimise (ingl *New Public Management,* NPM) taustal privaatsuse ja turvalisuse vastandumine.

1.1. Privaatsuse ja turvalisuse definitsioonid

Nii turvalisust kui privaatsust nähakse väga mitmedimensioonilise ning raskelt defineeritava mõistena. Kuigi nende mõistete käsitlused on ajas oluliselt arenenud ja muutunud, saab sõltuvalt raamistusest mõlemat iseloomustada kui teiste vabaduste eeltingimust (Kolliarakis 2017: 240). Ühtlasi sõltub mõistete tähendus sellest, millises valdkonnas ja kontekstis neid kasutatakse – nii „meedias, poliitikas, tehnoloogias, kriminoloogias kui õiguses kasutatakse nii privaatsust kui turvalisust mõnevõrra erinevalt“, mistõttu on ammendavate ja ühtsete definitsioonide loomine keeruline (van Lieshout et al. 2013: 123). Seetõttu on vajalik selgitada, kuidas privaatsust ja turvalisust mõistetakse ning uurimistöö konteksti seotakse.

1.1.1. Privaatsus

Privaatsus (ka era- ja perekonnaelu puutumatus[1]) on tugevalt kinnistunud kui üks inimese põhiõiguseid. See on sätestatud nii Euroopa inimõiguste ja põhivabaduste konventsiooni (EIÕK) artiklis 8.1, Euroopa Liidu põhiõiguste harta artiklis 7 kui ka Ühinenud Rahvaste Organisatsiooni (ÜRO) inimõiguste ülddeklaratsiooni artiklis 12. Kuigi privaatsus on Euroopas tugevalt kaitstud ning keskne tegur erinevate poliitikate kujundamisel, on

1 Eestikeelsetes õiguslikes tekstides kasutatakse väljendit era- ja perekonnaelu puutumatus. Käesolevas töös kasutatakse üldise mõistena privaatsust.

privaatsuse ühemõtteline sisustamine osutunud üpris keeruliseks. Põhjalikult privaatsust ning selle olemust analüüsinud autorid Gloria Gonzales Fuster ja Serge Gutwirth (2013) kirjeldavad, et Euroopa riikides on privaatsuse mõtestamine toimunud pidevas arengus ning võrdlemisi erinevatel alustel. Autorid väidavad, et 2000. aastatel ELi poliitilisel tasandil täheldatav keskendumine privaatsuse kaitsele on veelgi enam „muutnud tajutavaks lahknevad ja isegi vastuolulised arusaamad privaatsuse olemusest“ (Gonzales Fuster & Gutwirth 2013: 532). Tegemist on üsna loogilise arenguga, kuivõrd eelnimetatud inimõiguseid sätestavates raamdokumentides selgitused privaatsuse olemusest puuduvad. See omakorda muudab problemaatiliseks arusaamise, mida ning kuidas privaatsuse osas kaitsta tuleks (Lukacs 2016: 259).

Privaatsuse mõtestamine on keeruline ka seetõttu, et see kätkeb endas väga paljusid erinevaid tegureid. Näiteks avaldub euroopalik privaatsus kahes erinevas õiguslikus konstruktsioonis: privaatsuse enda kaitses ning isikuandmete kaitses (Gellert & Gutwirth 2013; van Lieshout et al. 2013). Nende erisus seisneb selles, et „privaatsus keelab sekkumise isiku sõltumatusse , andmekaitse defineerib aga tingimused, millal isikuandmete töötlemine on seaduspärane“ (van Lieshout et al. 2013: 120-121). Käesolev uurimistöö keskendub sideandmetele, mis tekivad sideettevõtte telekommunikatsiooniteenuste tarbimisel. Üldistatult on sideandmed andmed, mis võimaldavad tuvastada nii konkreetse teenuse kasutajat kui teenuse kasutamise täpset aega. Teisisõnu on tegemist isikuandmetega (vt Milaj 2015), mis moodustavad seeläbi osa privaatsuse terviklikust käsitlusest.

Kuivõrd privaatsus eeldab isikute sõltumatuse ja tegevusvabaduste säilitamist, on seda sotsiaalteaduslikul tasandil kontseptuaalselt väga erinevalt mõtestatud. Üldistatult on eristatud isikut ja tema käitumist, suhtlust, isiklikke andmeid, asukohta, tundeid ning muud isikuga seotust omavat infot (Milaj 2016: 121). Näiteks Paul De Hert (2005: 75) on kirjeldanud, et privaatsed ehk isiklikud andmed omavad teatud tunnuseid, mis võimaldavad konkreetset inimest tuvastada või iseloomustada. Seega on äärmiselt „privaatseteks“ andmeteks näiteks biomeetrilised andmed (Bowyer 2004). Tehnoloogiaajastule omases kontekstis on privaatsust iseloomustatud muu hulgas kui inimese kontrolli oma andmete ja informatsiooni liikumise ning leviku üle ehk individuaalset otsustusõigust, millises ulatuses, kes ja kuidas nende kohta informatsiooni teada saada võiks (Westin 2003: 431).

Privaatsusele ehk isiklikule sõltumatusele on viidatud ka kui seisundile, milles „inimene on vaba välisest sekkumisest“ (ingl *interference*) (Friedewald 2017: 260) ja üldiselt kui „õigusele olla rahule jäetud“ (ingl *right to be let alone*) (Rubenfield 2008: 115-118). Nagu ilmneb, on kõik need käsitlused mõnevõrra erinevad, moodustades keerulise terviku.

Ühetaoliste tõlgenduslike suuniste puudumisel on erinevate andmete kasutamine ning privaatsuse võimalik riivamine korduvalt kohtute tasandil vaidlustatud. See on omakorda tekitanud olukorra, kus Euroopa Liidu Kohus (ELK) (Gonzales Fuster & Gutwirth 2013) ja Euroopa Inimõiguste Kohus (EIK) on kohtupraktikat kujundades muutunud peamisteks privaatsuse mõiste sisustajateks, tõlgendades privaatsust erinevates kontekstides ning hinnates riivete proportsionaalsust erinevates tingimustes (Gellert & Gutwirth 2013: 524). Seevastu ei ole ka kohtupraktika suutnud pakkuda ammendavaid selgitusi privaatsuse olemusest. Näiteks on EIK sedastanud, et privaatsus hõlmab „muu hulgas isikute füüsilist ja sotsiaalset identiteedi, sh õigust isiklikule sõltumatusele, isiklikule arengule ning suhete loomisele ja arendamisele teiste inimeste ja välismaailmaga“ (Evans vs Ühendkuningriik 2007, § 71). Kuid ehk kõige olulisemaks EIK järelduseks saab pidada, et üheselt ja ammendavalt ei ole võimalik ega ka vajalik privaatsust terminina sisustada (vt nt Pretty vs Ühendkuningriik 2002, § 61). Seega „tuleb privaatsust sõltuvalt ajastu eripäradest ja ümbritsevast kontekstist vastavalt olukorrale ümber tõlgendada“ (Lukacs 2016: 258). Liigne tõlgendusulatus, nagu uurimuse peatükkides 3.4 ja 3.5. selgitatakse, soosib konflikti tekkimist.

1.1.2. Turvalisus

Uurimistöö analüüsitav kese lasub kuritegevusel ehk riikide õiuskaitseasutuste tegevusel kuritegevuse tõkestamisel. Sellest tulenevalt ei käsitleta turvalisuse kontekstis riiklikku julgeolekut (ingl *national security*), sest julgeolek on valdavalt sõjaline ja riigikaitseline, mitte politseiline ja üksikisikute õiguste kaitsele keskenduv valdkond (Walt 1991). Esiteks, vähemalt *de jure* ei reguleeri Euroopa Liit liikmesriikide riiklikku julgeolekut (Euroopa Liidu leping, art. 4. p. 2). Lisaks eristavad küsitlustes „riiklikku julgeolekut“ ja inimeste „individuaalset ohutust“ selgelt ka EL kodanikud (Porcedda 2017: 193). Euroopa Liidu tasandil on inimeste turvalisuse tagamisel tugevalt keskendutud kuritegevuse vastasele

võitlusele (vt Eckes & Konstandinides 2011), mida peegeldab osaliselt ka ELi aluslepingutes kasutatav väljend „vabadusel, turvalisusel ja võrdlusel“ põhinev ala.

Seega mõistetakse uurimustöös turvalisuse mõiste all laiemalt nii avaliku korra tagamist ja korrakaitset (ingl *public order, social order*) kui ühiskondlikku ja individuaalset turvalisust/ohutust/heaolu (ingl *societal security, public safety, individual safety*), millest olulise osa moodustab erinevat liiki kuritegevuse vastane võitlus. Kuritegevusevastase võitluse kõrval ja sellega osaliselt kattuvalt eksisteerib inimturvalisuse kontspetsioon (ingl *human security*), mis kätkeb endas inimeste heaolu kõikehõlmavalt, alates majandusest kuni tervishoiuni (Owen 2004), samuti vaesusest, haigustest, kliimamuutustest ja energeetikast lähtuvate probleemidega tegelemist (Strauß 2017: 258).

Sarnaselt privaatsusele võib selgepiiriliste definitsioonide puudumine tuua kaasa turvalisuse mõiste pideva ajas muutumise. Põhiõiguseid kajastavates raamdokumentidest ei selgu ühiselt, mida eelnimetatud mõisted olemuslikult tähendavad. Erinevalt privaatsusest ei paku raamdokumendid nendele mõistetele isegi abstraktset kirjeldust ning sama üldiseks on jäänud ka EIK (Somody et al. 2017: 163). Seevastu, sarnaselt privaatsuse kujunemisele, on ka erinevad võimalikud ohud ajas pidevalt muutunud ja arenenud. Näiteks küberkuritegevus ei saanudki enne tehnoloogia arenguhüpet ning massidesse levikut tänapäevasel kujul eksisteerida. Seega peaks turvalisuse kontseptsioon sõltuvalt ümbritsevast keskkonnast suutma samuti erinevate muutuvate tingimustega kohaneda (Dratwa 2014: 65). Tervikuna võib mõista turvalisust ka kui vaba olemist erinevatest riskidest ja ohtudest (van Lieshout 2013: 122).

Kaasaegses infoühiskonnas avalduvad ohud inimestele märksa erinevamalt, kui aastakümneid ja -sadu tagasi. Täna on peetakse üheks suurimaks ühiskondlikuks ohuks ja väljakutseks organiseeritud kuritegevust (Grabosky 2007), mis oma olemuselt ohustab nii avalikku korda, inimeste turvalisust kui nende individuaalset sotsiaalset heaolu. Sellest tulenevalt on tekkinud vajadus defineerida ka need tegevused, mida nähakse ühiskondlikult kahjulikena ning teisi inimesi kahjustatavatena. Kuritegevust defineeritakse õiguslikult läbi kriminaalsüsteemi, mille laiem eesmärk on „sotsiaalse korra tagamine“ (Farmer 2014: 399), mis määratleb ebaseaduslikud tegevused ning neile vastavad sanktsioonid.

Sotsiaalse korra tagamine ei seisne aga üksnes karistamises, vaid laiapindsema väärtuse loomises. Korrakaitseasutuste ülesandeid on kirjeldanud Herman Goldstein (1977), loetledes näiteks inimeste põhiõiguste kaitset, liikumisvabaduse säilitamist, inimeste kaitset füüsilise väärkohtlemise eest, erinevate gruppide vaheliste konfliktide lahendamist ning ühiskondlike, potentsiaalselt eskaleeruvate probleemide tuvastamist ja nende lahendamist. Sellest lähtuvalt mõtestab käesolev uurimustöö turvalisust kui ühiskonna heaolu seisundit, mille eesmärgiks on tagada kollektiivne turvaline keskkond, kus igal inimesel oleks individuaalselt ohutu tegutseda. Uurimuses keskendutakse konkreetselt kriminaalsüsteemis defineeritud tegevustele ehk kuritegevusele, mis annab riigile ühelt poolt õiguse, aga teisalt ka kohustuse oma jõudu rakendada ning seaduserikkujaid vastutusele võtta.

1.2. Privaatsuse riivamise mõtestamine

Privaatsuse riivamise mõtestamine on uurimistöö seisukohalt oluline, kuivõrd just nimelt privaatsuse riivet tõlgendatakse inimeste vabaduste, spetsiifilisemalt privaatsuse vähenemisena (vt nt Drozdova 2003; De Hert 2005; Liberatore 2007; Neocleous 2007; Taylor 2014; Vedaschi & Lubello 2015, üldisema ülevaate saamiseks vt Solove 2011; Friedewald et al. 2017). Kuna privaatsus ei ole absoluutne õigus, on riigivõimul õigus privaatsust teatud juhtudel eesmärgipäraselt seaduslikult riivata. Teisisõnu on privaatsuse riive lubatud, kui see on saavutatava eesmärgi suhtes proportsionaalne. Inimõiguste ja põhivabaduste kaitse konventsiooni (EIÕK) artikli 8 punkt 2 sätestab, et riik ei sekku inimeste privaatsusesse välja arvatud „kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks“. Kuigi Euroopa Liidu põhiõiguste harta näeb ette üksnes õiguse ilma piiranguteta, peegeldavad demokraatlike riikide põhiseadused EIÕK sõnastust (näiteks Eesti Vabariigi põhiseaduse § 26). Seevastu keerulisem on defineerida, kas olemuslikult seisneb privaatsuse riive üksnes tehnoloogiate kasutamises, andmete analüüsimisel ja töötlemisel või ainuüksi asjaolus, et andmeid mingil eesmärgil säilitatakse.

Akadeemilises kirjanduses on levinud üpris ühemõtteline akadeemiline seisukoht, mille kohaselt on üheks privaatsuse riive peamiseks allikaks olemuslikult tehnoloogia ise (vt nt

van Brakel & De Hert 2011; Aquilina 2015) ning selle kasutamine riikide poolt teatud eesmärkidel, näiteks turvalisuse tagamiseks, avaldub inimeste privaatsuse vähenemisena (vt nt Galetta & De Hert 2014; Taylor 2014). Õiguskaitse ehk turvalisuse tagamise kontekstis on nendeks tehnoloogiad, mis võimaldavad koguda, talletada või analüüsida teatud inimestega seotud informatsiooni. Kuritegude uurimise ja tõkestamise kontekstis näiteks kõnede pealtkuulamine (Somody et al. 2017: 162), turva- (Waiton 2010) ja liikluskaamerad (Wells and Wills 2009), lennujaamades ja mujal kasutatavad keha skaneerimise vahendid (Bellanova & Gonzalez Fuster 2013), droonid (Marin 2017) ja andmed, mis võimaldavad isikuid identifitseerida bioloogiliste tunnuste põhjal ehk biomeetria (näotuvastus, DNA, sõrmejäljed) (Bowyer 2004: 9). Seega, kui tehnoloogiad, mis inimeste privaatsust riivata suudavad on üsna üheselt mõistetavad, siis puudub selge arusaam sellest, milles privaatsuse riive olemuslikult seisneb.

Küberkuritegevus kaasaegse ja tehnoloogilise kuriteoliigina põhineb peaasjalikult andmete omavahelisel suhtlusel. Seetõttu on andmete töötlemine küberkuritegevuse tõkestamiseks möödapääsmatu (Brown 2015). Andmete töötlemine võimaldab kuritegevuse analüüsimise kontekstis teha konkreetse isiku osas kindlaid järeldusi. Seetõttu on andmete töötlemist peetud aga väga selgeks riiveks isikute põhiõigustele (Aquilina 2010: 136). Teoreetilisest vaatest on problemaatilisem küsimus, kas privaatsuse riive seisneb ka üksnes andmete kogumises (Aquilina 2010: 136). Teisisõnu, kas olemuslikult riivatakse kõikide isikute privaatsust ka juhul, kui nendega seonduvaid andmeid ei töödelda? Uurimistöö raamistuses saab analoogseteks andmeteks pidada eelkirjeldatud sideandmeid, mida riik on pidanud vajalikuks turvalisuse tagamise eesmärgil säilitada. Juriidiliselt on ELK hinnanud, et riigipoolne nende andmete säilitamise kohustamine on inimeste privaatsust riivav, sest säilitatud andmed võimaldavad teha põhjalikke järeldusi isiku eraelu kohta (*Digital Rights Ireland*, § 27). Järelduste tegemine eeldab aga eelnimetatud andmete töötlemist. ELK otsus liidetud kohtuasjas C-203/15 ja C-698/15 (ka *Tele2 Sverige*) viitab, et sideandmete üldine säilitamine on vastuolus Euroopa Liidu põhiõiguste harta privaatsuse põhimõtetega (§ 134 lg 1). Selle põhjal on võimalik tuletada, et ELK on privaatsuse riivamisena tõlgendanud ainuüksi andmete säilitamist, sõltumata sellest, kas neid andmeid kasutatakse järelduste tegemiseks või kuritegevuse tõkestamise eesmärgil analüüsimiseks.

Privaatsuse riivet ja vabaduste vähenemist kaasaegses infoühiskonnas iseloomustatakse peaasjalikult läbi riigivõimu. Näiteks on väidetud, et „jälgimistehnoloogiad“, nagu rahvaloendus ja kodanike registreerimine, loodi inimõiguste tagamiseks, kuid samal ajal võimaldas see riigil omandada inimeste üle sotsiaalse ja informatiivse kontrolli (Lyon 2004: 136, vt ka Abercrombie et al. 1983). Ehk ainuüksi andmete kogumine riigifunktsioonide täitmiseks annab riigile isikute üle teoreetilise kontrolli. Seevastu viitab Birch (2009: 145), et teoreetiliselt üldine privaatsus säilib, kui esineb üksnes võimalus isikute vajaduspõhiseks kindlakstegemiseks ja tuvastamiseks, kuid mitte isikute suhtes erinevate järelduste tegemiseks. Seetõttu on õigusteoreetiliselt võimalik argumenteerida küsimuse üle mitmeti ning erineva argumentatsiooni kaudu jõuda ka väga erinevate tulemusteni.

1.3. Privaatsus ja turvalisus: dilemma kontseptualiseerimine

Alljärgenevalt avab magistritöö esmalt väärtuste vastandumise olemuse Thomas Hobbesi, kes esimesena sellise võrdlemisi radikaalse mudeli ühiskonnateoreetiliselt konstrueeris, käsitlusest lähtuvalt. Seejärel selgitatakse privaatsuse ja turvalisuse dilemmat Jeremy Waldroni 2003. aasta tasakaalustavale käsitlusele tuginedes ning üldisemalt väärtuste tasakaalustamise loogikat. Samuti kõrvutatakse hobbesilikku nullsumma mängu (ingl *zero-sum* game) kontseptsiooni privaatsuse ja turvalisuse suhtega Georg Wilhelm Friedrich Hegeli riigi ja õiguse olemuste käsitlustele tuginedes. Seejärel mõtestatakse Hobbesi ja Hegeli käsitlusi tänapäevasemas kontekstis uue haldusjuhtimise (NPM) ja traditsioonilise, kontinentaalse ehk Madri-Euroopa õigusriikluse omavahelise suhte kaudu. Peatüki lõpetuseks esitatakse teoreetilisest raamistikust lähtuvalt täiendavad uurimisküsimused, mis käesoleva uurimistöö probleemi mõtestada aitavad.

1.3.1. Thomas Hobbesi riigiteooria: vabadus vs turvalisus

Thomas Hobbesi, kes kirjeldas esimesena üsna radikaalselt riigi tekkimist kui kompromissi inimeste individuaalsete vabaduste ja kollektiivse turvalisuse vahel, võib pidada vabaduste ja turvalisuse omavahelise dilemma rajajaks.. Vabaduste ja turvalisuse vastandumise tähendab, et iga kehtestatud seadus osutub hobbesiliku inimloomuse piiritlematu individuaalse vabaduse kontekstis piiravaks. Teisisõnu toimub ühiskondliku kokkuleppe

toel teadlik kompromiss isikute vabaduste ja vabaduste loovutamisest saadavate hüvede vahel.

Seda paradoksaalset suhet on iseloomustatud modernse poliitfilosoofia alguseks (Haker 2015: 4). Käsitluse keskel kohal on riik, õigemini selle puudumise seisund. Hobbes kirjeldab ilma riigita tingimusi loomuseisundina (ingl *state of nature*). Loomuseisund on oma olemuselt anarhiline „kõik kõigi" vastu keskkond, milles inimesed on enamjaolt hirmul, kuivõrd pole võimalik ette ennustada, kuidas teised inimesed nende ümber käituvad ja toimivad (Wolff 2005: 26-27). Hobbes põhjendab hirmu tekkimist inimvabaduste negatiivse ja indiviidipõhise iseloomuga. Ta väidab, et oma piiramatus individuaalses vabaduses on inimesel õigus ja tahe teha, mida iganes ta suudab ja tahab, et tagada enda heaolu ja turvalisus (Wolff 2005: 28; Hobbes 1996: 189). Kuivõrd kõik inimesed soovivad rahuldada oma isiklikke ja eripalgelisi vajadusi, on nad motiveeritud kasutama oma absoluutseid vabadusi omaenese heaolu suurendamiseks (Wolff 2005: 34). Seeläbi tekib anarhilistes tingimustes alaline ehk pidev konfliktiseisund (Wolff 2005: 34). Oma piiramatus ehk absoluutses vabaduses ja etteaimamatuses ohustavad kõik inimesed omakorda üksteise heaolu ja turvalisust.

Sellise alalise konflikti seisundi suudab Hobbesi hinnangul neutraliseerida üksnes riigi tekkimine. Anarhilise ja ohtliku keskkonna likvideerimiseks on inimesed nõus sõlmima kompromissi ehk „ühiskondliku lepingu" (vt nt Barker 1962), läbi mille moodustub suverääni ehk riigi ja alamate ehk kodanike suhe. Riigivõimu kehtestamine eeldab, et isikud määraksid juhi või juhid, kes koondaks kõigi inimeste isiklikud huvid ühtseks huviks (Hobbes 1996: 120). Samuti aktsepteerivad inimesed hiljem suverääni reegleid, et saavutada nii ühiskonna seesmine rahuseisund kui ka kaitse väljastpoolt (Hobbes 1996: 121). Seega saab suverään õiguse kehtestada jõumonopol. Jõumonopoli kaudu avaldub ka suverääni suutlikkus inimeste käitumist suunata, mõjutada ja jõustada (Wolff 2005: 30-31). Seeläbi loob suverään ühiskonnas etteaimatavad tingimused, kus inimestel on üldiselt võimalik üksteiselt eeldada, et oma käitumisega nad üksteist ei ohusta (Wolff 2005: 31). Teisisõnu, organiseeritud ja kontrollitud ühiskond on põhjuseks, miks inimesed on valmis oma absoluutsest vabadusest loobuma (Barker 1962: 50).

Ühiste huvide alla koondudes võtavad inimesed omale kohustuse aktsepteerida suverääni poolt kehtestatud reegleid ning loovutavad osa oma individuaalsest vabadusest. Ühelt poolt võib see osutuda inimestele ja nende vabadustele pärssivaks, sest Hobbesi kohaselt ei kohaldu suveräänile ühiskondliku turvalisuse ja rahu tagamisel mingeid piiranguid (Meos: 2000). Sellest lähtuvalt on väidetud, et ka tänapäeva ühiskondlikus kompromissis on „turvalisuse ja vabaduste omavaheline tasakaal tugevalt turvalisuse poole kaldu“ (Neocleous 2007: 134). Teisalt, kuigi inimestele ei pruugi riigi piiramatu võim meeldida, on riigivõimu kadumine või puudumine Hobbesi hinnangul kindlasti halvem variant, sest on taaskord eelduseks ühiskondlikule ohu- ja hirmuseisundile (Toomla 1990: 38).

Seega on privaatsuse ja turvalisuse dilemma ülesehitus üsna selgepiiriline – hobbesilik kontseptsioon viitab, et üldise turvalisuse saavutamiseks peavad inimesed loobuma mõnedest individuaalsetest vabadustest. Teoreetiliselt muudab see muudab hüved omavahel vastanduvaks ehk ühe väärtuse kasv saab tulla üksnes teise arvelt ehk nullsumma mängu raames. Kuigi tänapäevane demokraatlik ühiskond on Hobbesi absoluutse monarhia mudelist oluliselt erinev, siis on üldine põhimõte endiselt asjakohane – riik on ainus ühiskondlik üksus, kes võib omada jõumonopoli ning seadusandluse kaudu kujundatakse ühiskondlikku käitumist. Just nimelt viidatud käitumise reguleerimise vaatest on tekkinud ka mitmeid kaasaegseid debatte ja kaasuseid, kus riigi turvalisust tagavaid tegevusi ja suuniseid käsitletakse inimõiguste ja vabaduste piirangutena (Tsiftsoglou 2011, vt nt Christmas 2017; Rowe 2020). Kuivõrd väärtuseid mõtestatakse mitmete autorite poolt vastanduvatena, on oluline tasakaalustamise põhimõte.

1.3.2. Privaatsuse ja turvalisuse tasakaalustamine

Arvestades mitmete autorite poolt esitatud argumente, , et riigipoolse turvalisuse tagamisel leiab ühiskonnas aset hobbesilik nullsumma mäng (nt Waldron 2003; Liberatore 2007; Hildebrandt 2013), on vajalik kirjeldada tasakaalustamise loogikat. Tasakaalustamine on käsitletava dilemma otsene väljund, mille abil püütakse poliitikakujundamisel tagada, et ükski meede ei osutuks teiste suhtes liigselt ülimuslikuks. Seega on tasakaalustamise keskseks põhimõtteks proportsionaalsus. Proportsionaalsuse test võimaldab hinnata, kas privaatsuse riivamiseks kasutatav meede on eesmärgi saavutamiseks piisavalt asjakohane

(Milaj 2016: 116). On väidetud, et väärtuste tasakaalustamise loogiline ülesehitus viitab juba olemuslikult konfliktsusele (Waldron 2003; van Lieshout et al. 2013: 123) ning senine akadeemiline diskussioon on olnud sellel teemal võrdlemisi ühemõtteline (Neocleous 2007: 132-133). Seega saab väita, et tasakaalustamise ja proportsionaalsuse vajadus on analüüsitavat dilemmat ja selle eksisteerimist toetav.

Tasakaalustamise vastuolulisusele viitab oma abstraktse mudeliga Waldron (2003). Waldron (2003: 192) võtab eelduseks, et mis tahes olukordades on alati, ja seda rõhutatult, tarvis tasakaalustada vabadusi turvalisuse vastu. Ta mõõdab kujundlikult vabadusi (ingl *liberty* – L) enne-pärast formaadis ehk L_x (väiksem) vs L_y (suurem). R tähendab omakorda riski (ingl *risk* – R) – ohu/kahju suurus ja selle avaldumise tõenäosuse summa – R_k (kõrge risk), R_m (madal risk). Waldron selgitab, et isiku A vabadus mõjutab isiku B riski. Seega AL_x => BR_m ja AL_y => BR_k. Ehk väiksemad vabadused avalduvad väiksema riski ning suuremad vabadused suurema riskina. Antud suhe toimib ka vastupidiselt. Ehk Waldroni mudeli kohaselt suurendab kindel sündmus (näiteks 2001. a 11. septembri terrorirünnak) riski (R_m => R_k) ning R_k maandamiseks tagasi R_m tasemele peavad inimesed teatud vabadustest loobuma (L_y => L_x). (Waldron 2003: 193)

Erinevate uuringute kohaselt peavad privaatsust ja turvalisust vastandlikeks ka tavakodanikud (Pavone & Pereira-Puga 2009; Somody et al. 2017: 160). Seda toetab ka privaatsuse ja turvalisuse dilemma kaasaegne mõtestamine. Čas et al. (2017: 7) on selgitanud, et keeruline on luua tingimusi, kus ühiskonna ulatuslikum jälgimine näiteks valvekaamerate kaudu ühiskonna privaatsust suurendaks. See tähendab, et vastukaaluks tuleb luua garantii või näiteks õiguslike meetmete pakett, mis tagaks uue muutuse taustal ka inimeste privaatsuse kaitse (vt Dratwa 2014: 60). Printsiibis tähendab see, et kaalukausil on individuaalsed vabadused (nt privaatsus) ja avalik hüve (nt turvalisus) (Lewis et al. 2017: 30).

Arenevate tehnoloogiate ja sellest lähtuva võimaliku ulatuslikuma põhiõiguste riive taustal on tasakaalustamine muutunud veelgi olulisemaks. Käesolev uurimistöö keskendub peaasjalikult õiguskaitseasutuste tegevusele tehnoloogilise kuritegevusega võitlemisel. Probleem seisneb asjaolus, et „õiguskaitse- ja julgeolekuasutustele on oma ülesannete täitmiseks vajalikud piisavad volitused, aga nende tegevus on olemuslikult isikute eraelu ja

isikuandmete kaitset riivav“ (Caruana 2019: 249). Riive maandamiseks kasutatakse juriidilisi kaitsemeetmeid (ingl *safeguards*). 2000. aastate keskel Hispaanias läbi viidud uuringus kirjeldasid inimesed, et uute tehnoloogiate rakendamisel peaks privaatsuse riive olema õigustatud üksnes kuritegevusevastase ks võitluse eesmärgil, tagada tuleks selge regulatiivne raamistik, fikseeritud kontrollmehhanismid ja sanktsioonid ning süsteemi läbipaistvus (Pavone & Pereira-Puga 2009: 119-122). Fundamentaalselt hädavajalikuks tasakaalustavaks teguriks on peetud järelevalvet õiguskaitseorganite tegevuse üle (Bowyer 2004, van Brakel & De Hert 2011). Küsimus on, kas nende kriteeriumite täitmisel privaatsus väheneb, tasakaalustub või hoopis suureneb?

Kuigi privaatsuse ja turvalisuse dilemmat ja selle nullsumma mängu põhist ülesehitust on tugevalt kritiseeritud, ei joonistu paraku selgelt, kas dilemma olemuslikult kahtluse alla seatakse. On väidetud, et väärtuste vastandamine poliitikate kujundamisel on väär ning demokraatlikke väärtusi õõnestav (vt nt Solove 2011; van Lieshout et al. 2013). Samas ei argumenteerita nende väärtuste olemuslike kontseptsioonide üle. Näiteks on mitmed autorid viidanud, et printsiibis ei ole turvalisuse tagamiseks privaatsuse riive hädavajalik (Solove 2011: 2; Strauß 2017: 259-261). Samas on näiteks Strauß (2017: 269) selgitatud, et teatud olukordades võib nullsumma mängu loogika osutuda vältimatuks. See omakorda võimaldab tuletada, et Strauß ei sea seda dilemmat olemuslikult kahtluse alla, vaid viitab, et probleemide lahendamine ei tohiks olla lihtsakoeline ning erinevaid nüansse kergekäeliselt kõrvale heitev. Seega kritiseeritakse läbivalt riikide tegevust. Näiteks on kirjeldatud, et „riigid prioritiseerivad isikute füüsilist turvalisust teiste, analoogselt võrdsete põhiõiguste, näiteks privaatsuse arvelt“ (Esposti et al. 2017: 88), millest tulenevalt püüavad riigid kasvatada oma rolli ühiskondliku turvalisuse tagajatena demokraatlike väärtuste arvelt kasvatada (Pavone & Pereira-Puga 2009: 113).

Eelnevale tuginedes saab tuletada, et tasakaalustamine väljendub tänapäevases kontekstis hobbesiliku piiramatu ulatuse ja pädevusega riigivõimu piiramises just nimelt vabaduste ja inimõiguste kaitse eesmärgil. Ühtlasi on „väga ebatõenäoline, et kumbki äärmus – täielik jälgimine või täielik privaatsus, oleks meie ühiskonnale hea“, mistõttu on õige tasakaalu leidmiseks vaja eetilist debatti (Smith & Green 2016: 142). Uurimistöös käsitletava probleemi seisukohalt on oluline Stefan Straußi järeldus, mille kohaselt ei tohiks privaatsust

ja turvalisust mõtestada kui omavahel põrkuvaid väärtusi, vaid ühtse tervikuna ning üksteist täiendavatena (Strauß 2017: 269). Püüdes mõtestada privaatsust ja turvalisust koosmõjus, on võimalik tugineda Hegeli riigiteooriale, mille kohaselt saavad inimesed privaatsuse kvaliteeti nautida üksnes riikide poolt loodud seaduste kontekstis.

1.3.3. Georg Wilhelm Friedrich Hegeli riigiteooria: seadus kui vabaduste eeldus

Kaasaegse ühiskonna privaatsuse ja turvalisuse vastandumist saab selgitada hobbesiliku ja hegelliku käsitluste kaudu, milles vabadus on defineeritud fundamentaalselt erineval viisil. Erinevalt Hobbesist ei tähenda vabadus Hegeli käsitluses omavoli (Meos 2000: 167; Ovsjannikov 1974: 80-81) ehk seisundit, kus isikul on õigus absoluutne tegevusvabadus. Hegellik vabadus ei eelda ühtlasi piirangute puutumist. Vastupidi, Hegeli kohaselt on just riik vabaduse eeltingimuseks ning riik iseenesest muutub inimeste vabaduseks, kuivõrd vabadus ehk õigused tekivad inimesele riigi poolt loodud seaduste ja reeglite alusel (Meos 2000: 167-168). Seega üksnes läbi riigi ja seaduste realiseeruvad inimese vabadused (Pelczynski 1984) ning seadusandluse kaudu kujundatakse inimese vaba tahet mingeid tegevusi teha (Ovsjannikov 1974: 81). Teisisõnu toimub vabaduse organiseerimine institutsionaliseerimise teel (Dyde 1894: 659), mis annab Hegeli käsitluses inimestele võimaluse olla vaba ning saavutada oma vabaduste kvaliteet. Inimene saavutab institutsionaliseerituse kaudu „kõrgema, küllaldasema ja rahuldust pakkuvama vabaduse – tõelise, reaalse või tegeliku vabaduse“ (Pelczynski 1984).

Oluline on ka hegelliku vabaduse iseloom. Kuigi individuaalne vabadus on oluline, on olulisem, et individuaalsed „vabad tahted“ realiseeruvad kollektiivselt ehk peegeldavad kõikide inimeste idealistlikku ja universaalselt ühist eesmärki (Pelczynski 1984), mis omakorda iseloomustab vabadust ühiskonna liikmete ühise väärtusena. Seega on vabadus sõltuv ühiskonnaliikmete omavahelisest interaktsioonist (Pelczynski 1984). Inimeste „tegevus ja reaktsioon moodustavad struktuuri vabaks toimimiseks, näiteks mõtestades kuriteo ja karistuse omavahelise vajaliku seose“ (Duquette). Kuigi kurjategijale võib hegellikus riigis tunduda karistus tema isikliku vabaduse piiramisena, põhjendab Hegel, et karistus on kurjategija „tegude väljendus“ (Meos 2000: 168). See tähendab, et kurjategija, sooritades poliitilise kogukonna seadustega vastuolus oleva teo, peab aktsepteerima

suverääni poolt ettenähtud tagajärgedega, sest tema vabadus oli teha mis tahes tegusid ette nähtud seaduste kontekstis ning tema vabadus, küll riigi poolt jõustatud, on aktsepteerida ette määratud tagajärgi. Seega piirab isik teiste vabaduste rikkumisega iseenda vabadusi – rikkudes teiste vabadusi ei saa inimene ise olla vaba (Hinchman 1982: 530).

Ülaltoodust tulenevalt on võimalik argumenteerida, et hobbesilik negatiivne vabadus (ingl *liberty*) eeldab riigi välise sekkumise puudumist ning hegellik positiivne vabadus (ingl *freedom*) eeldab riigi poolt nende vabaduste tagamist ja võimaldamist. Kuigi riik kaotab Hobbesi kirjeldatud anarhilise keskkonna, siis jõuga inimeste seni piiramatut olemuslikku vabadust piirates loob riik tingimused, kus tervikuna omatakse rohkem turvalisust ja seeläbi ka ühiskondlikku stabiilsust. Hegeli kontseptsioon kirjeldab riiki ja selle seaduseid vastupidiselt kui eeldusi inimeste kodanlike vabaduste ja õiguste tekkimiseks ja seeläbi realiseerumiseks. Seadus ongi vabadus, mitte vabaduste piiramine muute oluliste väärtuste (näiteks turvalisus) saavutamiseks, millest tulenevalt ei ole Hegeli kontseptsioonis privaatsus ja turvalisus ka üksteisele vastanduvad.

1.3.4. Traditsiooniline avalik haldus vs uus haldusjuhtimine (NPM)

Hobbesi ja Hegeli teoreetiliste kontseptsioonide sidumiseks tänapäevaga, saab neid iseloomustada läbi avaliku halduse. Kuivõrd kontinentaalne avaliku halduse traditsioon näeb riiki olemuslikult positiivsena, saab siduda seda kontseptsiooni hegellike käsitlustega. Mandri-Euroopa ehk traditsioonilises avaliku halduse süsteemis peegeldub hegellik õigusriiklus ning riigibürokraatia tugev roll avalike hüvede ja ühiskondliku heaolu tagamisel ning inimeste vabaduste realiseerumisel (vt Jackson 1986; Shaw 1992). Seevastu NPM peegeldab hobbesilikku vabaduse käsitlust (vt Zanetti & Adams 2000) – inimestele antakse oma tegevustes suurem individuaalsus ehk riik peaks inimeste igapäevasesse toimimisse sekkuma võimalikult vähe. Seadused avalduvad seega inimestele kohustuste ja piirangutena (Hobbes 1996: 183), mitte hegellike „võimalustena“.

Traditsioonilist avalikku haldust on peetud uue angloameerikaliku haldusjuhtimise suhtes vastandlikuks (vt nt Dunn & Miller 2007). Traditsiooniline euroopalik mudel näeb ette tsentraalset ja hierarhilist riigi juhtrolli ning keskset haldust omavat riigiaparatuuri, milles riik ise tagab avalikud hüved ning teenused, mis omavahel ei konkureeri (Dunn & Miller

2007: 347-348). Üksnes riik vastutab üldiste probleemide lahendamise eest (Dunn & Miller 2007: 349). Traditsiooniline riigihaldus lähtub seega jõumonopolist ning orienteeritusest üldise heaolu tagamisele (Drechsler 2005: 95), mis seostub laiema ühiskondliku ja inimturvalisuse printsiibiga. Kesksel kohal on seadused, reeglid ja normid (Osborne 2006: 378), mille tõttu omab Hegeli kodanikuühiskond olulisi sarnasusi tänapäevase õigusriigi mudeliga (Shaw 1992: 386). Seevastu viimase mõne aastakümne jooksul on avaliku halduse traditsioonide piirid hägustunud ka Euroopas (vt nt Drechsler 2005; Dunn & Miller 2007) ning sõltuvalt riigist on seeläbi vähenenud ka riigi osatähtsus ja roll ühiskonna igapäevases toimimises.

Nimetatud hägustumise põhjuseks võib pidada kategooriliselt erinevat riigijuhtimise põhimõtet. NPM levik on toimunud alates 1970. aastate teisest poolest eelkõige angloameerika riikides (Samier 2001: 239). NPMile on üldiselt iseloomulik erasektori juhtimispõhimõtete kasutamine riigihalduse korraldamises (Samier 2001: 239) ning ideoloogiliselt neoliberalistlik orienteeritus kasumlikkusele ja tõhususele (Drechsler 2005: 97). See tähendab, et oluliseks eesmärgiks on riigiaparaadi efektiivsuse suurendamine ning bürokraatia vähendamine, mida püütakse saavutada riigifunktsioonide erastamise, dereguleerituse ja riigiaparaadi kulude vähendamise abil (Samier 2001: 244). Kui traditsiooniliselt pakkus teatud hüvesid üksnes riik, siis hüvede pakkumine kodanike poolt konkurentsi vormis suurendab NPMi mõistes saadava hüve kvaliteeti ning arendab hüve majanduslikult ja sotsiaalselt edasi nagu iga teist toodet. Kokkuvõtvalt on NPMi käsitletud kodanike isemajandamise ja isikliku vastutuse suurendamisena (ingl *self-governance*) (Dunn & Miller 2007: 247). Teisisõnu toimub NPMi mudelite rakendamise kaudu riigiaparaadi „õhendamine“ ning laiemalt on võimalik täheldada riigivõimu mõju vähenemist ühiskonnale ja inimestele. Töö uurib, kas riigihalduse ja vabaduste erinev mõtestamine aitab selgitada kaasaegset privaatsuse ja turvalisuse probleemi, kus riikide tegevust turvalisuse tagamisel on tõlgendatud liigselt sekkuvana.

Käesoleva uurimistöö peamiseks uurimisküsimuseks on, kuivõrd esineb Eesti turvalisust tagavate ja kujundavate ametnike arusaamades küberruumi õiguste kaitsel vastuolulist riigikäsitlust – turvalisuse pakkujana on riik ühteaegu vabaduste kaitsja ja vabaduse piiraja. Keskset küsimust toetavad neli omavahel seotud alaküsimust.

1. Milline on olnud küberruumi sisuline areng ehk kuidas avalduvad NPM ja kontinentaalne avalik haldus küberruumis ning millised loogilised ja praktilised probleemid avalduvad õiguskaitseasutuste tööle?
2. Kuidas võimaldab Hobbesi ja Hegeli kõrvutamine seletada EL õiguse konfliktsust privaatsust ja turvalisust reguleerivate valdkondade kujundamisel?
3. Kuidas avalduvad hobbesilik ja hegellik paradigma Euroopa Liidu Kohtu otsuste taustal, nende sobivuses digitaalmaailma sisulistesse arengutesse ning millised loogilised ja praktilised probleemid avalduvad nende otsuste tulemusena õiguskaitseasutuste töös?

2. Privaatsuse ja turvalisuse dilemma 21. sajandil

Käesolev peatükk loob uurimistöös käsitletavast probleemist tänapäevase konteksti ning selgitab privaatsuse ja turvalisuse omavahelise vastandumise loogikat kaasaegses teaduskirjanduses. Somody et al. (2017) kirjeldavad, et minevikust võib leida mitmeid analoogseid vastandumisi. Autorid selgitavad, et demokraatia kujunemise protsessi käigus oli vajalik välja töötada loogika, kuidas lahendada õiguslikult riigivõimu poolse inimeste põhiõiguste riive seaduspärasus (Somody et al. 2017: 157). See küsimus ei ole saanud ammendavat lahendust – sarnaselt mitmele teisele ühiskondlikule probleemile omaselt, on ka antud küsimus ajas kontekstipõhiselt muutunud. Tehnoloogiaajastu ja informatsiooni revolutsioon on muutnud õiguste, vabaduste ja turvalisusega seonduvad küsimused üha aktuaalsemaks (Erikkson & Giacomello 2006: 222).

Privaatsuse ja turvalisuse paradoksi lahendamine demokraatlikus ühiskonnas ei ole olnud lihtne seega eesmärk: inimesed soovivad tugevamat kontrolli oma isiklike andmete üle, kuid riikide kohustust inimestele kaitset pakkuda pole samuti võimalik ignoreerida (Lewis et al. 2017: 3; vt ka De Hert 2005: 86). Privaatsuse ja turvalisuse dilemma olemuse põhjalikuks kontseptualiseerimiseks keskendutakse peatüki esimeses osas probleemi avamisele tehnoloogia vaatevinklist. Seejärels selgitatakse aastatega üha tõsisemaks ja ulatuslikumaks rahvusvaheliseks probleemiks muutunud küberkuritegevust ning laiemalt tehnoloogial põhinevat kuritegevust.

2.1. Privaatsus ja turvalisus: probleem areneva tehnoloogia tingimustes

Ühiskond ootab õigustatult õiguskaitseasutustelt turvalisuse ja heaolu tagamist – see on neile seadusega määratud ülesanne ja kohustus. Soovitakse nii „piiramatut ligipääsu erinevatele andmetele kui turvalist ja kaitstud küberkeskkonda“ (Camp & Chien 2000: 14). Teisalt avaldub üha enam, et kaasaegsed õiguskaitsemeetmed tunnetatakse nii inimeste poolt kui teaduskirjanduses liigselt riivavatena. Eurobaromeetri (2017: 3) uuring tuvastas, et võrreldes varasema perioodiga 2015. aastal on suurenenud 11% võrra inimeste hulk, kelle hinnangul ei ole Euroopas turvaline elada (2015 = 17% ning 2017 = 28%). Ühtlasi avaldus, et uuringus osalenute hinnangul ei pruugi õiguskaitseasutused näiteks korruptsiooni, rahapesu ja

inimkaubandusega võitlemiseks piisavalt panustada (2017: 5). Oluliselt on vähenenud ka inimeste hulk, kelle hinnangul ei suuda nad end iseseisvalt küberohtude eest kaitsta (2014 = 74% ning 2019 = 59%) (Eurobaromeeter 2019: 19) ning enamik, ligi kaks kolmandikku tervest vastajaskonnast on mures võimaliku küberkuriteo ohvriks langemise pärast (Eurobaromeeter 2019: 20). Privaatsuse ja turvalisuse omavaheline suhe avaldub seeläbi huvitava paradoksina. Kuigi teaduskirjanduses viidatakse tugevale privaatsuse vähenemisele, sealhulgas Euroopas, ei kajastu see nt Eurobaromeetri vastavates uuringutes.

Eelnimetatud asjaolu võib olla osaliselt põhjuseks, miks on viidatud privaatsuse ja turvalisuse liigsele lihtsustamiseke ja üldistamisele akadeemilistes käsitlustes, mis valdkonna ekspertide hinnangul küsimuse objektiivset käsitlemist raskendavad (vt nt Tabansky 2012; Levy & Robinson 2018). Kahe viimase kümnendi jooksul on valdkondlik teaduskirjandus muutunud turvalisuse tagamise meetodite ja vahendite suhtes üha kriitilisemaks. Tugevalt prevalveerivad kaks seisukohta.

Esiteks on paljud autorid seisukohal, et tehnoloogia vähendab oma olemuselt olulisel määral kodanike privaatsust (vt nt Burgess 2008; Aquilina 2010; Hildebrandt 2013; Hinduja 2015; Rauhofer 2008). Teiseks seostatakse turvalisuse tagamist üha enam „jälgimisega“ (ingl *surveillance*) (vt nt Lyon 2004; De Hert 2005; Waiton 2010; Van Brakel & De Hert 2011; Galetta & De Hert 2014; Taylor 2014; Lischka 2016), mitte õiguskaitsealase tööga inimeste turvatunde tagamiseks ja kuritegevuse tõkestamiseks. Koosmõju jälgimise ning riikidepoolse tegevusega on tekitanud vettpidava järelduse: kuivõrd erinevaid tehnoloogiaid, sealhulgas jälgimistehnoloogiaid, kasutavad turvalisuse tagamiseks oma töös riikide jõustruktuurid (julgeoleku-, politsei- ja teised õiguskaitseasutused), on riigid ühtlasi peamiseks osapooleks, kes isikute õiguseid, sealhulgas inimeste õigust privaatsusele ulatuslikult riivavad (vt Sundquist 2012; Neocleous 2007; De Hert 2005; Solove 2011; Galetta 2013; van Lieshout et al. 2013; Galetta & De Hert 2014; Taylor 2014; Lynskey 2019).

Oma ülesehituselt on eeltoodud argument igati loogiline. Tehnoloogia puhul saab üheks kõige ilmestavamaks näiteks tuua asjaolu, et tänases arvutite- ja infosüsteemide põhises keskkonnas ei ole enam võimalik toimida ilma, et inimeste tegevused, näiteks teenuste tarbimisel, infosüsteemides ei kajastuks (Solove 2011: 2). Tekib niinimetatud tehnoloogiline

jalajälg ehk erinevate virtuaalsete teenuse tarbimisest või toimingute tegemisest moodustuv andmete kogum (vt Micheli, Lutz & Büchi 2018). Arvestades, et turvalisuse tagamise eest vastutab riik, on riik loogiliselt ka see osapool, kes turvalise tagamisega seonduvaid tehnoloogiaid kasutab. Seega nähakse erinevate taoliste tehnoloogiate (nt biomeetria, valvekaamerate, massandmete analüüsivõimekuse, kommunikatsioonitehnoloogiate jne) kiiret arengut ja kasutamist riikide poolt fundamentaalse tegurina, mis isikute põhiõiguseid ja vabadusi ohustab (Pavone & Pereira-Puga 2009: 113). Kriitilist suhtumist ilmestab näiteks George Orwelli „suure venna“ metafoori kasutamine, mis väljendub ühiskonna ja inimeste ranges kontrollimises (vt Liberatore 2007; Waiton 2010; Bauman et al. 2014). Ühtlasi on argumenteeritud, et „11. septembri terrorirünnaku järgset ajastut saab iseloomustada kui valitsuste soovi tekitada globaalne inimeste massjälgimise süsteem“ (Vedaschi & Lubello 2015: 15). Terrorirünnakute järel toimunud tugevat tasakaalu nihkumist kirjeldab ka Mitrou (2007), selgitades, et sideandmete säilitamine on „õiguskaitse eesmärkide täitmiseks metsikult ebaproportsionaalne“, mistõttu ei saa selline jälgimispõhine meede olla demokraatlikus ühiskonnas aktsepteeritav (Mitrou 2007: 427). Kriitikat võimendas veelgi Ameerika Ühendriikide luureteenistuse erinevate jälgimisprogrammide ning tehnoloogiliste võimekuste avalikustamine Edward Snowdeni poolt (vt Greenwald 2013; Lischka 2016). Seega seadis 2013. aastal toimunud dokumentide avalikustamine riigivõimu poolse andmete töötlemise ja tehnoloogia kasutamise veelgi suurema kahtluse alla.

Andmekaitset ja inimeste põhiõiguseid puudutavate probleemide taustal leidub paraku vähe teaduslikke analüüse, mis käsitleksid andmekaitsega seonduvate regulatsioonide ja tehnoloogiate arenemise negatiivset mõju kuritegevuse tõkestamisele ja inimeste turvalisuse tagamisele ehk õiguskaitseasutuste tööle laiemalt. Põhjalikult on käsitletud jälgimistehnoloogiate kasutamise eetilisi ja õiguslikke probleeme (vt De Hert 2005; Solove 2011, van Lieshout et al. 2013; Aquilina 2015; Lischka 2017), kuid puuduvad selgitused, millises kontekstis või millisel eesmärgil õiguskaitseasutused neid andmeid kasutavad. Samuti ei käsitleta teaduskirjanduses, miks on selliste tehnoloogiate või andmete kasutamine tehnoloogiaajastul osutunud vajalikuks. Seetõttu on selle tühimiku, eriti infotehnoloogia kontekstis (Europol 2019), täitnud valdkonna praktikud ja õiguskaitseasutused (vt nt Europol & Eurojust 2019; Europol 2020). Samas leidub hulgaliselt akadeemilisi analüüse, mis käsitlevad küberkuritegevust, selle tüpoloogiaid ning digitaalset kriminoloogiat (vt

Jewkes & Yar 2010; Britz 2013; Brown 2015; Stratton et al. 2017; Nurse 2018). Kuigi küberkuritegevust kirjeldavad ja selgitavad artiklid räägivad andmete vajalikkusest, ei seota neis kuritegevuse tehnilisemat ja keerulisemat iseloomu andmete analüüsivajaduse ega privaatsuse ja turvalisuse omavahelise vastuoluga.

Eelkirjeldatu põhjal ilmneb, et probleemi kajastatakse üsna ühekülgselt ehk eelkõige privaatsuse ja inimõiguste kaitse vaatest. Diskussioonist on puudu konkreetne argumentatsioon ja põhjuslik suhe, mille tõttu on juhitud juhtinud tähelepanu asjaolule, et kaasaegse õiguskaitse töömeetodite kriitika on pinnapealne ega hõlma probleemide ja detailide sisulist ega põhjalikku analüüsi (Lewis et al. 2017: 3). See on mõneti loogiline, kuivõrd õiguskaitseasutuste sisemise toimimise ja praktikate põhjalik uurimine, analüüsimine ja kajastamine võib kõrvalseisja jaoks osutuda keeruliseks. Siiski, puuduliku analüüsi ja erinevate detailide ignoreerimise tagajärjel võib arutelu taanduda „pelgalt lihtsustatud akadeemilistele üldistustele turvalisuse, privaatsuse ja riikide valitsuste rollist nende väärtustega seoses“ (Levy & Robinson 2018). Seevastu väidavad Hayes et al. (2015: 13) Euroopa Parlamendi jaoks koostatud küberkuritegevuse ja põhiõiguste teemalises analüüsis, et tehniliste arutelude asemel on palju olulisem diskussioon fundamentaalsete põhimõtete üle. Kuivõrd tehnoloogiline kuritegevus, eriti küberkuritegevus, on väga spetsiifiline, tehniline, detailirohke ning kõrget ekspertiisi nõudev valdkond (vt nt Britz 2013), tuleb privaatsuse ja turvalisuse probleemi 21. sajandil käsitleda oluliselt laiemalt, kui üksnes riikide poolt keskselt kontrollivat tegevust.

Privaatsuse ja turvalisuse paradoksi iseloomustamiseks on uurimistöö võtnud keskseks analüüsiobjektiks sideandmete säilitamise küsimuse. Emotsionaalselt on kirjeldatud ja kritiseeritud riikide „kasvavat isu“ erasektori andmete järele ning õiguskaitseasutuste poolt erasektorile esitatavate päringute hulga suurenemist kuritegevuse tõkestamisel (Jasserand 2018: 154). Samas võib see nähtus peegeldada mitte riikide poolset kontrolli, vaid oluliselt muutuvat kuritegelikku maastikku. Virtuaalsel tasandil toimepandavat ehk numbritel põhinevat kuritegevust ei ole võimalik lahendada ilma erinevaid andmeid analüüsimata ehk nagu on väljendanud Eesti eksperdid: „andmed on digitaalse maailma DNA“ (Aas & Gross 2021). Seega võib Jasserandi esitatud kriitika olla digitaliseerumise kontekstis paratamatu ja vältimatu, aga veelgi enam, igati loogiline 21. sajandit iseloomustav suundumus.

Privaatsuse ulatuslikule riivele vastukaaluks võib tänases infoühiskonna ja virtuaalruumi tingimustes näha ka rohkelt privaatsuse ja anonüümsuse probleemkohti. Peter Burgess (2008: 3) on iseloomustanud: „privaatsus on muutunud turvalisuse objektist ohuks turvalisusele“[2]. Virtuaalmaailma ja interneti olemus, ülesehitus ning väärtused on peamised asjaolud, mis küberkuritegevuse vastast võitlust raskendavad. Ühest küljest on anonüümsuse ja privaatsuse kaitsmine virtuaalruumis kujunenud eelnimetatud „digitaalse jalajälje“ tõttu eriti oluliseks. Teisalt on privaatsust kaitsvad tehnoloogiad muutunud küberkuritegevuse toimepaneku fundamentaalseks komponendiks. Selle tulemusena on küberruumis tegutsevaid kurjategijaid üha keerulisem vastutusele võtta (Brown 2015), mistõttu ongi privaatsusel võime olulisel määral turvalisuse tagamist negatiivselt mõjutada.

Kuritegu või turvalisust puudutav intsident tõstab automaatselt esile ka turvalisuse ja privaatsuse dilemma. Ilmselt võib privaatsuse ja turvalisuse vastandumist tuletada ka tõsiasjast, et ühe isiku õiguste ja heaolu kaitseks riivatakse kellegi teise omi (Dratwa 2014: 78-84). Seevastu on oluline silmas pidada privaatsuse riive olulist printsiipi, mille kohaselt on taoline riive õigustatud, kui sellega püütakse kaitsta ja tagada teiste inimeste vabadusi. Paraku „rõhutab igaüks enda individuaalset õigust privaatsusele, mis ei peegelda tõsiasja, et kollektiivsed ühiskondlikud fundamentaalsed väärtused vajavad samuti kaitset“ (Drewer & Miladinova 2017: 299). Seega ongi korduvalt tõstatunud küsimus, kuidas oleks võimalik ja teostatav turvalisuse tagamine 21. sajandil viisil, mis ühegi inimese õiguseid ega vabadusi ei riivaks? Tegemist on pikaajalise probleemiga, mida digitaalse kuritegevuse ja andmepõhise ühiskonna areng praktikas üha võimendab – andmeid, mille kaudu inimeste privaatsust on võimalik riivata, tekib igapäevaselt juurde hoomamatutes ühikutes.

2.2. Küberkuritegevus: kuritegevuse paradigmaatiline muutus ajas

Eelneva argumentatsiooniga seoses on hädavajalik on analüüsida, millest tulenevalt väidavad õiguskaitseasutused enda üha suuremat sõltuvust andmetest ning milles seisneb politseitöö ja turvalisuse tagamise peamine väljakutse 21. sajandil. Võrreldes varasemate aastakümnetega, on toimunud oluline ja kiire muutus – kommunikatsiooni- ja

[2] Inglise keeles: „privacy has metamorphosed from being the object of security to a very threat to security“.

infotehnoloogiad on muutunud ühiskonna lahutamatuks osaks. Nutiseadmed, targad autod, linnad ja kodumasinad, tehisintellekt, riiklikud süsteemid, pangandus- ja paljud tervishoiuteenused ning igapäevased olmetegevused põhinevad kõik tehnoloogial, tarkvaral ja algoritmidel. Kolm viimati nimetatut on aga ühtlasi virtuaalselt rünnatavad ja manipuleeritavad. Tundub, et ühest küljest on kuritegevuse sooritamine muutumas üha lihtsamaks, kuid teisalt muutub selle toimepaneku iseloom tehniliselt üha komplitseeritumaks. Kuivõrd eelmainitud areng on kiire ja jätkuv, peab muutustega pidevalt kohanema ka kuritegevuse ja sellega seonduvate võimaluste mõistmine (Brown 2015).

Kuigi oli ennustatav, et tehnoloogia toel toimub oluline arenguhüpe, alahinnati olulisel määral tehnoloogia arengu ühiskondlikku ja kuritegelikku mõju. Wasik (2010) kirjeldab, et 1970-1980. aastatel leidsid paljud teadlased ja eksperdid, et küberkuritegevuse näol on tegemist üksnes marginaalse nähtusega. Peagi ilmnes, et olemasolev seadusandlus ei olnud uut liiki kuritegude sooritajate vastutusele võtmiseks piisav ning virtuaalne kuritegevus oli muutumas pidevalt arenevaks ning ühiskonnale äärmiselt tõsiseks väljakutseks kujunevaks nähtuseks (Wasik 2010: 395-399). Kuivõrd interneti ja virtuaalmaailma kaudu tekkinud globaalne ühendatus on loonud lugematul hulgal majanduslikke ja sotsiaalseid edulugusid, on igati loogiline, et tehnoloogia on muutunud ka kuritegevuse lahutamatuks osaks. Seetõttu on tehnoloogiline areng võimaldanud tekkida ka ohtlikel kuritegelikel tendentsidel ning toonud kaasa revolutsiooni kuritegevuse toimepaneku osas. Kuigi globaalse küberkuritegevuse poolt tekitatud kahju arvutamine on keeruline, on prognoositud, et selle suurusjärk ulatub globaalselt kuni kuue triljonini dollarini (Morgan 2019).

Selleks, et digitaalsete ohtude olemust paremini mõista, on oluline eristada kahte enam levinud tehnoloogilise küberkuritegevuse klassifikatsiooni. Esiteks eristatakse traditsioonilist kuritegevust, mille toimepanemisel kasutatakse erinevaid tehnoloogilisi vahendeid eesmärgiga oma tegevusi varjata, lihtsustada ja füüsilises maailmas esinevaid kontakte minimeerida. Teaduskirjanduses on kuritegevuses tehnoloogiliste vahendite kasutamise probleemi tõstatatud näiteks inimkaubanduse (Gerry QC et al. 2016), lapsporno (Eneman, Gillespie & Stahl 2010), terrorismi (Tehrani, Manap & Taji 2013), narkokaubanduse (Eck & Gersh 2000) ja organiseeritud kuritegevuse puhul laiemalt (Grabosky 2007). Teiseks tuleb eraldiseisvana käsitleda üksnes tehnoloogial põhinevat

kuritegevust ehk küberkuritegevust, mille toimepanek oleks ilma tehnoloogia, interneti ja arvutite olemasoluta võimatu. Sellisteks kuritegudeks on näiteks viiruste, pahavara ja spämmi levitamine, infosüsteemide ründamine ja teenustõkestusründed (DDoS).

Kuigi küberkuritegevuse mõistet on sisustatud väga erinevalt, kasutatakse käesolevas uurimistöös Lior Tabansky definitsiooni. Tabansky mõtestab küberkuritegevust kui „küberruumi kasutamist ebaseaduslikel eesmärkidel, kasutades ära unikaalseid küberruumi võimalusi, nagu kiirust, vahetust, distantseeritust, krüpteeringuid ja toimingute tehnoloogilist hägustamist, mille tulemusel on nii konkreetset toimingut kui toimingu sooritajat keeruline tuvastada“ (Tabansky 2012: 118). Seega käsitleb uurimistöö mõlemat liiki kuritegusid – nii neid, millele tehnoloogia teatud tingimustes kaasa aitab kui ka kuritegusid, mida ei oleks tehnoloogiata võimalik sooritada, kuivõrd tehnoloogiline sideandmetest sõltuv komponent on aktuaalne mõlemal juhul.

Küberkuritegevus tundub olevat mitte üksnes ajutine populaarne nähtus, vaid üha tõsisemalt avalduv ühiskondlik probleem. Esiteks on küberkuritegevus muutumas üha ulatuslikumaks. Tehnoloogia arenemine soodustab olemuslikult kuritegevuse muutumist globaalsemaks ja virtuaalsemaks (Tabansky 2012; Tehrani, Manap & Taji 2013), mille tõttu on eri liiki kuritegude toimepanemisel vähenenud füüsiliste ja geograafiliste piirangute mõju (vt ka Wall 2010: 95-101). Piirangute puudumine avaldub rünnakute igapäevasuses ning nende mõju sadadele miljonitele inimestele (vt nt Gatlan 2019). 2020. aasta märtsi alguses avalikustati kurjategijate poolt kokku pandud andmebaas, mis sisaldas üle 300 miljoni Facebooki kasutajakonto isikuandmeid (Spadafora 2020) ning varastati ettevõtte Trident Crypto Fundi 266 000 kliendi kasutajakontode isikuandmed (Zmudzinski 2020). Ainuüksi 2019. aasta 12 suurimat andmeleket puudutasid kokku miljardeid kasutajakontosid ning nendega seotud isikuandmeid (Henriquez 2019). Andmete „pantvangistamise“ ehk lunavararünnete tõttu on Ameerika Ühendriikide Föderaalse Juurdlusbüroo (FBI) andmetel üksnes USA ettevõtted ja riigisektor aastatel 2013-2019 kaotanud 140 miljonit dollarit (Abrams 2020).

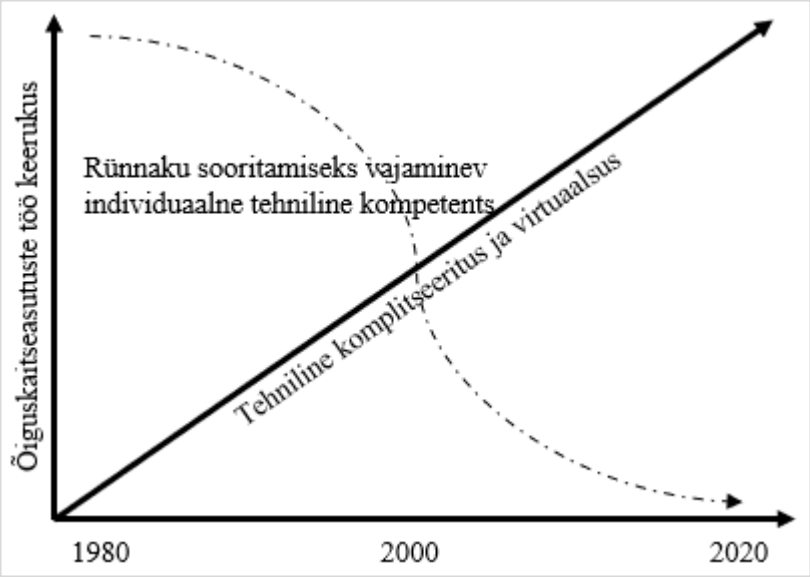
Erinevaid ettevõtete ja inimeste vastu suunatud ründeid toimub iga päev miljoneid. Seetõttu võib väita, et igapäevane virtuaalne küberkuritegevus on muutunud uueks normaalsuseks. Kuigi mitteammendava kinnitusena, viitab sellele ka jätkuv õiguskaitseasutuste

intsidentidest alateavitamine (Britz 2013: 10; Brown 2015: 59). Teoreetiliselt on arvutite abil ühel inimesel võimalik rünnata keda iganes ja millal iganes – inimesi, ettevõtteid ja riike ning seda üleilmsel tasandil. Ühtlasi võimaldab tehnoloogia lugematul hulgal erinevaid ründevektoreid (Nurse 2018), mis nii virtuaalset kui füüsilist mõju avaldavad. Äärmuslikku näidet tuues on täna finantsturge ja börsi reguleerivaid arvutisüsteeme pahavaraga rünnates võimalik tekitada globaalne majanduskriis (Yar 2010: 555). Küberrünnakute vägagi reaalne füüsiline mõju ilmnes selgelt 2020. a septembris, kui teatati, et küberrünnaku põhjustatud haigla süsteemirikke tagajärjel suri Saksamaal inimene (Eddy & Pelroth 2020). Tegemist on olulise pretsedendiga, mis ilmestab selgelt küberkuritegevuse potentsiaalse ohtlikkus tõsidust.

Teiseks saab paradoksaalselt väita, et küberkuritegevus on muutunud ühtaegu nii lihtsasti teostatavaks kui tehniliselt väga komplitseerituks. Lihtsus tuleneb juba mainitud globaalsusest ehk füüsiliste piirangute puudumisest. Teise olulise tegurina lihtsustab küberkuritegevust sadadesse miljonitesse ulatuva käibega kuritegelik turg (Campell 2021), kus virtuaalselt isikuandmeid, kuritegelikke teenuseid, pahavara lähtekoode ning nii-öelda valmis tooteid müüakse (Tabansky 2012; Weimann 2016). Kui paari aastakümne eest tähendas küberkuritegevus peaasjalikult tehnikanohikute ja arvutispetsialistide võimete testimist ja proovilepanekut, siis täna on pahatahtlikul isikul võimalik osta sihtmärkide meiliaadressid ja krüptotarkvara ning see inimestele laiali saata, omamata seejuures ise mingeid tehnilisi teadmisi. See avaldub omamoodi kuritegeliku teenuspõhisusena. Organiseeritus ja teenuspõhisus kätkevad endas erinevate meetodite arendajaid, nende testijaid ning tegevusi haldavaid „projektijuhte“, (Prokuratuur 2020), mis viitab selgelt kuritegeliku keskkonna keerulisele ülesehitusele.

Seevastu küberkuritegevuse tehniline komplitseeritus tähendab seda, et sõltumata rünnaku lihtsusest, on selle menetlemine õiguskaitseasutuste jaoks igal juhul keeruline. Rünnaku iseloom, olles olemuslikult tehnoloogiaga seotud, muudab kõik seadmed rünnatavaks (Heartfield et al. 2018). Rünnakute keerulist olemust iseloomustavad tehnoloogiline andmetel põhinev „keel“, andmete sorteerimisvajadus ning tõendusmaterjali leidmine (Dinant 2004; Britz 2013: 336-348) ehk terade eraldamine sõkaldest. Ühtlasi raskendab mistahes rikkumiste puhul krüpteeringute ja oma asukoha ja IP aadresside peitmine oluliselt

menetluse protsessi (Lewis et al. 2017: 2-17). Lisaks on täna kasutusel väga palju ning erinevat ründetarkvara ja viiruseid, mida on omakorda ümber arendatud tuhandetes variatsioonides ja modifikatsioonides (Choo 2011: 721). Allen et al. (2000) seostasid selle suhte ka ajafaktoriga – mida ajas edasi, seda tehnilisemaks ja raskemaks küberkuritegevus muutub. Seda trendi kinnitab ka Microsoft – 2020. aastal täheldati jätkuva trendina järjest keerulisema (ingl *sophisticated*) iseloomuga rünnakute arvu kasvu (Burt 2020).



Joonis 1. Õiguskaitseasutuste töö muutumine ajas keerulisemaks (vt ka Allen et al. 2000).

Eeltoodud paradoksaalset suhet ilmestab ülaltoodud joonis 1. Rünnaku sooritamiseks vajaminev individuaalne tehniline kompetents on ajas vähenev, kuid rünnakute tehniline komplitseeritus, virtuaalsus ja globaalsus on ajas suurenev. See on omakorda muutnud oluliselt keerulisemaks õiguskaitseasutuste tegevuse virtuaalruumi turvalisuse tagamisel ehk kuritegude menetlemisel. Seega on täheldatud korrelatsiooni tehnoloogia arengu ja õiguskaitseasutuste töö tehnilise keerukuse osas.

Privaatsuse küsimus on eriti teravalt tõusetunud küberkuritegevuse menetlemise ja sideandmete säilitamise puhul. Eelnevas peatükis selgitati hinnanguid, mille kohaselt on tehnoloogia olemuslikult inimeste privaatsust riivav ning riigid kujutavad tehnoloogia kasutamisel endast inimeste privaatsusele veelgi suuremat ohuallikat. Nende argumentide kõrval tuleb veelkord toonitada, et tehnoloogiat kasutavad üha enam ka kurjategijad (Broadhurst et al. 2014; Hayes et al. 2015; Peters & Jordan 2019). Privaatsuse vaatest

avaldub peamise probleemina asjaolu, et küberkuritegevus põhineb oma olemuselt andmetel ja nende omavahelisel suhtlusel. Seetõttu seisneb keskne küsimus isiku tuvastamises, mida paraku on samuti võimalik teostada üksnes andmeid analüüsides. Seega on andmed kuritegude lahendamiseks hädavajalikud (Aas & Gross 2021), kuid andmete paljusus ei muuda õiguskaitseasutuste tööd lihtsamaks, vaid pigem vastupidi (Drewer & Miladinova 2017). Kuivõrd erinevad andmed on virtuaalruumis läbisegi, riivab õiguskaitseasutuste töö paratamatult erinevate isikute privaatsust. Põhjalik andmeanalüüs on aga vajalik „sündmuste rekonstrueerimiseks, võimaldades vastata küsimustele nagu „kes, mis, kus, millal, miks ja kuidas““ (Beebe & Clark 2004: 4). Statistika kinnitab seda argumentatsiooni: 2018. tuvastati Ameerika Ühendriikides, et tuhande intsidenti kohta leidis aset üksnes kolm arreteerimist, mis on võrreldes teiste kuriteoliikidega äärmiselt väike suurusjärk (Eoyang et al. 2018: 2-3).

Menetlusliku keerukuse suurenemine seisneb kahes väga praktilises asjaolus – isiku ja tema asukoha tuvastamises (Europol 2018: 5-14). Oluline on rõhutada, et virtuaalruumis privaatsust ja anonüümsust kaitsvad mehhanismid, näiteks krüpteeringud, ei ole loodud kuritegelikul eesmärgil, vaid inimeste privaatsuse, turvalisuse ja heaolu kaitseks. Teisalt on nende võimaluste tõttu rünnete toimepanijaid väga keeruline tuvastada või rünnet neile omistada ja seeläbi kuritegu tõendada (Davidoff & Ham 2012; Shamsi et al. 2016). Näiteks on võimalik kasutada oma tegevuste umbisikustamiseks krüpteeritud sõnumivahetuskanaleid, varikontosid, välismaiseid või isikustamata kõnekaarte, satelliittelefone, virtuaal- ehk krüptovaluutasid ja Tumeveebi (Europol 2017). Krüpteeringute tugev mõju turvalisusele ja kuritegevuse arengule avaldus juba 1990. aastate lõpus (vt Denning & Baugh 1997; 1999). Lisaks pakutakse ettevõtete poolt privaatsete võrkude ja serverite teenust, mille olemuslikuks eesmärgiks on luua umbisikustatud ja oma tegevusi privaatsena hoidev internetiühendus. Tervikuna saab väita, et kuigi tehnoloogia tõepoolest võimaldab tugevat ja ulatuslikku põhiõiguste riivet, sõltub see pigem asjaolust, kuidas tehnoloogiat inimeste poolt kasutatakse. Seega omandab olulise rolli ka see, millistel eesmärkidel inimesed anonüümsust ja privaatsust võimaldavaid tehnoloogiaid kasutavad. Kuigi tegemist on üpris loogilise järeldusega, avaldub selle põhiline kandvus väite puhul, et privaatsus on muutunud ohuks turvalisusele.

Eeltoodu põhjal on võimalik argumenteerida, et kuritegelik maastik on tõepoolest olulisel määral nii kvalitatiivselt (oma sisult ja olemuselt) kui kvantitatiivselt (rünnakute ja intsidentide paljususelt) muutunud. Paratamatult on andmekaitse, privaatsus ja eelkõige anonüümsus loonud uusi võimalusi ka kurjategijatele, mis enne tehnoloogia laialdast levikut ühiskonda sellises ulatuses ei mõjutanud. Seda nii turvalisuse kui privaatsuse osas. Kuivõrd me elame tehnoloogiakeskses maailmas, on kasvanud ka rünnatavate objektide liikide hulk ning rünnak küberruumis võib omada füüsilisi, halvimal juhul fataalseid tagajärgi. Seega, kui kuritegevuse sooritamine muutub üha lihtsamaks, selle omadused tehniliselt keerulisemaks, kuid ümbritsev õiguskeskkond ei toeta andmete analüüsimist ühiskondliku turvalisuse kaitseks, seisab ühiskond silmitsi väga tõsise probleemiga. Samas kinnitab statistika üheselt, et erinevate andmevarguste taustal riivatakse igapäevaselt miljonite inimeste privaatsust. See on oluline kontekst, mida on vaja senisest oluliselt paremini ühiskondlikul tasandil teadvustada ja tajuda.

3. Analüüs

3.1. Uurimuse ülesehitus

Uurimistöö kesksek probleemiks on privaatsuse ja turvalisuse vastandlik käsitlemine. Levy & Robinson 2018 heitsid ette teema liigset üldistamist ja ebapiisava detailsusega käsitlemist. Kuivõrd analüüsitav dilemma on väga mitmetahuline, on otstarbekas probleemi lahti mõtestada mitmel erineval viisil. Probleemi analüüsimiseks ja selgitamiseks kasutatakse kolme lähenemist. Töö filosoofiline argumentatsioon tugineb oluliselt erinevate riigiteooriate – hobbesiliku ühiskondliku lepingu, mida ilmestab *New Public Management* (NPM), ja hegelliku kontinentaalse õigusriigi käsitluse omavahelisele konfliktile, mis omakorda aitab peegeldada filosoofide oluliselt erinevat „vabaduste" mõtestatust. Kahe autori ning neile omaste riigiteooriate omavahelist kõrvutamist kasutatakse töös esitatud uurimisküsimustele vastamiseks. Seega on tegemist kvalitatiivse sisuanalüüsiga, mille eesmärgiks on kontseptualiseerida olemasolevates käsitlustes (Kalmus et al. 2015) leiduv väärtuste omavaheline vastandumine ning avada nende käsitluste ja argumentatsioonide taustal alternatiivseid võimalusi viidatud dilemma käsitlemiseks.

Avalikku arvamust dilemma kehtivuse osas on Euroopa Liidu liikmesriikide kodanike seas korduvalt uuritud (näiteks projektid SurPRISE; PRISE ja PRISMS) ning uuringute tulemusi mitmete autorite poolt analüüsitud (vt nt van den Broek et al. 2017; Esposti et al. 2017; Vermeersch & De Pauw 2017; Somody et al. 2017). Seevastu on puudulik turvalisust kujundavate ametnike poolne vaade ning sisend, kuidas nähakse seda ühiskondlikult olulist dilemmat riiklikust vaatenurgast. Seetõttu ongi peamiseks uurimisküsimuseks, kuidas tajuvad privaatsuse ja turvalisuse dilemmat Eesti turvalisust kujundavad ehk õigusruumi reguleerivad riigiametnikud. Riigiametnike dilemma tunnetuste mõistmine on oluline, kuna seadusandluse kujundamise kaudu on just nemad suurel määrala privaatsuse ja turvalisuse dilemma haldajad ning „tasakaalustajad".

On teada, et väärtused mõjutavad vähemalt teatud ulatuses indiviidi otsuseid ja käitumist. Näiteks on seda tuvastatud inimeste poolt turvalisust tagavate meetmete aktsepteerimisel või nende mittetunnustamisel (vt nt Bug & Bukov 2017). Kuivõrd ametnikkonna suurenev

väärtuspõhisus on leidnud ka teaduslikku kinnitust (Montpetit 2011), on võimalik argumenteerida, et ametnike isiklikud väärtused ja hinnangud peegelduvad ka nende igapäevatöös turvalisust kujundavate poliitikate loomisel ja valdkondade reguleerimisel. Ametnike arvamuse teadasaamiseks viidi läbi sihistatud valimi põhine ankeetküsitlus (Lisa 1). Ankeet edastati 25 ametnikule (Riigikantselei, Siseministeerium, Justiitsministeerium, Majandus- ja Kommunikatsiooniministeerium, Politsei- ja Piirivalveamet ning Eesti julgeolekuasutused), vastus saadi 21 ametnikult. Kokku esitati 28 küsimust, mis olid jaotatud kolme teemablokki. Esiteks uuriti NPM ja kontinentaalsest tsentraliseeritusest lähtuvalt õiguskaitse muutumist ajas ehk kas ametnikud mõtestavad riigipoolset inimeste kaitset õiguse või teenusena. Teiseks küsiti küberruumi spetsiifilisi küsimusi reguleerituse ja ning kodanike õiguste kaitsmisel ehk turvalisuse tagamisel. Kolmandaks uuriti vastajate isiklikke hinnanguid vabaduse olemusliku mõtestatuse kohta ning erinevate dilemmat peegeldavate olukordade tajumist.

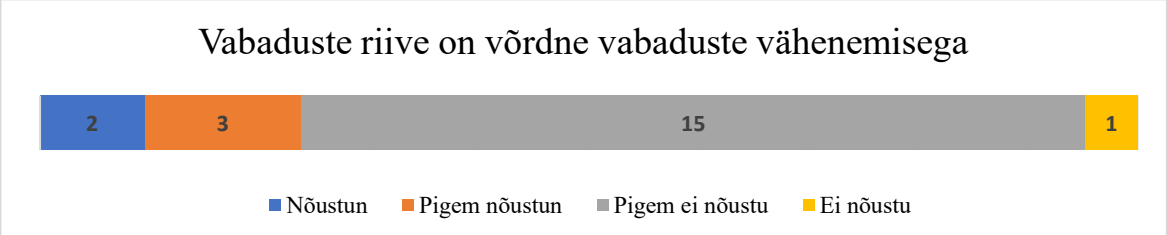
Arvestades, et õigusruum on privaatsuse, turvalisuse ning tasakaalustamise läbivaks keskkonnaks, uuriti juhtumiuuringu abil ka antud aspekti. Juhtumiuuring viidi läbi sideandmete säilitamise ja küberkuritegevuse kontekstis. Sideandmete kasutamine privaatsuse ja turvalisuse dilemma selgitamiseks on asjakohane kolmel põhjusel. Esiteks, nagu iseloomustati peatükis 2.2, on küberkuritegevus kasvav ja suurenev ühiskondlik oht. Teiseks, teatud juhtudel sõltub küberkurjategijate tabamine otseselt võimalusest sideandmeid kasutada (Europol 2017: 5-6). Kolmandaks, Euroopa Liidu Kohus on sideandmete säilitamist hinnanud tugevaks ja ebaproportsionaalseks põhiõiguste riiveks, mis privaatsuse ja turvalisusedilemmat sobivalt iseloomustada võimaldab. ELK kohtuotsustele ja hinnangutele tähelepanu pööramine on oluline, kuivõrd ELK on muutunud väga tugevaks õigusruumi kujundajaks ja rakenduslikuks suunajaks (Blauberger & Schmidt 2017). Samuti on tuvastatud avaliku arvamuse mõju ELK otsustele (Blauberger et al. 2018) ning argumenteeritud, et ELK tugev suund privaatsusele on Edward Snowdeni vilepuhumise tagajärg (Loideain 2015), mis mure privaatsuse pärast tugevalt avaliku debati keskmesse asetas. Viidi läbi väikse-N sisuanalüüs kõikide (5) ELK kohtulahendite osas, mis analüüsisid sideandmete kasutamist kuritegevuse vastase võitluse eesmärgil puudutavate. Esimene kohtulahend (*Digital Rights Ireland*) on pärit 2014. aastast, mil tühistati Euroopa Liidu sideandmete direktiiv ning viimane teemakohane, Eestit puudutav, ELK otsus (H.K vs

Prokuratuur) avalikustati 02.03.2021. aastal. ELK argumentatsiooni kõrvutatakse küberkuritegevuse menetluspraktika teadusartiklitega.

3.2. Privaatsuse ja turvalisuse vastandumine: Eesti riigiametnike tunnetus

Mitmed varasemad käsitlused (vt nt Hildebrandt 2013; van Lieshout et al. 2013; Strauß et al. 2017). Samuti juhiti tähelepanu proportsionaalsuse testile (vt nt Somody et al. 2017). Kui aga järeldub, et proportsionaalsuse test päädib üksnes tehnoloogia õigustamisega, siis ei muuda see asjaolu, et privaatsust ja turvalisust tõlgendatakse vastuolus olevana, vaid välditakse üksnes võimalikku nullsummat. Käesolev peatükk uurib, kuidas tunnetavad probleemi Eesti turvalisust kujundavad ametnikud. Esiteks avaldus selgelt, et pigem on riigiametnikud seisukohal, et vabaduste (näiteks privaatsuse) riivamine ei tähenda automaatselt vabaduste vähenemist (vt joonis 2). Ametnikud selgitasid:

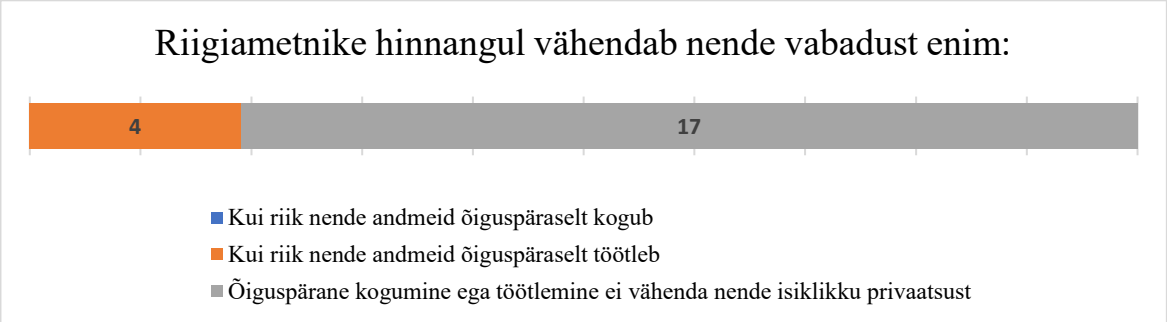
- V1: „Kui riivega tagatakse muud vabadust, siis ei tähenda see alati vabaduse vähenemist, vaid tasakaalu erinevate õiguste ja vabaduste vahel.“
- V19: „Kui see on põhjendatud privaatsuse riivamine, siis on ok.“
- V21: „Üksikisiku vabaduste piiramine ühiskonna julgeoleku tagamiseks seaduslikul alusel ja proportsionaalselt ohuga peaks olema võimalik.“
- V23: „See on absoluutne tõde - vabaduse riive tähendab automaatselt vabaduse vähenemist. Ainult riive puudumisel ei vähene vabadus. Küsimus on riive proportsionaalsuses.“



Joonis 2. Vabaduste riive on võrdne vabaduste vähenemisega.

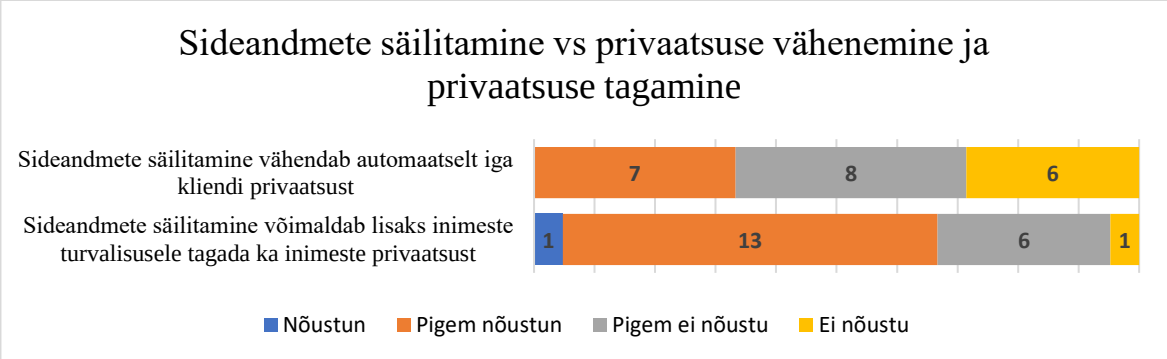
Ehk riivet mõtestatakse proportsionaalse ja lubatud meetmena, mis peaks olema sõltuvalt olukorrast lubatud ning mis olemuslikult ei vähenda konkreetse inimese vabadusi. Seega oli üksnes 2 vastanutest selgel seisukohal, et mistahes riive avaldub automaatselt vabaduste vähenemisena ning 3 olid nullsumma loogikaga pigem nõus. See kinnitab mõnevõrra ka

varasemas teaduskirjanduses (nt Liberatore 2007), et mistahes kaitsemeetmeid või kui tahes eetiline riigi poolne tegevus ka ei ole – väärtused avalduvad alati olemuslikult nullsummana. Seda kinnitas teinegi küsimus, mille osas oli valdav enamus riigiametnikest (17) seisukohal, et õiguspärane riigi poolne andmete kogumine ega töötlemine ei vähenda nende isiklikku vabadust (joonis 3).



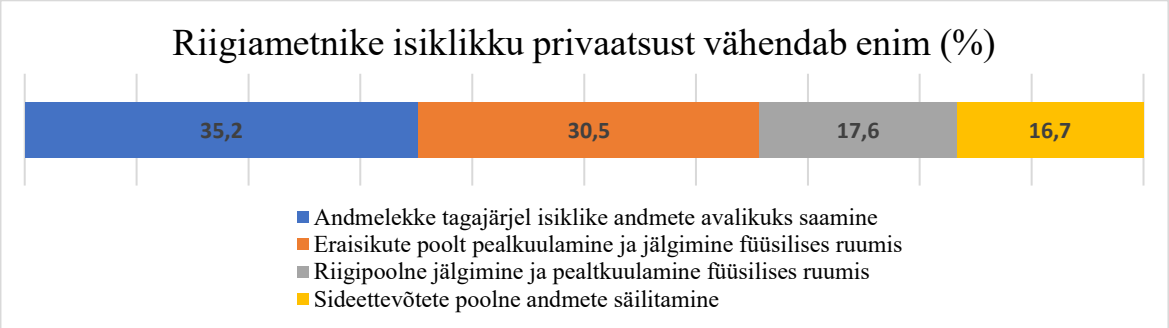
Joonis 3. Vabaduste vähendamine riigi poolse andmete kogumise ja töötlemise kontekstis.

Siinkohal ilmneb huvitav nüanss. Sideandmete säilitamise puhul (joonis 4) olid 7 vastanut seisukohal, et sideandmete säilitamine vähendab nende isiklikku privaatsust – mis on võrreldes eelmise küsimuse vastustega mõnevõrra suurem hulk vastanuid, kui võiks eeldada. Võimalikku erisusust võiks selgitada sellega, et sideandmete säilitamine ei ole teostatud riigi poolt – ehk võimalik vähesem usaldus erasektori suhtes. Samas võivad vastused olla sõltuvas ka kontekstist, kuivõrd sideandmete puhul on tegemist väga detailsete ja põhjalike andmetega. Seevastu 14 vastanut olid taaskord enamuses seisukohal, et lisaks turvalisusele aitavad sideandmed tagada läbi õiguskaitse tegevuste ka privaatsust. Seega võib täheldada oluliselt erinevat hinnangut ümbritsevale keskkonnale.



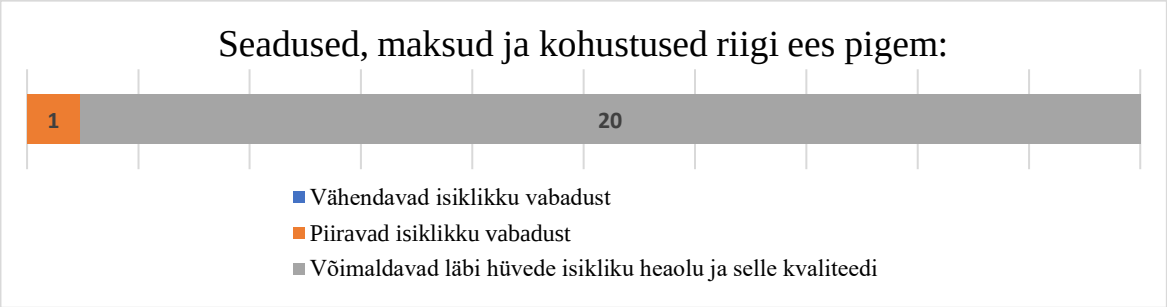
Joonis 4. Hinnang sideandmete säilitamisega kaasnevale turvalisusele ja privaatsuse riivele.

Ühtlasi uuriti, millises kontekstis tunnevad inimesed enim, et nende privaats väheneb (joonis 5). Ametnikud hindasid kõige enam privaatsust vähendavaks asjaolu, kui andmelekke tagajärjel nende isiklikud andmed avalikustuvad. Seejärel avaldus kõige riivamana eraisikute poolne pealtkuulamine ja jälgimine füüsilises ruumis, kolmandana riigi poolne jälgimine ning viimasena, kõige vähem vabadusi vähendavana sideandmete säilitamine.



Joonis 5. Riigiametnike isiklikku vabadust enim vähendavad tingimused.

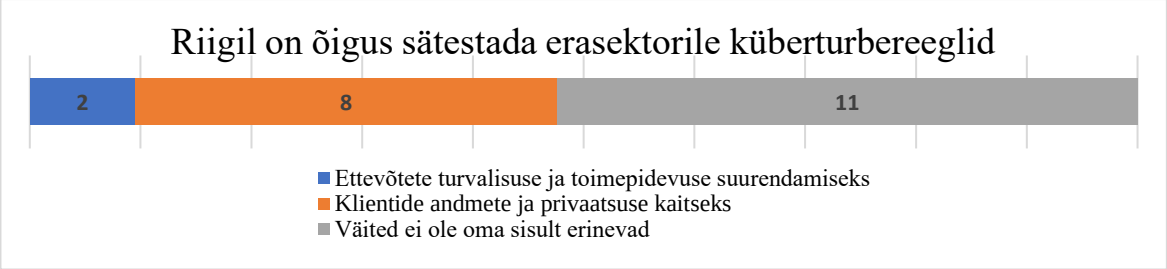
Suurima privaatsuse vähendajana andmeleket võib pidada mõnevõrra eelduslikuks, kuid see on oluline nüanss. Riigi poolne ebaseaduslik tegevus ei tohiks mingitel tingimustel olla lubatud, ehk selline käitumisviis on juba iseeneses ebaeetiline ning õigusvastane tegevus – seega on loogiline, et see vähendaks vabadusi ilmselt enim. Aga oluline on eelkõige mõista riigi seaduslikke tegevusi ning nagu ilmneb, mõtestavad Eesti riigiametnikud, et seaduspärane tegevus ei ole iseenesest vabadustega konfliktis



Joonis 6. Seaduste ja kohustuste avaldumine inimese isiklikele vabadustele.

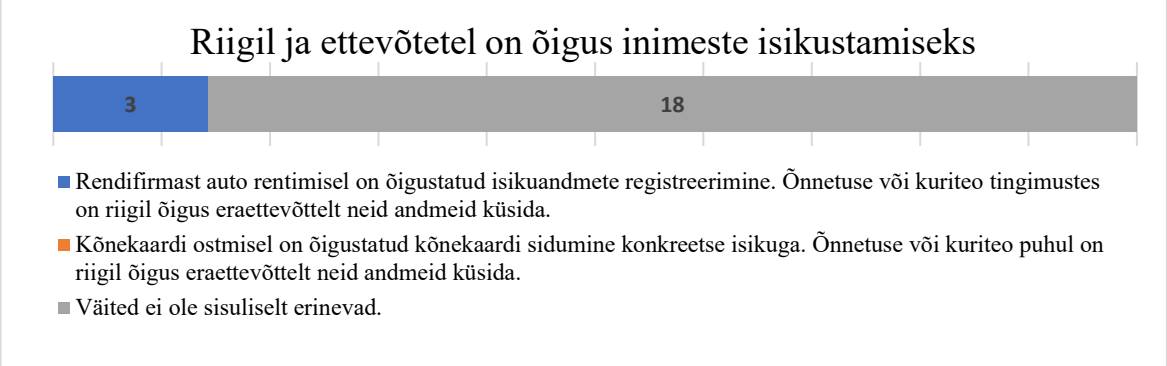
Hegellik positsioon peegeldus ka selles, kuidas ametnikud mõtestasid riigi poolseid seaduseid, makse ja muid kohustusi. Vaid ühe vastanu hinnangul avalduvad riigi poolsed seadused vabadustele teatava piiranguna. Seevastu 20 vastanu hinnangul võimaldavad reeglid, seadused ja kohustused avalikke hüvesid, mille toel on võimalik saavutada isiklikku heaolu ja kvaliteeti (joonis 6).

Seega kajastub valdava osa ametnike vastustes konkreetsele küsimusele, et seadus ei avaldu iseeneses mitte hobbesiliku piiranguna, vaid hegelliku kvaliteediga. Analoogset seisukohta peegeldas ka küsimus, mis uuris, kas normide kehtestamisega ettevõtetele piirab riik ettevõtte tegevusvabadust, aitab tagada turvalisust või lisaks turvalisusele ka privaatsust. Seejuures 15 vastanut olid selgel seisukohal, et reeglid lisaks turvalisusele võimaldavad ka privaatsuse kaitset ning üksnes ühe vastanu hinnangul avalduvad nõuded ettevõttevabadusele piiravalt. Ühtlasi uuriti, kas ettevõtetele on õigus riigi poolt sätestada kohustusi pigem ettevõtete turvalisuse ja toimepidevuse vaatest või klientide andmete ja privaatsuse vaatest (joonis 7).



Joonis 7. Eraettevõtetele küberturbereeglite kehtestamise õigustatus.

Mõneti vastuoluliselt ilmnes, et kui eelnevale küsimusele märkisid 15 inimest vastuseks, et nad nõustuvad pigem seisukohaga, et nõuete sätestamine aitab tagada nii ettevõtte turvalisust kui klientide privaatsust, siis kaheksa inimese hinnangul oleks kõige õigustatud seda teha üksnes privaatsuse ja andmete kaitseks. Ehk nõustuti, et nõuete sätestamine võimaldab tagada mõlemaid väärtuseid, kuid õigustatuks peeti peaaegu poolte vastajate poolt nõuete sätestamist privaatsuse kaitsmise kontekstis. Seevastu inimeste isikustamise osas (joonis 8) järeldati, et füüsilises ruumis ja virtuaalses ruumis ehk nt kõnekaardi isikustamise puhul ei



Joonis 8. Riigiametnike hinnang inimeste isikustamise põhjendatusele.

peaks olema erisust. Teisisõnu hindas valdav osa ametnikest, et rendifirmast auto rentimine ja kõnekaardi tarbimine on oma olemuselt sarnased. Siiski oli ühe vastanu hinnang, et see ei ole võrdne. V21: „Kõnekaardi sidumine isikuga võib olla põhjendatud muudel alustel. Võimaliku õnnetuse või kuriteo uurimiseks on nõue ebaproportsionaalne."

Nagu küberkuritegevust iseloomustavas peatükis selgitati, on avaldunud probleem küberkuritegevuse vastase võitluse osas. Selle taustal uuriti, kas riigiametnikud nõustuvad demokraatlikus ühiskonnas välja kujunenud põhimõttega, et kõikidel inimestel on õigus nende õiguste rikkumise korral riigi poolsele kaitsele? 20 ametnikku nõustusid selle põhimõttega ning ühe hinnangul ei pruugi see nii olla, mis kajastub ka alljärgnevas selgitused, mille vastaja andis (V19).

- V1: „Isegi siis, kui inimene on ise õiguskorda rikkunud, tuleb tagada tema inimõiguste kaitstus, sest see on väärtus, millel rajaneb muu riigikorraldus."
- V24: „Jah, kuid legaliteedi põhimõte avaldab mõju õiguskaitseasutuste koormusele ja tasub analüüsida, kas selles võtmes oleks vajalik muutus – nt prioriteetsusel põhinev või muul kriminaalteabel põhinev otsuste tegemine, kas algatada kriminaalmenetlus või mitte (praegu ainult teatud erandid lubatud)."
- V19: „Igas aspektis ei pruugi olla õigus riigi abile, eriti mis on seotud karistus ja kriminaalseaduse karistustega."

Nagu küberkuritegevust iseloomustavas peatükis selgitati, on avaldunud probleem küberkuritegevuse vastase võitluse osas. Selle taustal uuriti, kas riik riivab inimesi õiguseid rohkem, kui riik isiku vastu toime pandud õigusrikkumie korral ei suuda adekvaatselt tagada tema õiguste kaitset või kui riik kuriteo lahendamiseks võimalike kahtlusaluste andmeid töötleb. Riigiametnikud olid eranditult seisukohal, et riik rikub inimese õiguseid suuremal määral, kui riik ei suuda õigusrikkujat tabada. Kuigi ühe vastaja hinnangul tundus küsimus mõneti suunav, võimaldab see töö autori hinnangul tuua väga lihtsakoelise näite kaasaegsest probleemist.

Kui fundamentaalsel tasemel on privaatsus ja turvalisus omavahel konfliktis ning riik, implementeerides kaasaegseid õiguskaitsetehnoloogiaid olemuslikult privaatsust ja teisi vabadusi õõnestavad, rikub riik igal juhul inimese õiguseid. Eesti riigiametnike hinnang

lükkab selle käsitluse mõneti ümber, kuid on ka neid, kelle vastuste põhjal eelnimetatud näide avaldub.

Ühtlasi uuriti ametnike seisukohti, millistel tingimustel tuleks või oleks võimalik teha erandeid riigi poolsele kohustusele tagada kõigi õiguste kaitse. Kuigi 20 vastanu hinnangul kõikidel isikutele selline kaitse tuleks võimaldada, avaldus, et kuue ametniku hinnangul peaks riik küberkuritegevuse paljususes vähem prioriseerima kergemaid rikkumisi ning üheksa vastanu hinnangul seda teha ei tuleks. Kuus ametnikku selgitasid oma seisukohti erinevalt ning kommentaaride põhjal toetati pigem tasakaalustatud lähenemist:

- V1: „Ilmselt tuleb prioriteete seada, aga ka leida tasakaal nende lahenduste vahel. Ühtki kuriteo liiki ei saa tähelepanauta jätta – tõenäoliselt nendest valdkondadest kasvaks välja uued suured probleemid, seda enam et süütegude toimepanemiseks kasutatakse ka küberruumi.“
- V11: „Siinkohal sõltub, mida lugeda kergemaks rikkumiseks. On oht, et aja jooksul see "kergema rikkumise" lävend on järjest kasvab ning see, mis kunagi oli tabu, ei pruugi ühel hetkel enam olla. Seega võtmekoht on leida tasakaal.“
- V17: (…), kui ressursse napib, peaks mõlemal juhul prioriseerima raskemaid rikkumisi.“
- V23: „Kergemate rikkumiste menetlemata jätmine mõjutab oluliselt keskmise kodaniku usaldusväärsust riigi suhtes.“
- V25: „Toimiva õiguskaitsesüsteemi üks alustalasid on see, et kõiki kuritegusid tuleb lahendada, olenemata kurjategijast, kuriteo subjektist või kuriteo raskusastmest. Teatud prioriteedid aga paratamatult on.“

Seega avaldub ka ametnike sõnul mõneti ressursi probleem kõiki kergemaid rikkumisi küberrumis tagada, kuid samas ilmestati, et see võib tõepoolest vahendada keskmise inimese usaldust riiki. Üks vastanu mainis ka „katkiste aknate teooriat“ (ingl *Broken windows theory*), mille kohaselt suutmatus inimestele kaitset pakkuda võib soodustada kuritegevuse toimepanekut (vt nt Chapell et al. 2010, vt ka Akers 1990; Mann et al. 2016). See on väga asjakohane märkus, kuivõrd see argumenteerib mõneti hobbesiliku konflikti poolt, mis on eelduseks, et riik saaks seaduseid ja reegleid kehtestama hakates seda korratust likvideerima hakata.

Küberkuritegevuse probleemsusest ajendatult uuriti ka ametnike seisukohti, kes peaks nende hinnangul uute avalduvate ohtudega ühiskonnas enim kohanema. Kui 9 vastanut leidsid selgelt, et see peaks olema riik, siis ülejäänud 12 argumenteerisid, et see peaks olema terviklik ühiskondlik pingutus. Kuigi see iseloomustab mõneti NPMi ja sellele omast individuaalset vastutust, avaldub siiski keskne riigi rolli olulisus kodanike turvalisuse tagamisel.

- V15: „Riigil tuleb paratamatult tehnoloogia ja õiguse osas ühte sammu käia, sest uuendusi tuleb pidevalt peale.“
- V1: „Kuigi pigem arvan, et siin peaks riik/ korrakaitseasutused kohanema, siis lõppkokkuvõttes on tarvis siiski mõlema poole tegevusi. Mh kodanike teadlikkuse tõstmist, millele riik kindlasti kaasa saab aidata.“
- V20: „Võrdväärselt kohaneda tuleb nii riigil kui kodanikel.“
- V21: „Mõlemad. Ühtpidi ei saa riik teha kõike kodaniku eest ära ja isikud peavad ennast ise tehnoloogiate arengutega kaasnevate ohtudega kursis hoidma, teisalt ei saa ohtude eest kaitsmist / nendega võitlemsit panna ainult kdaniku õlule. Oluline on keskne, süsteemne lähenemine.“

Seevastu avaldub selgelt, et kui ametnikud pidid hindama õiguskaitseasutuste vaatest, kas kõige olulisem on kiirus (NPMilik efektiivsus), suutlikkus (hegellik riigivõimu suutlikkus kodanikke kaitsta), tulemuslikkus (NPMilik statistiline suutlikkus tabada võimalikult palju rikkujaid) või õigulus (ehk hegellik võrdne kohtlemine), avaldus, et kõige olulisemaks peeti suutlikkust ja tulemuslikkust. Järgnes õiglus ning kiirust peeti kõige vähem oluliseks.

Saab üldistada, valdav osa riigiametnikest ei käsitle privaatsust ja turvalisust nullsummana, kui seda neilt otse küsitakse. Samas oligi uurimuse ja küsitluse üks eesmärk tuvastada võimalikke vastuolusid, küsides sarnast küsimust erinevas stiilis ja käsitluses. Samas avaldub ka siin oluline ebakõla privaatsuse riive, vähenemise ja proportsionaalsuse vahel.

3.3. Küberruum vs füüsiline ruum: olemuslik võrdlus

Käesolev peatükk võtab keskmesse küberruumi ja füüsilise ruumi olemusliku võrdluse ning analüüsib teemat teise uurimisküsimuse kontekstis. Nagu eelnevalt selgitatud, on küberkuritegevus tugevas kasvutrendis ning ulatuslikult leviv kuritegevuse vorm, mille sooritamine on ühest küljest muutunud järjest lihtsamaks, kuid küberrünnakud ise avalduvad komplitseeritud ja keeruliste menetlusprotsessidena. Peatükk analüüsib, kuidas avalduvad hobbesilik NPM ja hegellik õigusriiklus küberuumis ning millised praktilised probleemid on küberruumi iseloomu tõttu õiguskaitse valdkonnas tekkinud. Probleemi analüüsitakse riigivõimu positsioonilt ehk riigivõimu laienemise teguritest lähtuvalt, mida iseloomustavad kolm alltoodud omadust. Traditsiooniline euroopalik avalik haldus näeb ette riigi tugevat juhtrolli – riik on keskne toimija ja normide kujundaja, keskne hüvede pakkuja (näiteks kodanike kaitsja) (Dunn & Miller 2007: 347-349) ning keskse regulatiivse raamistiku kujundaja (Osborne 2006: 378). NPMi iseloomustab vastupidiselt riigi keskse juhtrolli vähenemine ehk detsentraliseeritus, riigifunktsioonide üleandmine erasektorile ning reguleerituse vähenemine (Samier 2001: 204).

Esiteks avaldub küberruumis traditsioonilise tegutsemise piiranguna asjaolu, et küberruum ei ole riikide poolt koordineeritud ega kujundatud. Castells (2000) prognoosis kaks kümnendit tagasi, et tehnoloogia arenemisel väheneb suveräänsete riikide roll. Algselt loodud nn „testkeskkonna“ ja „tööriistana“ domineerisid internetis „euroopaliku avaliku halduse“ põhimõtted (Curran 2009: 32). Seevastu 1990. aastate tehnoloogiarevolutsioon võimaldas lisaks riikidele ka ulatuslikku indiviidide tegevust virtuaalmaailmas ning täna saab Castelli väidet üsna ühemõtteliselt kinnitada. Internetti haldavad erinevad detsentraliseeritud sotsiaalsed võrgustikud (Parti 2011; Williams 2009: 468) ja ettevõtted (Giacomello 2005: 5-7). Sotsiaalmeediaplatvormid, digitaalsed suhtluslahendused jms on erasektori ettevõtete innovaatiliste projektide, mitte riikide töö tulemus. Seega on internetis toimuvad arengud suunatud ja initsieeritud suuresti erasektori ja aktiivsete kodanikerühmituste poolt. Samas on internet võimaldanud traditsioonilisest oluliselt erineva konteksti – üleilmsuse – teket. Interneti abiga on erinevate suurkorporatsioonide (nt Facebook, Google) pakutav teenus globaalse ulatusega. Seevastu virtuaalruumi globaalne iseloom on juurpõhjuseks, miks suveräänsetel riikidel ei ole tänapäevaste infovoogude

juures võimalik virtuaalruumi ega selles toimuvat täielikult kontrollida (Erikkson & Giacomello 2006: 224). Seetõttu esitavad küberohud „väljakutse riigi seesmisele suveräänsusele ehk suutlikkusele kontrollida enda territooriumit ja inimeste tegevust sellel territooriumil“ (Erikkson & Giocomello 2006: 227).

Kuivõrd virtuaalruumi juhivad ja haldavad erinevad sotsiaalsed grupid, on nad ühtlasi ka väärtuste kujundajateks.. Samuti on jäänud virtuaalruumi oluliseks väärtuseks tegevusvabadus, mida omasid interneti algsed kujundajad (Curran 2009: 19). Kuivõrd küberruumi nähti kui seni suurimat teenust, kujundasid seda NPMile omased turupõhimõtted (Curran 2009: 20). Interneti loojate vabadusel ja isikupõhisusel rajanev lähenemine võib olla põhjuseks, miks interneti üheks peamiseks väärtuseks on kujunenud anonüümsus (Berman & Mulligan 1999: 558-563). Osaliselt on anonüümsus küberruumi sisse ehitatud – erinevates võrgustikes puudub vahetu füüsiline kontakt ja tugev kontroll registreeritavate kasutajakontode üle. Küberkuritegevust iseloomustavas peatükis selgitati, et internetis pakubpalju meetodeid oma tegevuste varjamiseks ja umbisikustamiseks. Võrdlusena füüsilises ruumis on anonüümsus kujunenud pigem erandiks, mis on seega oluline põhimõtteline erisus. Uurimistöö raames Eesti riigiametnike seas läbi viidud küsitluse vastused aitavad eelmainitut kinnitada. Vastajate hinnangul oli küberruumis enim tajutav tasuta ja piiramatu informatsioon, seejärel tegevusvabadus, anonüümsus ja privaatsus ning vähim tajutavaks hindasid vastajad ohutut keskkonda. Arvestades, et küberruumi areng ja kujundamine on toimunud detsentraalselt ja eriti erasektori arengutuules, võib seda näha ühe, kuid mitte kindlasti ainsa ega ammendava põhjusena, miks riigid ei suuda virtuaalset territooriumi füüsilise ruumiga võrreldes analoogselt kontrollida.

Suutmatus virtuaalset territooriumi kontrollida võib aga esitada riigile olulisi väljakutseid enda jõu kehtestamiseks ning seeläbi ka kodanike kaitsmiseks. Selle tulemusel võib väheneda küberruumis ka riigi keskne roll hüvede pakkumisel. Traditsiooniliselt on see ühtlasi üheks nn läbikukkunud riigi tunnuseks (Jackson 1993; Krasner 2004). Suveräänse riigi suutmatus end globaalses küberruumis kehtestada erineb oluliselt riigi seesmisest toimimise loogikast. Nagu viidatud, siis küberruum on globaalne keskkond. Seeläbi on riigid küberruumis ka üksteisega vahetus ühenduses, mis omakorda võimaldab panna kuritegu virtuaalselt toime tuhandete kilomeetrite kauguselt. Kuivõrd küberkuritegevus on piiriülene,

avaldub varasemast oluliselt erinevana jurisdiktsiooni küsimus – kurjategija paikneb mujal. See on tekitanud olulisi õiguslikke probleeme kuritegevuse menetlemisel ning tõendite hankimisel (Blažić & Klobućar 2020). Veelgi olulisemaks tehnoloogiajastule iseloomulikuks trendiks on aga asjaolu, et suur osa virtuaalsete kuritegude lahendamisest on sõltuv teisest riigist ehk suveräänist. Traditsioonilises rahvusvahelises riigivalitsemise süsteemis ei saa üks riik sundida teist, rääkimata sealsetest ettevõtetest, vahetult ennast aitama, sest riigid on rahvusvahelisel tasandil võrdsed. Seetõttu avaldubki jõumonopoli niinimetatud jõustamise lünk (ingl *enforcement gap*) (Eoyang et al. 2018). Kokkuvõtlikult, kuivõrd riigid ei saa küberruumis traditsioonilisel viisil oma riiklikke reegleid jõustada (Parti 2011: 667), on riikide traditsiooniliste ülesannete täitmine virtuaalses keskkonnas raskendatud (Berman & Mulligan 1999: 555). Seetõttu võib küberruumi globaliseeritust ja detsentraalsust pidada oluliseks põhjuseks, mis kontinentaalse avaliku halduse süsteemi rakendamist takistab.

Arvestades, et virtuaalruumi on kujundanud suurel määral erasektor, on ilmselt loogiline tagajärg, et erasektor on omandanudolulise rolli ka inimeste turvalisuse tagamisel. Samuti on oluliseks peetud inimese enda järjest suuremat vastutust oma turvalisuse ja heaolu tagamisel küberruumis (Lambert 2020), mis peegeldab NPMilikku isemajandamist (ingl *self governance*) (Dunn & Miller 2007: 247). Ilmselgete näidetena on võimalik tuua arvutite turvatarkvara ja küberturbelahendusi pakkuvaid eraettevõtteid ja turvameeskondi, kes teisi ettevõtteid, nende töötajaid ja tundlikku teavet ohtude eest kaitsma peaksid. Samuti pakub erasektor anonüümsust võimaldavaid ühendusi, et üksikisikuid võimalike kurjategijate eest kaitsta. Samuti võib riikide suutmatus küberruumis korda tagada avalduda selles, et võib täheldada kolmandate osapoolte tekkimist, kes riigi asemel küberruumis korda püüavad tagada (Yar 2010; Button 2020).

Elanikkonna võimalik nõudluse suurenemine virtuaalse turvalisuse järele on tekitanud õiguskaitse erastamise (ingl *privatization*) nähtuse (Yar 2010: 552-555). Sellest lähtuvalt argumenteerib Yar, et inimesed muutuvad turvalisuse klientideks ja väheneb traditsioonilise ühiskondliku lepingu roll (Yar 2010: 552-553). Drozdova (2001) kirjeldatud kaitsvad ehk ennetavad meetmed on seega paljuski tagatud erasektori poolt, kuid reageerivad meetmed valdavalt endiselt riigi poolt.

Mõningane turvalisuse erastamise trend peegeldub ka Eesti riigiametnike vastustest. Kuigi 13 vastanut hindas, et riigipoolne inimeste õiguste kaitse on igaühe õigus, nagu on sätestatud ka näiteks Eesti Vabariigi põhiseaduses, mõtestas viis vastanut riigipoolset inimeste õiguste kaitsmist teenusena ning kolm vastanut hübriidsena ehk kombinatsioonina mõlemast. Näiteks iseloomustati:

- V25: „Õiguste kaitse peaks olema igaühe õigus, et oleks tagatud võrdne kaitse erineva majandusliku taustaga isikutele. Õiguste (sh põhiõiguste) kaitse ei peaks olema sõltuv isiku majanduslikust seisust."
- V11: „Kombinatsioon mõlemast - kodanikel on õigus, et tema õigused oleksid kaitstud, kuid tihti peale toimub selle tagamine teenuse põhiselt (osutab seda siis kas riik ise või erasektor või keegi kolmas)."
- V23: „Võimalused kodanike õiguste kaitse mõtestamiseks on laiemad. Näiteks võib seda näha ka kohustusena. Põhiseaduse kohaselt olekski võimalik seda ka läbi kohustuse defineerida - kohustuste kogum, mis tuleneb teiste kaaselanike õiguste tagamise vajadusest."

Eelneva küsimusega haakub mõneti loogiliselt 16 küsitluses osalenu vastus, et nad ei oleks valmis õiguskaitseasutuste teenuse eest tasuma (kuivõrd hinnati, et läbi maksude see juba on tasutud ning samuti hinnati, et see täiendav tasustamine tekitaks inimeste ebavõrdse kohtlemise ning „tarbimiskultuuri"). Ainult üks vastanu oleks nõus täiendavalt teenuse eest maksma ning nelja vastanu hinnangul esinevad teatud juhud, kus tasu kehtestamine võiks olla mõistlik, kuid ei täpsustanud seda täpsemalt. Siiski selgus vastuste kommentaaridest, et üldine õiguskaitse peaks olema kõikidele võrdselt kättesaadav.

Küsitluses osalenud riigiametnike hinnangul peaks „jõumonopoli" omama siiski valdavalt riik. Ükski vastanutest ei väitnud selgelt, et erasektori ettevõtetel võiks olla riigivõimuga analoogsed õiguslikud pädevused. Üheksa vastanut hindas, et see ei peaks nii olema ning 12 vastanu hinnangul on teatud funktsioonid, mida riigi asemel võiks tagada ka erasektor (nt kergemad rikkumised nagu plekimõlkimised ja piletita reisijad, ka turvafirmade tegutsemine avalikel üritustel ja mainiti ka küberkuritegevust). Ka riigiametnike vastustest ilmnes erinev arusaam ja nägemus riigi rollist tänapäevases ühiskonnas turvalisuse tagamisel. Isegi juhul, kui vastajad pooldasid teatud pädevuste üleviimist avalikult sektorilt erasektorile, ei

pooldanud valdav osa vastanutest kommentaaride põhjal erasektorile riigivõimuga analoogsete pädevuste andmist.

- V1: „Rollid, mida riik ise ei suuda või ei soovi ise vajalikus mahus täita, ning mis ühiskondliku õigluse tagamise aspektis ei pea olema riigi enda täidetavad. Plekimõlkimised on hea näide. Ilmselt selliseid ülesandeid ei ole väga palju.“
- V23: „Üldine avaliku korra tagamise pädevuse jaotus ka näiteks turvaettevõtjatega on täiesti kaalumist väärt mõte. Mõlemi puhul on eelduseks kindlasti täiendav koolitus ja vastav väljaõpe. Mõeldav oleks kindlasti ka teatud õigusrikkumiste osas erasektori kaasamine.“
- V17: „Andmete analüüsimine kuritegude lahendamiseks võiks konfidentsiaalsuse lepinguga olla isegi mõistlik. Samas ilmselt jälitusõiguseid ja muid teenuseid, mis oluliselt riivavad isiku eraelulist või füüsilist puutumatust (...) ei ole riik valmis, vähemalt lähiajal, üle andma.
- V21: „Digidomeenis võiks seda kaaluda. Oluline lahendada enne küsimus, kes kontrollib siis erasektorit.“
- V7: „Nt küberkuritegudes, kus võib erasektori pädevus olla kõrgem kui politseis.“
- V28: „Väga piiratud ulatuses. Pigem jõu kasutamisega seonduvas osas. Isikuandmete töötlemisega seonduv peaks olema minimaalne või välistatud.“

Kolmanda aspektina käsitleb uurimus NPMi ja kontinentaalse avaliku halduse ja riigivõimu jõustamise kontekstis seadusandlust. Kuigi seadustik kehtib igas riigis ning reguleerib sealseid tingimusi, võib juba uurimuse eelnevates lõikudes kaudselt probleemi täheldada – küberruumi ülesehitusest tingituna on riikidel end keeruline jõustada. Kas peamine probleem avaldub aga „jõustamise lüngas“ või ebapiisavas reguleerituses? Sõltumata füüsilise maailma seadustest on argumenteeritud, et virtuaalmaailm ei ole reguleeritud samadel alustel (vt nt Tabansky 2012; Brown 2015: 61; Malik 2018; Liaropoulos 2019: 286). Antud hinnangut kinnitasid ka kõik 21 küsitlusele vastanud riigiametnikku. Muuhulgas iseloomustati, et virtuaalruumis tegutsemiseks on väga palju „halli ala“ ning viidati suurkorporatsioonide vähesele vastutusele. Samuti arvati, et dereguleeritus tuleneb küberruumi ebapiisavast mõtestatusest ning esines ka kategoorilisem väide, et küberruum on „suures osas täiesti reguleerimata“. Üks vastaja viitas, et tulevikus võib eeldada järjest

enam ühtlustamist. Sellega seonduvalt hindasid 20 ametnikku, et kurjategijatel on virtuaalses ruumis kindlasti turvalisem tegutseda kui füüsilises keskkonnas, üks vastanu leidis, et nii see siiski pole.

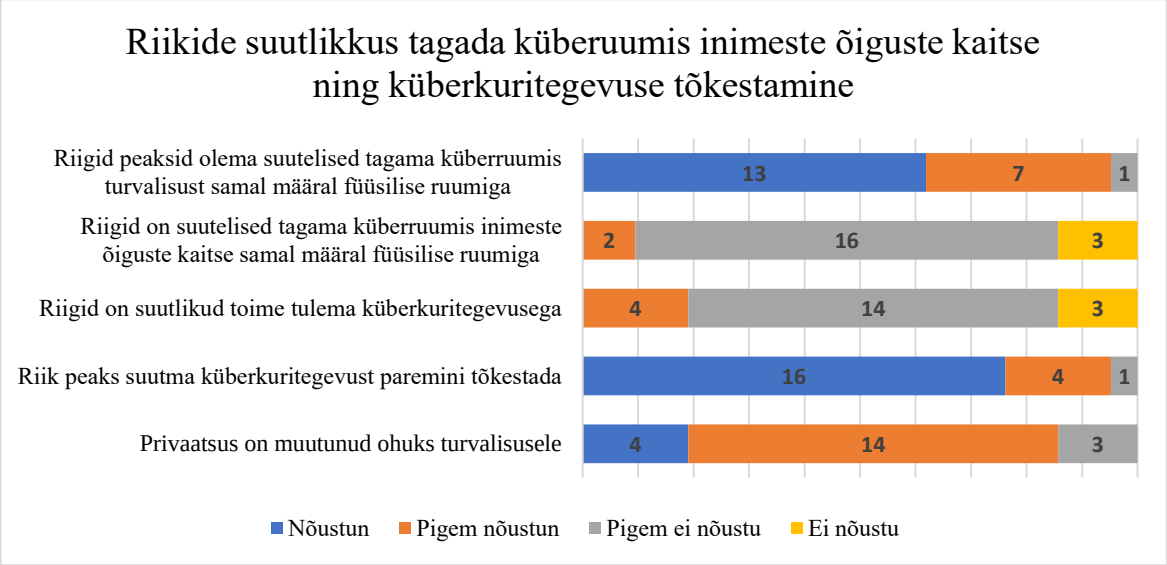
Küsimusele, kas küberruum peaks olema samadel alustel reguleeritud, vastas 13 ametnikku „jah" ning neli ametnikku „ei". Neli ametnikku märkisid, et regulatsioon peaks võimaldama küberruumi eripärade arvestamist. Kolme vastanu hinnangul puudub põhjus erisuse vajaduse järele ning ühe vastaja hinnangul ei ole võrdväärne reguleerimine võimalik.

- V25: „Virtuaalruum on füüsilise maailma osa, seal peaksid kehtima samad reeglid keskkonnast tulenevate erisustega."
- V2: „Virtuaalruumis peaks üldjoontes kehtima sama põhimõte, mis n-ö tavamaailmas. Ehk mis ei ole lubatud päriselus ei peaks olema lubatud ka virtuaalruumis."
- V5: „Võib olla mitte täielikult, aga õigused ja kohustused tuleb tagada mõlemas maailmas."
- V27: „Hea näide on suurkorporatsioonid, kes alluvad mingitele abstraktsetele asukohapõhistele reeglitele ning seni ei ole sihtriigis vastutanud, kuigi seda EL tasandil parasjagu püütakse reguleerida, on vastukaja olnud väga suur."
- V15: „Kas just analoogselt, kuid võiks olla rohkem reguleeritud."
- V23: „See ei ole võimalik. Füüsiline maailm ja virtuaalruum ei ole võrdväärsed."

Dereguleeritusele või vähemalt selle olemuslikule vajadusele viitavad internetiaktivistid ka ise. John Perry Barlow on väitnud oma kuulsas küberruumi iseseisvuse manifestis (1996), et kuivõrd küberuumis puudub isikul füüsiline keha, konkreetne identiteet ja see on erinevate riikide üleselt killustunud, ei ole võimalik inimest allutada küberruumis ka füüsilisele sunnile. Sarnaselt on küsitud: „mis õigustusega reaalse maailma seadusandlus sekkub sõltumatute kogukondade igapäevastesse tegevustesse virtuaalruumis?" (Parti 2011: 647). Samuti on laiemalt iseloomustatud ka eelnevalt küsitluse vastuses välja toodud suurkorporatsioonide tegevuse probleemi. Vaatamata ulatuslikust ja globaalsest haardest ei ole ettevõtted erinevalt riikidest allutatud rahvusvahelise humanitaarõiguse süsteemile (Hayes et al. 2015: 45). Seega on traditsiooniliselt neile kehtinud asukohariigi seadusandlus, mis tähendab, et kolmandal riigil võib nende suhtes nõudeesitamine kujuneda keeruliseks ja

pikaks protsessiks. Kuigi riigil on võimalik ettevõtet siseriiklike seaduste rikkumise eest trahvida, ei ole võimalik sundida ettevõtet otseselt mingeid riigis sätestatud kohustusi täitma.

Riigiametnikud olid üsna ühesel seisukohal, et kuigi õiguskaitseasutused ei ole täna võimelised inimeste õiguseid virtuaalses ruumis kaitsma samaväärselt füüsilise ruumiga, peaks see siiski olema võimalik. Lisaks oldi seisukohal, et praegustes tingimustes riik pigem ei suuda küberkuritegevusega sammu pidada ning peaks seda tervikuna paremini suutma. Üldiselt nõustuti ka Peter Burgessi väitega, et privaatsus on avaldunud turvalisusele ohuna (joonis 9).

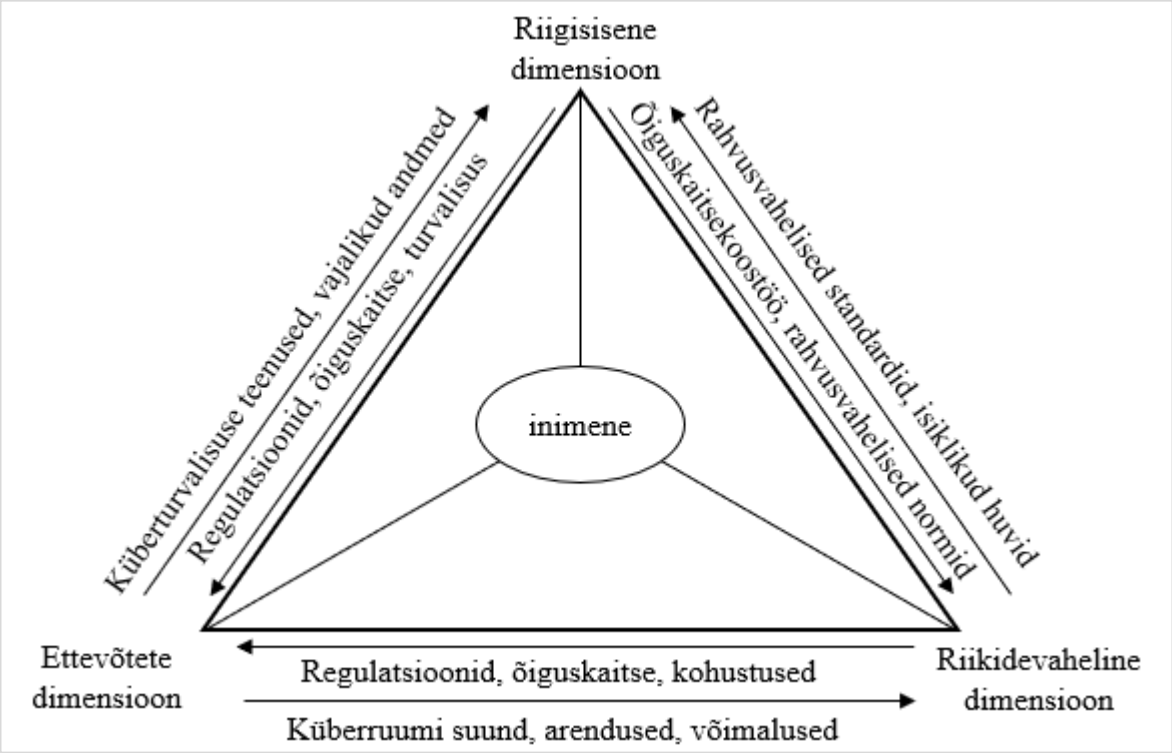


Joonis 9. Riikide suutlikkus tagada küberruumis inimeste õiguste kaitse ning küberkuritegevuse tõkestamine.

Küberruumi reguleerimise probleem võib tuleneda ka asjaolust, et rahvusvahelisel tasandil on riigid teatud küsimustes väga erinevalt meelestatud. Näiteks valitseb suur arvamuste lahknevus selles osas, kas ja mil määral rahvusvaheline õigus üldse küberruumile kohaldub (Schmitt 2017: 21-24). Ühtset läbivat seisukohta ei ole selle osas ka Euroopa Liidus (Komisjon 2020b: 21). Rahvusvahelisel tasandil on erimeelsus ka küberkuritegevuse piiritlemise (Brown 2015) ja küberruumis vastutustundliku käitumise osas (vt Schmitt 2017: 79-157). Vastutustundliku käitumise tagamiseks on seaduste asemel algatatud erinevaid vabatahtlikke initsiatiive (vt Peters & Jordan 2019: 500-501) ning püütud sätestada ühiseid rahvusvahelisi norme ja väärtusi (Euroopa Komisjon 2020b: 21; Williams 2009: 472). Kuivõrd kodanikel, kogukondadel ja riikidel on olnud ja on siiani erinevad nägemused ja

seisukohad küberruumi reguleerimisest, on küberruumi puudutavates põhimõtetes kokku leppida valdavalt samameelsete riikide koostöös. Samas on jõutud järeldusele, et sageli ei ole killustatud ja abstraktsed mehhanismid suutnud omaeesmärke täita (Peters & Jordan 2019: 499-500).

Joonisel 10 on koondatud eelnevalt selgitatud asjaolud, mis küberruumi tingimustes on traditsioonilisele riikide tegevusele takistuseks saanud. Oluline on näha kesksel kohal inimest, kellel on küberruumist tuleneva ulatusliku vabaduse ja võimaluse tõttu võimalik mõjutada nii ettevõtteid, riike kui ka teisi inimesi. Samas riik on küberkuritegevuse lahendamisel väga tugevalt sõltuv erasektorist, kellelt on vaja saada inimesi isikustavaid ja rünnakut iseloomustavaid andmeid kurjategijate tabamiseks.



Joonis 10. Virtuaalruumi globaalne 3-dimensiooniline haldus (vt Bigo 2012: 29-30, autori poolt muudetud ja täiendatud).

Joonis x....Virtuaalruumi globaalne 3-dimensiooniline haldus (vt Bigo 2012: 29-30, autori muudetud ja täiendatud).

Probleemiks on riigi ja seaduse territoriaalsus – kriminaalõiguse rakendamine ning kuritegevusevastane võitlus on olnud siseriiklik protsess, mis tehnoloogia tõttu on muutunud üha piiriülesemaks. Seetõttu on inimesed muutunud turvalisuse tagamisel sõltuvamaks mitte

üksnes enda riigist, vaid ka teistest riikidest ja erasektorist. See iseloomustab mõnevõrra hobbesilikku loomuseisundit, sest riigi jõumonopol ei ole turvalisuse tagamiseks piisav, vaid muu hulgas sõltuv teiste riikide ja ettevõtete koostööst ehk lisandunud on rahvusvaheline ja ettevõtete dimensioon. Lisaks on oluline, et näiteks suutmatusel hea viirusetõrjeprogrammi eest tasuda muutub turvalisuse saavutamine inimesele mõneti teenuspõhiseks ehk väheneb senine võrdsuse põhimõte.

Õigusaktide mittevastavus digitaalsete eripäradega on toonud esile õiguse, riigivõimu ja ka käitumisnormide jõustamise probleemi küberruumis (Sundquist 2012; Tabansky 2012; Peters & Jordan 2019). Seega saab probleemi näha nii küberruumi reguleerimatuses, aga ka küberruumi iseloomust tulenevalt riikide puudulikus võimekuses erinevaid regulatsioone tulemuslikult jõustada. Seetõttu on ka loogiline, miks privaatsuse ja turvalisuse dilemma küberruumis nii teravalt avaldub. Virtuaalsete ohtude tõttu on pikaaegne *laissez faire* põhimõte küberruumis muutumas, kuivõrd riigid püüavad seal järjest enam oma territoriaalsust ja suveräänsust kohaldada (Lewis et al. 2017: 31). Avalikkuse silmis on aga taolised püüded seni dereguleeritud keskkonda tagantjärele reguleerida tugevalt piiravad. Ka Eesti meedias on argumenteeritud, et virtuaalruumi reguleerimine mõjub äärmiselt piiravana senistele interneti ulatuslikele vabadustele ja inimeste privaatsusele (vt Pau 2020; Laks 2020).

Riigiteoreetiliselt on seda võimalik seletada läbi hobbesiliku käsitluse. Rein Toomla on selgitanud, et Hobbesi kohaselt on riiki lagundav olukord, kus riik ei kasuta oma võimu piisavalt. Kui riik jõustab võimu üksnes hädaolukordades, võib avalikkus hakata seda tõlgendama ja tunnetama kui riigivõimu paljusust ja liigset sekkumist (Toomla 1990: 47). Seetõttu on küberruumi senisest enamat reguleerimist võimalik näha kontinentaalse avaliku halduse ja NPMi omavahelise põrkumisena, mis avaldub konfliktina vabaduste mõtestamises.

Eeltoodud argumentatsiooni põhjal jõuab uurimistöö esimese küsimuse vastusena järeldusele, et küberruumi areng ilma keskse kontrolli ning koordineerituseta on võimaldunud avalduda mitmetel NPMile omastel loogikatel. Ühegi konkreetse riigi ega regiooni küberpoliitiline lähenemine, olenemata kui tahes laiapõhjaline ja erinevaid valdkondi ning tegureid arvestav, ei saa iseseisvalt olla läbinisti toimiv, kuivõrd küberruumis

sõltutakse turvalisuse tagamisel väga paljudest teistest riikidest ning ettevõtetest. Seega avaldub riikide suutmatuses jõumonopoli rakendada ka mõnetine hobbesilik anarhilisus. Küberruumi kiire arengu ning laialdase leviku tõttu on see probleem muutunud igapäevasemaks ning tõsisemaks. See tuleneb loogilisest paradoksist – ühest küljest tegutsevad riigid jätkuvalt siseriiklikul tasandil, kuid teisest küljest on kõik riigid osa globaalsest virtuaalruumist, mis on muutunud suurimaks ja enim läbipõimunud supranatsionaalseks instantsiks. Seega võib kuritegevuse igapäevases piiriülestumises täheldada võrreldes küberruumi-eelse ajaga olulist põhimõttelist muutust. Küberruum on muutnud riigi traditsioonilist jõumonopoli loogikat ning riikide praktilist suutlikkust oma kodanikke ohtude eest kaitsta. Kuigi ka kodanike endi vastutus oma turvalisuse tagamisel on suurenenud, on õiguslikult kohustus inimeste turvalisuse tagamise eest asetatud riigile, mis omakorda on tõstnud päevakorrale loonud võimaluse mitmed eetilised probleemid seoses riigi tegevustega seni reguleerimata keskkonnas.

3.4. Privaatsus ja turvalisus: Euroopa Liidu õigusloome paradoks

Euroopa Liidu õigusruum on privaatsuse ja turvalisuse mõtestamisel hädavajalik, kuivõrd õigussüsteemi kaudu toimub lubatu ja lubamatu defineerimine ning riigivõimu volituste ja piirangute defineerimine. Ehk õigussüsteem on fundamentaalne kontekst privaatsuse ja turvalisuse omavahelise suhte mõtestamisel. EL orienteeritus privaatsuse ja isikuandmete kaitsele on silmnähtav. Andmekaitsereformi ja isikuandmete kaitse üldmäärusega (GDPR) on loodud raamistik, millele tõenäoliselt ei leidu võrdväärset mudelit üheski teises ühenduses või riigis. Sellegi poolest on levinud üsna jõuline akadeemiline hinnang, et Euroopas kehtiv õigusruum ei suuda õigusliku ebaselguse tõttu inimeste privaatsust ja andmete kaitset piisavalt tagada (vt Aquilina 2010; Balboni & Pelino 2013; Milaj 2015; Vedaschi & Lubello 2015; Jasserand 2018). Käesolev peatükk uurib erinevate autorite näidetele tuginedes, millel selline hinnang põhineb ning milles avaldub privaatsuse ja turvalisuse omavaheline konflikt kaasaegses EL õiguses.

Esiteks avaldub privaatsusega seonduv probleem terminoloogilises õiguslikus ülesehituses, mida lühidalt kirjeldati ka töö teoreetilises osas privaatsuse ja turvalisuse mõtestamisel. EL põhiõiguste raamdokumendid ei defineeri ega anna ka kaudset selgitust õiguslikus

konstruktsioonis kajastuvatele mõistetele. EIÕK artikkel 8 sätestab, et privaatsuse riive on lubatud muuhulgas „riigi julgeoleku“ (ingl *national security*), „ühiskondliku turvalisuse“ (ingl *public safety*), „riigi majandusliku heaolu“ (ingl *economic well-being of the country*) või „korratuse“ ja „kuritegevuse“ ärahoidmiseks. Riik defineerib õigussüsteemi kaudu üsna selgelt, mis on ebaseaduslik, kuigi riigiti võivad erineda kuriteoliigid ning nende karistusmäärad. Samas eeltoodud mõistete kohta dokumentides selgitus puudub – ei selgu, mis on ühiskondlik turvalisus või korratus ning kuidas need omavahel suhestuvad.

Ühtlasi on puudulikult mõtestatud ka muude, raamdokumentide väliste, kuid nendega siiski olulisel määral seotud mõisted. EL tasandil ei ole üheselt piiritletud „rasket kuritegevust“ (ingl *serious crime*), „pädevat asutust“ (ingl *competent authority*) (Vedaschi ja Lubello 2015: 30) ega „avalikku korda“ (ingl *public order*) (Caruana 2018: 255). Seetõttu võivad need riigiti ja sõltuvalt ühiskonna võimalikust ohutajust olla erinevalt mõtestatud ning potentsiaalselt avaldub see ka selles, mida inimesed on turvalisuse nimel valmis aktsepteerima (Bug & Bukow 2017) ning kuidas privaatsust ja selle riivet tajutakse (Budak et al. 2017). Kuivõrd on võimalik, et riigid sisustavad mõisteid erinevalt, võimaldab see kriitikat, et põhiõiguste riivamise alused ei ole selgelt välja toodud (vt nt De Hert 2005; Vedachi & Lubello 2015). Mõistetega seoses avaldub huvitav vastuolu – kui ühelt poolt on leitud, et privaatsust ei ole vaja ammendavalt defineerida (Pretty vs Ühendkuningriik 2002, § 61; Niemetz vs Saksamaa 1992, § 29), siis privaatsust ja põhiõiguste riivet sisaldav regulatsioon peaks olema võimalikult detailne (De Hert 2005: 79).

Teiseks on viidatud Euroopa Liidu õigusaktide üldisele puudulikule kvaliteedile, mis väljendub näiteks õiguslikus ebaselguses. On argumenteeritud, et turvalisust ja jälgimistehnoloogiaid reguleerivad õigusaktid ei ole taganud vajalikku õigusselgust ning põhiõiguste riive proportsionaalsust (vt Aquilina 2010; Balboni & Pelino 2013; Milaj 2015; Vedaschi & Lubello 2015; Jasserand 2018). Neid väiteid saab illustreeridamõne õigusliku analüüsi järelduste abil. Näiteks on analüüsitud, et õiguskaitsedirektiiv ((EL) 2016/680) ei sisalda piisavalt politsei poolt uuritavate kahtlusaluste privaatsust ja andmekaitset tagavaid garantiisid (Jasserand 2018). Enamgi veel, kuivõrd GDPRi ja õiguskaitsedirektiivi võrdlusel on järelevalve ja pädevused sätestatud äärmiselt erinevalt (Caruana 2019: 259), tekitab järelevalve teostamine erinevate ebaselgete mõistete kontekstis juba olemuslikult teoreetilise

probleemi. Kui erinevad riigid rakendavad ja tõlgendavad õigusakte erinevalt, muutub probleemseks ka järelevalve teostamine ja järelevalve ühetaolisus. Lisaks on leitud, et erinevate isikustamata andmehulkade analüüsimine võib, aga ei pruugi alati isikuandmeteks kvalifitseeruda (Drewer & Miladinova 2017: 306), mis andmete töötlemise ja järelevalve mõttes võib tõlgenduste lahknevuse tõttu viia väga erinevate järeldusteni.

Eelkirjeldatud õiguslikku ebaselgust või puudulikku kvaliteeti ilmestab ka asjaolu, et EL õigusaktide rakendamise ja tõlgendamise osas on väga vajalikuks osutunud mahukad selgitavad dokumendid (Wessel 2012: 354). Euroopa Andmekaitsenõukogu koostas 20-leheküljelise analüüsi, et selgitada, kuidas toimub järelevalveasutuste sünergia e-privaatsuse direktiivi (2002/58/EÜ) ja GDPR vahel elektroonilist sidet puudutavates küsimustes (EDPB 2019). Seega saab kinnitada, et tõepoolest viitab õigusaktide selgitamisvajadus osaliselt kindlasti normide puudulikule kvaliteedile ja ebapiisavale üheselt mõistetavusele.

Kuivõrd käesolev uurimistöö keskendub praktilise näitena sideandmete säilitamisele, tuleb ilmestada ka Euroopa Liidu Kohtu poolset kriitikat aastatel 2005-2014 kehtinud EL sideandmete direktiivi suhtes, mida on ulatuslikult kritiseeritud ka teaduskirjanduses (vt Milaj 2015; Ochodec 2018; Tracol 2020). ELK viitas 2014. aasta kohtuotsuses *Digital Rights Ireland* (liidetud kohtuasi C-293/12 ja C-594/12), et EL sideandmete direktiiv ei piiritlenud mingil viisil isikute ringi, kelle andmeid sideteenuse osutajad säilitama peavad (§ 57). Samuti sätestati, et direktiiv ei nõua isiku suhtes „mingi seose olemasolu säilitatavate andmete ja ohu vahel avalikule julgeolekule“ (§ 59). Direktiiv ei sisaldanud kriteeriume, mis suunaksid ametiasutusi andmeid eesmärgipäraselt kasutama (§ 60) ehk andmetele ligipääsu tingimusi. Samuti piirdus direktiiv üksnes suunisega, et „iga liikmesriik kehtestab menetluse, mida tuleb järgida, ja tingimused, mis peavad olema täidetud säilitatud andmetele juurdepääsu saamiseks vastavalt vajalikkuse ja proportsionaalsuse nõuetele“ (§ 61). Lisaks ei piiranud direktiiv isikute ringi, kes andmetele ligi võivad pääseda (§ 62). Direktiivi kriitikana nähti ka liigset abstraktsust, mis võimaldas liikmesriikidel ise sätestada andmete säilitamise tähtaja kuuest kuust kuni 24 kuuni (§ 64) ning et direktiiv ei sätestanud reegleid põhiõiguste riive ulatuse piiritlemiseks (§ 65). Samuti heideti ette ebapiisavaid kaitsemeetmeid (§ 66), mis uurimistöö teoreetilises ülesehituses väljendub ebapiisava

tasakaalustamisena. Näiteks viidati, et EL direktiiv ei näe koosmõjus teiste õigusaktidega ette teenusepakkujatele piisavaid infoturbemeetmeid isikuandmete kaitsmiseks (§ 67).

Eelnimetatud hinnanguid õigusselguse osas saab pidada kindlasti asjakohasteks, kuid samas avalduvad nad mõneti vastuolulisena EL õiguse aluspõhimõtete suhtes. Euroopa Liidu õiguses on kesksel kohal proportsionaalsus:

> „Vastavalt [proportsionaalsuse] põhimõttele tuleb põhjalikult kontrollida, kas õigusakt on vajalik ja kas muud tegevusvahendid ei oleks piisavalt tõhusad. See tähendab eelkõige, et liiga üksikasjalikele õigusnormidele tuleb eelistada raamregulatsioone, miinimumnõudeid ja korda riiklike eeskirjade vastastikuseks tunnustamiseks ning et ühtlustatud õigusnorme tuleb võimaluse korral vältida.“ (Borchardt 2016: 56)

Euroopa Liidu toimimise leping (ELTL) sätestab artiklis 288, et määrused kohaldatakse kõigile üldiselt ning need on õiguslikult siduvad, kuid direktiiv „jätab vormi ja meetodite valiku selle riigi ametiasutustele“. Kuigi õigusselguse osas võib tõesti nentida, et direktiivide ja määruste erinev sisustamine ei pruugi tagada vajalikul või piisaval määral EL liikmesriikide õiguslikku ühetaolisust, on see olnud EL integratsiooni läbiv loogika. Nimelt on direktiivide eesmärgiks tagada liikmesriikide ühtlasem lähenemine, kuid „säilitada riiklike eripärade mitmekesisus“ (Borchardt 2016: 101). Eeltoodud paragrahvide alusel võib aga järeldada, et just nimelt seda alusloogikat on Euroopa kõrgeim kohus *Digital Rights Irelandi* kohtuasja puhul läbivalt kritiseerinud. Ühtlasi, kui direktiivi loomise ajal, üle 10 aasta varem hinnati seda vähema tehnoloogia levikuga proportsionaalseks, on huvitav, et hinnang tugevalt muutus (*Digital Rights Ireland*, § 69).

Põhjendatud on küsimus, mis võib olla sellise õigusloomelise paradoksi põhjuseks. Või täpsemalt, kuidas on võimalik, et EL demokraatlikus ja pluralistlikus õigusloomeprotsessis koostati õigusakt, mille osas ELK niivõrd palju ja ulatuslikke puudujääke leidis? Siin võib esitada kaks erinevat spekulatsiooni. Esiteks õiguse puudulik kvaliteet, mis on EL mitmetasandilise õigusloomeprotsessi tulem. Teiseks võib tuua sisse avaliku arvamuse mõju ELK otsustele peale Snowdeni avalikustamisi (Loideain 2015).

Esiteks on EL õigusloomeprotsessi defineeritud kui „post-regulatiivset“, mida iseloomustab killustatud õigusloome, mis seisneb erinevate osapoolte läbirääkimistel põhinevale

üldistamisele (Chowdhury & Wessel 2012: 337). Sellist mitmetasandilist seadusloomet on peetud olemuslikult demokraatiat võimestavaks. Liberatore (2007: 124-125) väidab, et Euroopa Liidu seadusloome mitmetasandiline ülesehitus ja paljude osapoolte osalemine õigusruumi kujundamises on loonud demokraatliku keskkonna, milles regulatsioonide kujundamisel ei domineeri üksnes ühe osapoole seisukoht. Seetõttu peaks teoreetiliselt olema kajastatud seadusloomes nii „turvalisust" kui „privaatsust" edendavate kogukondade huvid. Seevastu Chowdhury ja Wessel näevad seda mitmetasandilisust probleemina – „õigusliku ebakindluse suurenemine on taolise killustatuse ja õigusliku ühtsuse puudumise tõttu sellises regulatiivses ruumis loogiliseks tagajärjeks" ning regulatiivse ruumi ebaselgus võib omakorda avaldada negatiivset mõju õigusaktide õigusselgusele tervikuna (Chowdhury & Wessel 2012: 355).

Kuivõrd õigusloomeprotsess on kompromissipõhine (Euroopa Komisjoni avalik konsultatsioon huvigruppidega, õigusakti ettepanek, seejärel Euroopa Komisjoni ja liikemsriikide praktikute- ja ametnikevahelised läbirääkimised ning lõpuks ka politiseeritud triloogide tasand, milles lisandub eelnevatele osapooltele ka Euroopa Parlament) võib pidada õigusaktide üldisust loogiliseks tulemiks. Eelnevatest näidetest ilmneb EL õiguse laiem ja põhimõttelisem probleem – regulatsioonide ebaselgus ja tõlgendatavus võimendab praktilist konflikti õiguskaitse ja andmekaitse vahel. Kuivõrd valdkondi reguleerivad EL tasandil väga mitmed mahukad ja tehnilised, sealhulgas eelnimetatud õigusaktid, saab väita, et õiguslik keskkond on muutumas üha keerulisemaks. See omakorda tingib konflikti õigusaktide mõistmise ja rakendamise osas nii järelevalve kui õiguskaitseasutuste vaatest ja seda liikmesriikide põhiselt. Seega on kujundlikult võimalik argumenteerida, et ELK, kritiseerides direktiivi õiguslikku ebapiisavust, kritiseeris olemuslikult ka EL aluslepingutes sätestatud õiguspõhimõtete ülesehitust.

Teiseks võib tuletada seose ELK otsuste seose avaliku arvamusega. Euroopa Liidu Kohtul ELTL artiklis 267 sätestatust lähtuvalt pädevus tõlgendada aluslepingute põhjal sekundaarseid õigusakte. Lisaks mõjuvõimule kujundada ja suunata õigusaktide rakendamist (vt nt Wasserfallen 2010; Davies 2016; Blauberger & Schmidt 2017) on analüüsitud, et läbi õigusloome tugeva suunamise on ELK omandanud paratamatu pädevuse kujundada ka olulisel määral liidus loodavaid poliitikaid (Wasserfallen 2010: 1129;

Blauberger & Schmidt 2017: 908). Ühtlasi on Gareth Davies (2016: 847) argumenteeritud, et uurimistöös kirjeldatud terminoloogiline üldsõnalisus ja piiritlematus on võimaldanud ELK-l poliitikasse veelgi tugevamalt sekkuda, kuivõrd mõistete ebaselgus võimaldab kohtul neid ise sisustada. Daviese hinnangul on veelgi hämmastavam, et „paljud valdkonna teadlased ega liikmesriigid ei ole sellest asjaolust täielikult teadlikud“ (Davies 2016: 858).

Davies selgitab, et vastupidiselt liikmesriikide põhiseadustele, mis igapäevaselt riikide toimimist ei mõjuta, dikteerib ELK oma pädevuses pidevalt aluslepingute liidu poliitikate toimimist ja näeb ette vajalikud tõlgendused (Davies 2016: 848), mis muudab kohtu justkui „aluslepingute omanikeks“ (Davies 2016: 849). See tähendab, et „kohtulahendeid, mis põhinevad aluslepingute tõlgendamisel, ei ole võimalik kooskõlla viia sekundaarsete õigusaktide abil“ (Blauberger & Schmidt 2017: 913; vt ka Davies 2016: 849). Kuivõrd Euroopa põhiõiguste harta muutus 2009. aastal õiguslikult siduvaks, muutus see ühtlasi aluslepinguks, mille suhtes sideandmete direktiiv 2014. aastal vastuolus olevaks kuulutati. Kaks aastat hiljem, kohtuotsusega C-203/15 ja C-698/15 (*Tele2 Sverige ja Watson jt*) hindas kohus üldise sideandmete säilitamise ehk andmete säilitamise kõikide teenust tarbivate inimeste osas samuti hartaga vastuolus olevaks. Seega saab seda loogikat muuta üksnes harta muutmisega või varasema kohtuotsuse tühistamisega (Szabados 2015: 145), mis ilmestab veelgi enam ELK tugevat rolli liidu õigusloome ja poliitika kujundamisel.

Kuigi eelduslikult objektiivne, on tuvastatud, et ELK on „keskkonnatundlik“. Blauberger et al. (2018) väidavad, et ELK otsused ja põhjendused on korrelatsioonis avaliku arvamuse ja poliitiliste suunistega. Tuvastati, et kohtunikele on rõhutatud näiteks migratsiooniküsimustes nende tehtavate otsuste „poliitilist kaalu“ (Blauberger et al. 2018: 1437). Lisaks on kohtunikud ise osa üldsusest ning seeläbi võib kujuneda nende avalik arvamus ja hinnang nagu igal teisel kaaskodanikul (Blauberger et al. 2018: 1429). Seotust kohtulahendite ja avaliku arvamuse vahel on tuvastatud ka Ameerika Ühendriikide Ülemkohtu puhul (vt nt Blackstone et al. 2008; Clark 2009). Seonduvalt on Lischka (2016) tuvastanud, et avalik debatt privaatsuse ja jälgimise osas elavnes tugevalt peale Snowdeni paljastusi Ühendriikide valitsuse ulatusliku jälgimisprogrammi kohta. Seonduvalt on argumenteeritud, et ELK tugev orienteeritus privaatsusele on Edward Snowdeni vilepuhumise tagajärg (Loideain 2015), mis mure privaatsuse pärast tugevalt avaliku debati keskmesse asetas. Ehk see on üks võimalik

seletus kohtuotsuste ulatuslikule kriitikale sideandmete säilitamise suhtes nii 2014. kui 2016. aasta otsustes.

Hobbesi ja Hegeli käsitluste omavahelise suhte osas võib EL õiguses täheldada huvitavat kontseptsiooni. Vastusena teisele uurimistöö kesksele küsimusele võib väita, et privaatsuse ja turvalisuse omavahelist konflikti on võimalik selgitada kahe äärmiselt erineva riigifilosoofia kokkupõrke läbi. Ühest küljest püütakse Euroopa Liidus tagada inimeste maksimaalset individuaalset vabadust ja tugevat põhiõiguste kaitset, kuid sõltuvalt vabaduse mõtestatusest, eeldab see teoreetiliselt kas hobbesilikku anarhiat ja dereguleeritust või hegellikku riigi keskset rolli nende vabaduste realiseerumise võimaldamisel. Uurimistöö tuvastas, et küberruum omab sarnasusi nii Hobbesi kui NPM käsitlustega. Riigiväline keskkond on tõstatanud vajaduse seda senisest enam reguleerida, mis oma olemuselt satub konflikti seniste ulatuslike vabaduste põhimõttega. Teisisõnu avalduvad regulatsioonid nullsummana kodanlikele õigustele, sh privaatsusele virtuaalruumis. See on huvitav nähtus, kuivõrd väga paljud valdkonnad on isegi hegellikult reguleeritud - näiteks tarbimine, konkurents, ravimid, reklaamid, kalandus, lennundus, tootmine, jäätmepoliitika, kvaliteedinõuded jpm on EL ühisturu kaitse raames reguleeritud, et tagada „vabadusel, turvalisusel ja õigusel“ põhinev liit. Kuigi põhiõiguste kooskõla püütakse saavutada kõikjal, on privaatsus ja andmekaitse reguleeritud oluliselt indiviidikesksemalt, kuid indiviidikesksus ei pruugi tagada põhiõiguste läbivat ja süsteemset kaitset. Seevastu Hegeli argumentatsioonile tuginedes luuakse supranatsionaalsel tasandil ühise reguleerimise kaudu võrdsed alused, standardid, reeglid ja normid, mis omakorda organiseerituse kaudu aitavad tagada ühiskonna kollektiivset heaolu palju enama kui üksnes turvalisusena.

3.5. Sideandmete säilitamine: Euroopa Liidu kohtupraktika mõju kodanike turvalisusele ja privaatsusele

Käesolev peatükk teostab ELK sideandmeid puudutavate kohtulahendite osas õigus-praktilise analüüsi. Esmalt kirjeldab peatükk ELK mõju ja rolli Euroopa Liidu õigusloomes. Seejärel kirjeldatakse sideandmete olemust, nende praktilist väärtust ning analüüsitakse üldiselt kõikide avaldatud kohtulahendite suuniseid. Seejärel analüüsitakse sisuliselt kohtulahendite praktilisi suuniseid sideandmete säilitamiseks ja kasutamiseks. Kõrvutamise

abil on eesmärk tuvastada, milline praktiline ja loogiline probleem õiguskaitseasutustele kohtulahendite suuniste taustal avaldub. Lõpetuseks argumenteeritakse, et küberkuritegevuse puhul ei seisne sideandmete säilitamine üksnes hobbesilikus nullsummas ehk turvalisuse kasvus privaatsuse vähenemise arvelt, vaid peegeldab mõneti ka hegelliku vabaduse kvaliteeti.

Sideandmeid puudutavate kohtulahendite analüüsimiseks on oluline mõista esmalt, millega on tegemist, ning teiseks, milles seisneb nende praktiline väärtus. Sideandmed (ka metaandmed) tekivad erinevate kommunikatsioonitehnoloogiate kasutamisel ettevõtte registritesse, kes konkreetset teenust pakuvad. Üldistatult näitavad need andmed, kes kellega ja millal ühenduses oli, kui kaua, millise vahendiga ning kes on konkreetse telefoninumbri või IP aadressi ehk teenuse reaalne klient ja kasutaja. Internetiühendusega seonduvad andmed on käesoleva töö probleemi taustal peamiseks murekohaks. Metaandmed puudutavad üksnes kommunikatsiooni lähteandmeid, mitte klientide sõnumite ja kõnede sisu. Seevastu tuleb rõhutada, et metaandmete puhul viidatakse ekslikult andmete kogumisele riikide ja valitsuste poolt (vt Loideain 2015: 54). Direktiivi alusel oli kohustus säilitada direktiivi alusel andmeid üksnes eraettevõtetest teenusepakkujad. Siseriikliku õiguse alusel sätestati, millise juriidilise protsessi käigus ja millistel õiguslikel alusel õiguskaitseasutused ehk riik kuritegevuse tõkestamiseks vastavaid andmeid sideettevõtetelt küsida tohivad.

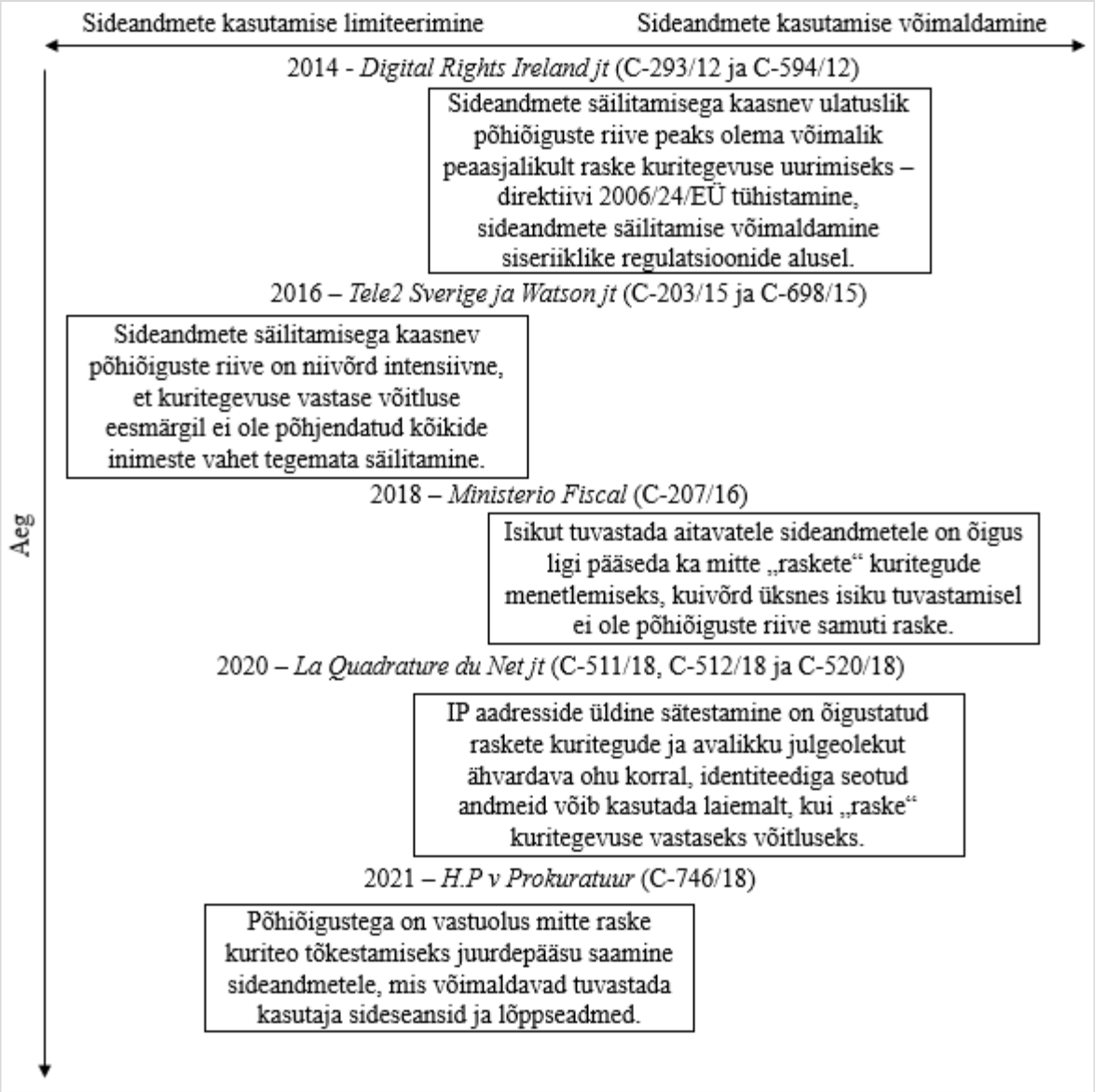
Nagu küberkuritegevust käsitlevas peatükis selgitati, on võrreldes varasemate aastakümnetega kuritegevuse toimepanekul toimunud oluline muutus. Traditsioonilise kuritegevuse puhul esineb inimeste kontakt ja suhtlus vahetult ning kuritegevus „aktina“ leiab aset füüsilises maailmas. Seevastu digitaalne küberkuritegevus, sõltumata oma potentsiaalsetest füüsilistest tagajärgedest, on virtuaalne ning andmepõhine. Seetõttu osutuvad sideandmed tihti ainsateks reaalseteks indikaatoriteks, mille abil on võimalik tuvastada ja isikustada kuriteo toimepanijat, kuid mis olulisem, konkreetset kuritegu läbi isiku seostamise tõendada (Dinant 2004; Kao & Wang 2009; Europol 2019).

> „Need andmed võimaldavad muu hulgas teada, millise isikuga ja millise sidevahendi kaudu abonent või registreeritud kasutaja suhtles, ning teha kindlaks side toimumise aja

ja koha. Need andmed võimaldavad ka teada, kui sageli abonent või registreeritud kasutaja teatud isikutega mingil ajavahemikul suhtles.“ (*Digital Rights Ireland*, §. 26)

Sideandmete olulisust kinnitasid ka kõik 21 küsitlusele vastanud ametnikku: 13 nõustusid ja 8 pigem nõustusid, et sideandmed võimaldavad virtuaalruumis inimeste turvalisuse tõhusamat tagamist. Seega ilmneb, et sideandmete praktiline väärtus seisneb just nimelt selles, mida ELK oma otsuses, aga ka teaduskirjanduses tugevalt kritiseeritakse (vt nt Tracol 2014; Loideain 2015, Milaj 2015).

Järgnevalt esitatakse ülevaatlik joonis abstraktse skaala näol kohtulahendite suunistest sideandmete säilitamisele ja kasutamisele. Skaalale paigutamine toimus kohtulahendite üldist iseloomu ja piiranguid arvestades, lähtuvalt kohtulahendite sisuanalüüsist (vt joonis 11). Kohtulahendite analüüsi tulemusena paigutub sideandmete direktiivi tühistamine (*Digital Rights Ireland jt*) endiselt oluliselt kasutamise võimaldamise poole.



Joonis 11. Sideandmete säilitamise ja kasutamise õiguslik võimaldamine ELK poolt 2014-2021.

Kuigi kohtuotsuses kritiseeriti tugevalt direktiivi ennast ning kohus selle ka tühistas, ei antud tugevat õiguslikku sisendit sideandmete kasutamise või kasutamise keelamise osas. Siiski argumenteeriti, et nende kasutamine saaks olla õigustatud raske kuritegevuse osas (§ 49-51). Seevastu *Tele2 Sverige ja Watson jt* otsusega kuulutati mistahes sideandmete säilitamine põhiõigustega vastuolus olevaks, mis avaldus väga tugeva õigusliku piiranguna (§ 134 lg 1). 2018. aastal omakorda otsustas ELK, et siiski sideandmed võivad olla vajalikud mistahes kuriteo tõkestamiseks (§ 56-58). Seega lahendis *Ministerio Fiscal* leevendati õiguslikku suunist oluliselt. Peaaegu samasugust suunist omas ka lahend *La Quadrature du Net jt* 2020.

aasta oktoobris, andes suunise, et isiku identiteeti peaks saama tuvastada ka kergemate kuritegude puhul (§ 229 lg 1 p 4). Seevastu IP aadresside säilitamine ja kasutamine, mis küberkuritegevuse seisukohalt on rünnaku päritolu ja kasutatud seadme tuvastamiseks äärmiselt olulised, piirati üksnes raske kuritegevuse, riikliku ja avaliku julgeoleku kontekstis (§ 229 lg 1 p 3). 2021. aastal Eestiga seonduva lahendi (*H.K v Prokuratuur*) järelm oli aga taaskord, et lõppkasutaja tuvastamiseks on sideandmete kasutamine õigustatud üksnes raske kuritegevuse puhul (§ 39). Ehk kui lahend *Ministerio Fiscal* võimaldas peale 2016. aastat oluliselt paindlikkuma lähenemist, siis 2020. ja 2021. aasta lahendid üldist õiguslikku suunist taaskord karmistasid.

Eelnevalt esitatud joonise alusel ilmneb, et kohtulahendite üldine sisend on olnud mõneti vastuoluline. ELK kohtupraktika õiguslikku ebaselgust ja tõlgendusruumi on uuringutega tuvastatud nii üldisemalt (vt nt Blauberger & Schmidt 2017: 917), kui ka sideandmete valdkonna puhul (vt Brkan 2019). Ta selgitab, et sideandmete kohtulahendite suuniseid saab illustreerida „segamini rägastikuna, mille lõppsiht jääb varjatuks [ELK] argumentatsiooni tõttu, mis on täis (...) ettearvamatuid pöördeid“. Kuigi peale sideandmete direktiivi leiti liikmesriikide poolt õiguslik konstruktsioon, mille alusel sideandmete säilitamine siiski jätkuda sai (Tracol 2017: 542), muutus liikmesriikide praktika ja lähenemine väga erinevaks (Tracol 2017). See olukord on jätkuv tänaseni. Seega on vaja mõista, milles seisnevad sisulised puudused valdkond õiguspäraselt reguleerida viisil, mis arvestaks nii inimeste õiguste ja vabaduste huvisid kui ka õiguskaitsevajadusi. Seetõttu on asjakohane lisaks kohtulahendite üldpõhimõtetele analüüsida ka konkreetseid ELK argumente, hinnanguid ja soovitusi probleemi lahendamiseks. Metodoloogiliselt kõrvutatakse need praktikute sisendiga, mis aitavad teha praktilisi, teoreetilisi ja loogilisi järeldusi kohtulahendite suuniste rakendatavuse osas.

Tabel 1. Euroopa Liidu Kohtu suunised ja nende praktiline rakendatavus

ELK lahendite paragrahvide suunised	Selgitus praktilise rakendatavuse osas
Kuigi sideandmete direktiiv tühistati, ei andnud ELK kohtuotsusega *Digital Rights Ireland jt* sisulisi suuniseid olukorra parandamiseks.	Säilitamise aluseks kujunes 2002. aasta e-privaatsuse direktiivi (2002/58/EÜ) artikkel 15(1).

Kuritegude tõkestamisel tuleks anda sideandmetele ligipääs üksnes isikute osas, „keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või eelnevas toimepanemises või niisuguse kuriteoga ühel või teisel viisil seotud olemises“ (*Tele2 Sverige ja Watson jt*, § 119).	Tihti ei ole otsitavad isikud teada, küberkuritegevuse kontekstis jäävad üksnes elektroonilised jäljed, mille abil on vaja tuvastada isikud, kes võivad olla potentsiaalsed kahtlusalused (Brown 2015: 80; Europol 2019: 6). Lisaks on probleem, et mitmed olulised küberruumis toime pandavad teod (kelmused, pettused) ei kvalifitseeru alati raskeks. Seetõttu jääksid inimesed sellises olukorras riigi poolse kaitseta.
Põhiõigustega „on vastuolus liikmesriigi õigusnormid, mis näevad kuritegevuse vastu võitlemise eesmärgil ette kõiki elektroonilise side vahendeid puudutava kohustuse säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik liiklusandmed ja asukohaandmed“ (*Tele2 Sverige ja Watson jt*, § 134 lg 1).	„Küsimus ei ole uurimiste tõhususe tagamises, vaid uurimiste ja kriminaalmenetluse läbiviimise tagamises iseenesest (eelkõige arvutikuriteod, ründed seadmete vastu, lasteporno käitlemisega seotud kuriteod ning sidevahendi ja arvutisüsteemide vahendusel toime pandud kuriteod, sealhulgas laste seksuaalse kuritarvitamise juhtumid, kus süüteo toimepanija otsib lapsohvreid ja paneb kuriteod toime küberruumis).“ (Välisministeerium 2020:18) Seega muutub keerulisemaks virtuaalruumis toime pandud kuritegude menetlemine ja tõendamine, sest puudub võimalus analüüsida erinevate osapoolte seotust (Brown 2015: 68).
Andmete säilitamine peab olema eesmärgipärane ja ennetav (ingl *targeted retention*), mille tõttu võib liikmesriik sätestada normid, „mis võimaldavad meetme suunata isikutele, kelle liiklus- ja asukohaandmetest võib avalduda kas või kaudne seos raskete kuritegudega“ ehk isikute suhtes, kes on tuvastatud riigisiseste	Võimalik säilitada üksnes juba tuvastatud kurjategijate või kahtlusaluste suhtes, kuid puudub võimalus kuritegusid sideandmete põhjal tõendada ega tuvastada võimalikke kaasosalisi (mis raske ja organiseeritud kuritegevuse puhul tihti oluline on). St probleem avaldub ajalooliste andmete puudumises (Kao & Wang 2009: 197-203).

menetluste käigus (*La Quadrature du Net jt*, § 148-149).	Seega hõlmab sihistatud säilitamine andmeid üksnes edasi ulatuvalt.
ELK hinnangul võib liiklus- ja asukohaandmete säilitamine olla ka geograafiliste asukohtade põhine: „need piirkonnad võivad olla näiteks kohad, kus raskete kuritegude arv on suur, kohad, mis on raskete kuritegude toimepanemiseks eriti soodsad, nagu paigad või ehitised, mida pidevalt külastab väga suur hulk inimesi, või ka strateegilised kohad, nagu lennu-, raudtee- ja bussijaamad või kiirteemaksu kogumise alad“ (*La Quadrature du Net jt*, § 150).	Suunis, mis mille praktiline toimimine on küsitav, sest see viitab iseeneses käimasolevatele menetlustele või operatsioonidele. Lisaks viitab kuritegevuse arvu suurus piirkonna määramisel iseeneses diskrimineerivale kriteeriumile. Ennustus-põhist politseimudelit on mitmetel alustel kritiseeritud (vt nt De Hert 2005; Bauman et al. 2014: 125-126; Lynskey 2019). Geograafilise asukoha puhul on oluline ka asjaolu, et ebaseaduslike tegevuste toime paneku ajaks on võimalik „piirkonnast“ lihtsalt väljuda.
Kuigi IP aadresside üldist säilitamist saab kohtu hinnangul pidada põhjendatuks virtuaalselt toime pandud kuritegude iseloomu arvestades (*La Quadrature du Net jt*, § 155), saab seda riivet põhjendada üksnes võitlusega raskete kuritegude vastu ja avalikku julgeolekut ähvardavate suurte ohtude ärahoidmisega, nagu ka riigi julgeoleku kaitsega (*La Quadrature du Net jt*, § 156).	Üksnes IP aadresside säilitamisest kurjategijate vastutusele võtmiseks ei piisa (Kao & Wang 2009: 202). Samuti on probleem selles, et paljud virtuaalruumis toime pandud kuriteod ei pruugi kvalifitseeru „rasketeks“, mis viitab, et isegi, kui kõikide klientide osas neid säilitatakse, ei tohi nt kelmuste jm puhul neid andmeid uurimiseks kasutada, olgugi, et tegemist on üksnes virtuaalruumis toime pandud tegevusega, mille „korral võib IP-aadress olla ainus uurimisvahend“ (*La Quadrature du Net jt*, § 154).
Põhiõigustega ei ole vastuolus seadusandlus, „millega on konkreetse tähtajata kehtestatud elektroonilise side teenuste osutajatele kohustus säilitada elektroonilise side vahendite kõikide kasutajate identiteediga seotud andmed kuritegude ennetamise, uurimise, avastamise ja	Kohus loob väga sisulise ja praktilise probleemi õiguskaitseorganitele: tuvastada on võimalik füüsiline identiteet, kuid andmed, mis võimaldaksid siduda isikut kuriteo toimepanemise ajahetke jm asjaoludega, säilitada lubatud ei ole. Sellegi poolest on

menetlemise ning avaliku julgeoleku kaitsmise eesmärgil, ilma et oleks vaja, et kuriteod oleksid rasked või avalikku julgeolekut ähvardav oht oleks suur või avaliku julgeoleku kahjustamine oleks oluline“ (*La Quadrature du Net jt*, § 159).	füüsilise identiteedi säilitamine ja tehnoloogiaga sidumine väga oluline suunis.
Kohus argumenteerib (*La Quadrature du Net jt*, § 162-165), et põhiõigustega on kooskõlas õigusnorm, mis võimaldab kohustada sideettevõtet sideandmeid teatud perioodini kiirsäilitama.	Kiirsäilitus ei lahenda tõenduslikke probleeme, sest see saa hõlmata minevikku, kuivõrd sideteenuse ohustajal ei ole EL õiguse kohaselt lubatud andmeid ajalooliselt vahet tegemata säilitada.

Mõneti arusaamatuks jääb üks peamiseid ja laiapõhjalisemaid õiguslikke hinnanguid. 2016. aastal sedastas ELK, et põhiõigustega on „vastuolus liikmesriigi õigusnormid, mis näevad kuritegevuse vastu võitlemise eesmärgil ette kõiki elektroonilise side vahendeid puudutava kohustuse säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik liiklusandmed ja asukohaandmed“ (*Tele2 Sverige ja Watson jt,* § 134 lg 1). Kuidas tuleb aga seda suunist õiguslikult mõista 2020. aasta kohtulahendi valguses, mille hinnangul, ei ole põhiõigustega vastuolus seadusandlikud meetmed, mis „näevad ette riigi julgeoleku kaitsmise, kuritegevuse vastu võitlemise ja avaliku julgeoleku kaitsmise eesmärgil elektroonilise side vahendite kasutajate identiteediga seotud andmete üldise ja vahet tegemata säilitamise“ (La Quadrature du Net jt, § 134 lg 1 p 4). Ehk milline on suunis, mida riik oma õigusruumi kujundamisel peaks arvestama? Kuivõrd 2016. aasta kohtulahendi loogikat on võimalik muuta üksnes uute oluliselt erinevate kohtuotsustega (Szabados 2015: 145), avaldub praktiline probleem kohtulahendi sisulises järgmises, sest üldine säilitamise keeld on endiselt kehtiv, kuigi, tõsi, mõnevõrra täpsustunud. Umbmääraseid ja mõneti vastuolulisi sisendeid võib pidada üheks põhjuseks, miks viidatakse, et EL liikmesriigid on endiselt ELK suunistega vastuolus on ning miks on peetud ka kriitikute poolt vajalikuks luua uus EL ülene õigusakt olukorra selgepiiriliseks määratlemiseks (vt Tracol 2017).

Võimalik probleem võib tuleneda kohtu poolt valede või ebapiisavate meetmete kasutamisel. Milaj (2015: 613) selgitab, et kohus kasutas 2014. aastal direktiivi tühistamisel

proportsionaalsuse testi, mille eesmärk oli tuvastada asjaolud, mis on vältimatult vajalikud eesmärgi saavutamiseks. Seevastu oleks olnud võimalik ka metodoloogiliselt läbi viia proportsionaalsuse test, mis analüüsiks „vähem piiravaid alternatiive" üldisele sideandmete säilitamisele (Milaj 2015: 613). Loogiliselt argumenteerides, tõepoolest, füüsiliselt aset leidva kuriteo uurimiseks (näiteks tapmised ja vargused) selliste andmete kasutamisele on alternatiive, kuivõrd kuritegu on võimalik menetleda füüsiliste sündmuste ja tõendite põhjal. Nagu eelnevalt selgitatud, küberruumi puhul alternatiive ei eksisteeri. Lisaks avaldub üldise keelustamise taustal olulise vastuoluna asjaolu, et isegi, kui sideandmeid tohib ELK suunisel raskete kuritegude uurimiseks kasutada, siis ajalooliselt neid andmeid vastavalt 2016. aasta *Tele2 Sverige ja Watson jt* kohtuotsusele ei tohiks. See on ka üks peamiseid kriitikaid teaduskirjanduses, viitega EL õiguse rikkumisele (vt Milaj 2015; Tracol 2017). Kuivõrd uurijate suurim väljakutse on tuvastada konkreetsetel perioodidel juhtunu (Kao & Wang 2009: 197-203), võib argumenteerida, et paraku ei pruugi olla „vähem" piiravat alternatiivi, kui kõikide klientide teatud andmeliikide säilitamine teatud ajaperioodi jooksul.

See kajastub ka hilisemates, 2018. ja 2020. aasta kohtuotsustes. ELK sedastab, et sideandmete kasutamine peaks olema võimaldatud laiemalt, kui üksnes raske kuritegevuse uurimisel (*Ministerio Fiscal*, § 63 ja 64) ning et üldise kuritegevuse tõkestamiseks peaks olema võimalik säilitada andmeid, mis on vajalikud isiku tuvastamiseks (*La Quadrature du Net jt*, § 159). Kuigi virtuaalselt toime pandud kuritegevuse puhul teadvustab ELK ise IP aadresside hädavajalikkust (*La Quadrature du Net jt*, § 152-159), viitab paragrahv 156, et IP aadresside kasutamine on õigustatud üksnes raskete kuritegude vastaseks võitluseks. Seevastu IP aadress on üks olulisemaid komponente digitaalse kriminalistika puhul, mille tõttu on võimalik teha järeldus, et ELK on oma vastuoluliste suunistega raskendanud küberkuritegevuse vastase võitluse tarbeks teostatava kriminaalmenetluse läbiviimiseks vajaminevate andmete kasutamist. Seega saab eelneva analüüsi põhjal argumenteerida, et ELK ei ole oma otsustes küberkuritegevuse iseloomu piisaval määral arvestanud. Seejuures ei väida uurimistöö, et küberkuritegevuse uurimine muutuks absoluutselt võimatuks, kuid ka kehtivates tingimustes on kübekuritegude menetlemise ajaline mõõde väga pikk, ulatudes mitmetesse aastatesse (Europol 2017: 28).

Siinkohal avaldub kolmanda uurimisküsimuse vastuolu. Sideandmete säilitamine iseeneses on tõlgendatud fundamentaalselt põhiõiguseid riivavaks. Seega ELK viitab iseeneses nullsummale – sellise meetme kasutamine turvalisuse tagamiseks ei ole õigustatud. Sideandmete mitte säilitamisel ei toimu ka riikide poolset privaatsuse riivet ning seega on kohtu hinnangul kodanike eraelu riigi eest kaitstud. ELK argumentatsioonis puudub viide hegellikule paradigmale, et arvestades küberkuritegevuse isikuandmevarguste ja manipuleerimise iseloomu, võiks sideandmete säilitamine ühiskonnas tervikuna aidata tagada positiivselt ka teiste oluliste väärtuste, näiteks privaatsuse kaitset. Enamgi, inimestel on selleks õigus ning Euroopa Inimõiguste Kohus (EIK) on seda õigust ka mitmetel juhtudel kaitsnud (vt nt K.U vs Soome, nr 2872/02; X ja Y vs Holland, nr 8978/80). Uurimistöö konteksti sobitub hästi K.U vs Soome kohtuasi, kuivõrd see seostus otseselt õiguskaitseasutuste suutmatusega digitaalset kuritegu sideandmete konfidentsiaalsuse tõttu menetleda.

Kohtuasjas K.U. vs Soome järeldas EIK, et riik läbi õiguskaitseasutuste peab tagama suutlikkuse kaitsta inimõiguste ja põhivabaduste kaitse konventsioonis sätestatud isikute eraelu ja privaatsuse rikkumist teiste isikute poolt. Kohus kritiseeris, et riik ei suutnud uurimise käigus alaealisest isikust internetti alasti pilte postitanud isikut tuvastada: „praktiline ja tõhus kaitse hagi esitaja suhtes eeldasid mõjusate meetmete kasutamist kuriteo toimepanija isiku tuvastamiseks ja vastutusele võtmiseks“, kuid Soome sellist kaitset isikule oma põhiõiguste kaitseks ei võimaldanud (K.U. vs Soome, § 49). Enamgi, kohus nägi probleemi asjaolus, et "tõhusat kriminaalmenetlust ei olnud võimalik läbi viia väga ülekaaluka konfidentsiaalsusnõude tõttu", kuid selline nõue ei saa kohtu hinnangul olla absoluutne, kuivõrd see piirab teiste isikute õiguste kaitset (K.U. vs Soome, § 49). EIK toonitas, et isikute privaatsust riivavate tegevuste vastu tuleb riigil luua tõhus kriminaalõigussüsteem (K.U. vs Soome, § 43) ning alaealiseid puudutavate intsidentide puhul on selline suutlikkus eriti oluline (K.U. vs Soome, § 46). Seega võib K.U. vs Soome kohtuasjas täheldada hegellikku argumentatsiooni.

Avalduv probleem on üllatavalt lihtne, kuid uurimistööks analüüsitud teaduskirjanduse põhjal ilmnes, et ükski autoritest ei ole kohtulahendites ilmnevatele vastuoludele sisulist tähelepanu pööranud. Esiteks on kõikidel inimestel õigus EL põhiõiguste harta artikli 6

alusel turvalisusele, olgugi, et see on täpselt sisustamata. EIÕK artiklis 13 on sätestatud inimeste õigus tõhusale õiguskaitsevahendile tema õiguste rikkumise korral. Ühtlasi on põhiõiguste harta artiklis 47 ja Ühendatud Rahvaste Organisatsiooni (ÜRO) Inimõiguste ülddeklaratsiooni artiklis 8 sätestatud inimeste õigus tõhusale kohtumenetlusele tema õiguste rikkumise korral. Seega on eranditult kõikidel inimestel õigus saada riigilt oma turvalisuse tagamist, tõhusat õiguskaitset ning kohtumenetlust, seda nii füüsilises, kui ka virtuaalruumis. Seda on peegeldanud ka valdav osa uurimistöö küsimustikule vastanud Eesti riigiametnikest. Kui teoreetiliselt puudub tulevikus sideandmete kasutamise võimalus kuritegude menetlemiseks, siis võib juhtuda, et digitaalsete kuritegude menetlemine muutub oluliselt probleemsemaks. Sellisel juhul avaldub riigile otsene piirang tagada inimeste turvalisust ja õigust tõhusale õiguskaitsele virtuaalruumis toime pandud rikkumiste puhul.

Võib argumenteerida, et seni on avaldunud Euroopas hegellik paradigma, milles eeldati, et reguleeritud keskkonnas tagavad seadused inimeste õigused ja vabadused. Konkreetse kriminaalmenetluse raames (põhjendatud olukord) on olnud võimalik õiguskaitseasutuste poolt sideandmeid (meede) näiteks kohtu loa (*ex ante* järelevalve) alusel analüüsida ning kasutamise proportsionaalsust ja õigust hinnatakse ka peale uurimistoimingute teostamist (*ex post* järelevalve). Teisisõnu, seadus tagab isikute vabadused ja õiguste kaitse ning seadus tagab ka riive ja selle lubatuse ja õiglase täitmise. Seevastu tugev orienteeritus individuaalsetele vabadustele võimaldab argumentatsiooni, et toimub liikumine jälgimisühiskonna suunas. Eelneva analüüsi põhjal saab väita, et ELK kohtulahendid ei ole privaatsuse kaitset tõhustanud, kuid on oluliselt mõjutanud õiguskaitseasutuste potentsiaalset suutlikkust virtuaalruumis inimeste turvalisust tagada. Hegelliku paradigma jätk oleks olnud seaduslike garantiide, näiteks järelevalvemeetmete tugevdamine. Kaasuste näitel avaldub seevastu hobbesilik paradigma, millest tõlgendub, et meetme tühistamisel Euroopa kodanike individuaalne privaatsus suureneb. Seega on kodanikud vabamad ja privaatsemad, kui neile kohalduvad vähemad seaduslikud piirangud, mis nende vaba tahet mõjutaks. Tulenevalt digitaalmaailma arengutest avaldub seevastu loogilise ja paratamatu tagajärjena õiguskaitseasutuste suutlikkuse vähenemine, kuivõrd küberruumis kehtivaid omapärasid ei ole kohtulahendites arvestatud.

4. Privaatsus ja turvalisus muutuvas keskkonnas: üksteist mõjutavad väärtused

Mitmed töös analüüsitud autorid (Solove 2008, Aquilina 2010) on viidanud, et privaatsus ja turvalisus ei pea olema omavahel vastanduvad. See on igati asjakohane argument, kuid nagu ilmneb, sõltub see väga suures ulatuses sellest, kuidas ühiskonnas erinevaid riigi poolseid tegevusi tajutakse. Ehk tegu on mõneti metafüüsilise probleemiga. Uurimistöö argumenteerib, et keskne olemuslik küsimus seisneb jätkuvalt vabaduse erinevas tõlgendamises ja mõtestamises. Tõepoolest, piiramatu ja läbipaistmatu riigivõim „võib viia paljude raskete tagajärgedeni“ (Toomla 1990: 38), kuid hegellik riigivõim oma positiivse ehk sekkuva vabaduse läbi ei pea tähendama türanniat ega autokraatiat. Hegellikus riigis seovad inimesed oma isiklikud huvid kollektiivsete huvidega ning läbi usalduse antakse kodanike poolt kinnitus, et riigi poolt tehtavad toimingud on ühiste väärtustega kooskõlas (Shaw 1992: 386). Lisaks avaldub autokraatlike elementide ja riigi omavoli maandamine palju kasutatud, kuid ka kritiseeritud, „tasakaalu“ metafooris – näiteks tugeva ja mitmetasandilise järelevalve toel. Seevastu võib vähemalt osaliselt teaduskirjanduse põhjal argumenteerida, et tänases Euroopas on see usaldus mingitel põhjustel kadumas. Paraku on usaldus eriti kaasaegses ühiskonnas hädavajalik:

> „Edukas reageerimine [tänapäevastele digitaalsetele ohtudele] sõltub sellest, kas riigiasutustele usaldatakse piisavad volitused, et piirideta virtuaalmaailmas kahtlusaluseid tuvastada ja kinni püüda. Kuid usalduse saavutamiseks on vaja kontrolli. Iga inimeste õiguseid riivav pädevus peab olema vajalik, selgelt seaduses sätestatud, piiritletud kooskõlas rahvusvaheliste inimõiguste standarditega ja allutatud põhjalikele ja tajutavatele kaitsemeetmetele.“ (Anderson 2015)

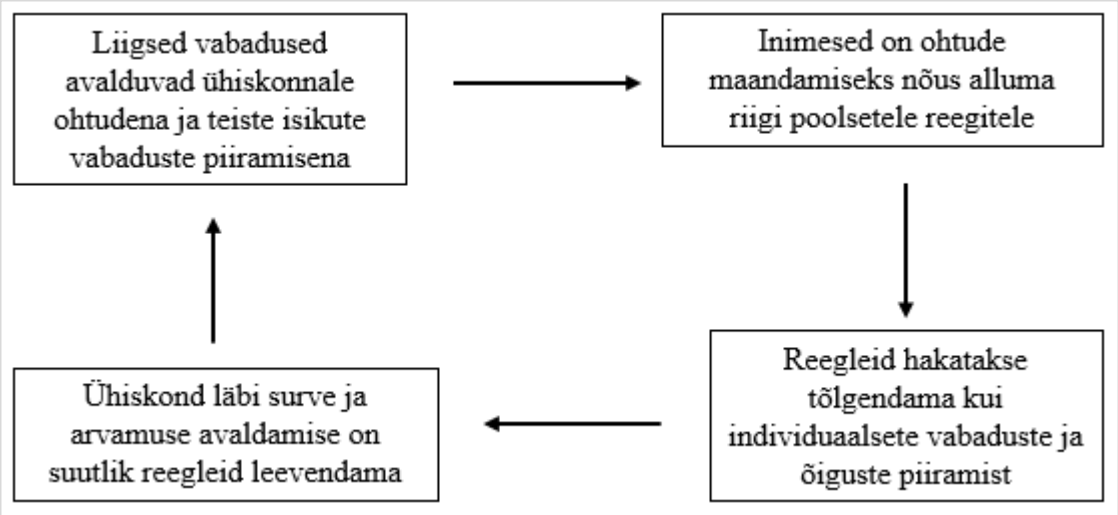
Kuivõrd usaldus avaldab olulist mõju avaliku arvamuse ja riigivõimu kasutatavate meetmete osas (Pavone & Pereira-Puga 2009; Garcia & Geva 2016; Vermeersch & De Pauw 2017), on asjakohane märkida, et kaasaegse NPM ja traditsioonilise avaliku halduse vahel avaldub ka usalduse osas oluline teoreetiline vastuolu. Hegeli filosoofias on paljud olulised ühiskondlikud funktsioonid antud riigile täitmiseks, sest riik suudab tagada hüvede võrdse jaotuse (Jackson 1986). Seetõttu asetub kesksele kohale moraalne missioon saavutada üldine

ühiskondlik heaolu, mille tagamisel peavad ametnikud ületama oma isiklikud ambitsioonid (Jackson 1986: 147). Üldise heaolu nimel on vajalik selgelt reguleeritud keskkond, läbi mille säilitatakse kehtivad normid (Shaw 1992: 386). Seega erinevalt NPMst ei ole hegelliku riigi eesmärk maksimaalne kuluefektiivsus ja tõhusus, vaid kõikide inimeste võrdne kohtlemine. Seonduvalt argumenteerivad Zanetti & Abrams (2000), et NPM praktikate rakendamine avaldub demokraatiale potentsiaalse ohuna, kuivõrd eetika ja inimeste võrdne kohtlemine aeglases bürokraatiamehhanismis asendatakse turupõhimõtteid järgiva efektiivsusele orienteeritusega. Teisisõnu demokraatlik võrdsus asendub liberalistlike individuaalsete vabadustega (Zanetti & Abrams 2000: 537), mis õiguskaitseasutuste konteksti asetatuna kõrvutab samuti sotsiaalsed ja majanduslikud eesmärgid (Newman 2002). See võib omakorda tekitada kodanike seisukohalt mitmeid omanäolisi probleeme – nt ebaefektiivsete tehnoloogiate kasutamine turvalisuse ja efektiivistamise eesmärgil, riigivõimu taandamine väiksemate rikkumiste menetlemisel jpm.

Hegellikku argumentatsiooni iseloomustab küberruumi näitel asjaolu, et „kui puudub institutsionaalne keha, kes jõustaks ja tagaks individuaalsete vabaduste kaitse, siis isiklike, sotsiaalsete ja institutsionaalsete ressursside tõttu ei suuda üksikisikud ise oma vabadusi realiseerida“ (Queiroz 2018). Küberruumi arengute taustal on riikidel paratamatult avaldunud huvitav paradoks õiguste ja seaduste jõustamise suutlikkuse osas. Teisisõnu küberruumi praeguses anarhilisuses ei saa inimesed ennast virtuaalsete ohtude olemuse tõttu kunagi päris turvaliselt ega kindlalt tunda. Samuti on inimesed sõltuvad individuaalsest võimekusest, kuid küberruumi tehnilisuses ei suuda kõik olla iseseisvad valdkonnaeksperdid. Seega taandub küsimuste sisuline lahendamine asjaolule, kas kodanikud usaldavad, et riik kaitseb nende õigusi ja vabadusi suuremal määral, kui nad seda individuaalselt teha suudavad.

Tsiftsoglou (2011) on väitnud, et turvalisus avaldub vabaduste piirangutena. Seevastu kas liigne autonoomne vabadus ilma hegellike õiguslike piirangute ja institutsionaliseeritud raamideta mõjub vabadustele hoopis negatiivselt ehk taastoodab piiranguid? Küberruumi näitel võiks see mõttekäik paika pidada – ulatuslik vabadus on tinginud olukorra, kus järjest suuremad ja omanäolisemad ohud avalduvad. Hobbesi riigifilosoofia sellel argumendil põhinebki – loomuseisundis on inimesed ise nõus aktsepteerima suverääni piiranguid

turvalisuse nimel. Piirangute taasloomine seevastu kajastub ka Hegeli filosoofias. Aleksandr Wansbrough on Hegelile tuginedes selgitanud, et „progressiivsed väärtused, näiteks sõnavabadus, võimaldavad regressiivseid konflikte ning poliitilised [individuaalsed] vabadused, mille eesmärk on inimesi eraldiseisvalt võimestada, võivad esile kutsuda ebameeldivusi ja omakasupüüdlust“ (Wansbrough 2019: 840). Eelnev mõttekäik on selgitatud joonisel 12.



Joonis 12. Vabaduste ja piirangute tekkimise tsükkel (autori joonis).

Seda argumenti ilmestab üks kaasaja ilmekamaid debatte virtuaalruumis aset leidva vihakõne ja ebaseadusliku sisu kontekstis. Kehtib tugev sõnavabaduse põhimõte, kuid kui seda sõnavabadust kasutatakse individuaalsetel ja vastuolulistel eesmärkidel või mingite inimgruppide ründamiseks? Kas sellist „üle piiri minevat“ sõnavabaduse piiramist tuleks tõlendada kui vabaduste vähenemist või analoogiat füüsilise ruumiga, kus ebaseaduslikele tegudele on tõenäoline ka sanktsioon? Leif Kalevi selgitus võimaldab kalduda pigem teise seisukoha poole. Ta argumenteerib, et avaliku korra rikkumise ehk seadustega „vastuolus olevaid tegevusi ei mõisteta isikuvabaduste teostamisena, vaid korravastasena ning kodanik muutub õigusrikkujaks, kelle avalik võim korrale kutsub (Kalev 2011). Seega, vastavalt Hegeli käsitlusele, kui karistus on inimese seadusevastase teo väljendus, siis peab inimene olema valmis ja ka vaba aktsepteerima ettenähtud tagajärgi. Seevastu on inimene vaba mitte vastutama tagajärgede eest, kui riik on õiguse mõistmise protsessi käigus tema õiguseid rikkunud.

Töö esimeses osas viidati Strauß (2017) argumendile, et pirvaatsust ja turvalisust tuleks tõlgendada kontekstis. Uurimistöö argumenteerib, et selline lähenemine võimaldab anda väärtustele sügavama mõtestatuse. Näiteks sideandmed – küberkuritegevuse puhul on nad digitaalsele ajastule omases kontekstis muutunud hädavajalikuks. Kuivõrd Hegeli kohaselt on vabadus alati sõltuv inimeste omavahelistest sotsiaalsetest suhetest (Pelczynski 1984), on see olemuslikult ka ajas jätkuv probleem, mille tõlgendus, käsitlus ja kontseptsioon võib erinevate ühiskondlike protsesside tulemusel muutuda. Samuti sõltub see vahendite kasutamise kontekstist – privaatsuse tagamise meetmed, loodud inimeste kaitseks, võimaldavad ka ohtu turvalisusele. Seega võib argumenteerida, et täna, kui kohus on püüdnud tugevalt inimeste individuaalseid vabadusi kaitsta, võib see tervikuna kuritegevust ja seeläbi turvalisust ning privaatsust veelgi negatiivsemalt mõjutada, mis omakorda avaldub pärssivana ka inimeste vabale tahtele. Seega võib väheneda ka inimeste usaldus riigivõimu vastu – kuigi inimesed ootavad kaitset, ei suuda riik seda teatud juhtudel pakkuda, mis omakorda võib süvendada virtuaalruumi teatavat anarhilisust.

Käesoleva uurimistöö eesmärk ei olnud lahendada igipõlist metafüüsilist probleemi, vaid läheneda sideandmete säilitamise ja küberkuritegevuse juhtumiuuringu toel privaatsuse ja turvalisuse dilemmale läbi konkreetse konteksti. Tõepoolest, on üheselt mõistetav, et sideandmete ulatuslik, ebaseaduslik ja ebaeetiline analüüsimine võimaldab teoreetiliselt jälgimisühiskonna teket. Sõltuvalt usaldusest võib ühiskond rohkemal või vähemal määral uskuda riigivõimu eetilisusesse ja moraalsusesse. Eeldades, et inimeste õigust privaatsust rikutakse üksnes eesmärgipäraselt, tunnevad inimesed ennast vabana ja hästi. Seevastu eeldades, et riik kõikide kodanike üle pidevat jälgimist ja kontrolli teostab, võimaldab see argumenteerida ka orwelliliku „suure venna“ tekkimise poolt.

Seega mille suhtes ühiskond ihkab olla vaba? Olles vaba riigivõimust ja selle kehtestatud reeglitest osutub meile piiravaks anarhiline keskkond, mis vähendab läbi hirmu ja ebakindluse inimeste elukvaliteeti ning inimesed ei saa loota, et nad oleksid allutatud institutsionaalsele kaitsele. Hirm ja ebakindlus seevastu muudab ühiskonna „mitte vabaks“ hoopis teistsugusel viisil. Kuigi inimestel on virtuaalruumis ulatuslikud vabadused, ei pruugi tulevikus suuta riigivõim eraettevõtteid ega üksikisikuid kuritegevuse ohvriks langedes kaitsta, mille tõttu ei saa need reaalsuses oma vaba tahet ellu viia. Kui püüda välistada

mingite tegurite olemuslik vabaduste vähendamise moment, on võimalik argumenteerida, et turvalisus ja privaatsus ei ole mitte üksteisele vastanduvad, vaid selgelt ja otseselt üksteist, sõltuvalt kontekstist, nii negatiivselt kui positiivselt mõjutavat väärtust.

Kokkuvõte

Käesolev magistritöö uuris privaatsuse ja turvalisuse omavahelist vastandlikku käsitlust küberkuritegevuse ja sideandmete kontekstis. On selge, et kaasaegses ühiskonnas soovivad inimesed mõlemat, kuid tehnoloogiaajastu eripärad on muutnud erinevate meetmete ja tehnoloogiate kasutamise riigi poolt küsitavaks. Tehnoloogia puhul on väga selge, et selle kasutamine ebaeetilistel eesmärkidel võib viia mitmete ühiskonna jaoks negatiivsete tagajärgedeni. Küberkuritegevus on üks konkreetsemaid näiteid. Tuginedes üksteisest oluliselt erinevatele riigiteooriatele – hobbesilikule ühiskondliku lepingu kompromissile ja hegellikule õigusriigile ning ühtlasi nende erinevale vabaduse mõtestamisele. Ühtlasi analüüsiti, kas konflikti saab selgitada kummalegi iseloomuliku riigihalduse mudeli, hobbesiliku vabadusega sarnasusi omava uue avaliku halduse (NPM) ning Hegeli vabadusekäsitlust peegeldava tugeva ja tsentraalse Kontinentaal-Euroopa õigusriigi mudeli abil.

Esiteks analüüsis uurimistöö probleemi tehnoloogiaajastu olemust. Kirjeldati privaatsuse ja turvalisuse kaasaegset vastandumist ning kirjeldati põhjalikult küberkuritegevust. Suurem osa riigiametnikest kinnitas sissejuhatuses püsitatud eeldust, et privaatsus võib tehnoloogiaajastu iseloomu tõttu turvalisust olulisel määral ohustada. Erinevalt uurimistöö käigus analüüsitud artiklitest argumenteerib töö, et (jälgimis) tehnoloogia iseenesest ei ole probleemne, vaid turvalisuse edendamiseks loodud tehnoloogiate olemus sõltub nende kasutusviisidest.

Privaatsuse ja turvalisuse dilemma analüüsimiseks esitati viis uurimisküsimust. Esiteks selgus, et Eesti turvalisust kujundavad riigiametnikud mõistavad privaatsuse ja turvalisuse omavahelist suhet üsna mitmekesiselt, kuid valdavalt oldi seisukohal, et need ei ole olemuslikult vastandlikud. Enamik vastanutest olid seisukohal, et privaatsuse riive ei tähenda automaatselt privaatsuse vähenemist ning privaatsust vähendav ei ole ka see, kui riik põhjendatud juhul isikute andmeid kogub ja töötleb. Seetõttu võib järeldada, et riigiametnike erinevate küsimuste vastustest peegeldus teatav usaldus protsesside õiguspärasuse suhtes. Siiski avaldus teatav vastuolu riigi tegevuse suhtes. Kui tehnoloogia kasutamine läbi põhiõiguste riive on automaatselt vabadusi vähendav, ei ole kasu kaitse- ega

järelevalvemeetmetest, sest algupärane valem avaldub igal juhul negatiivse mõjuna privaatsusele. Lisaks tuvastati, et riik riivab riigiametnike hinnangul kodanike õigusi rohkem siis, kui ta ei suuda nende õiguste kaitset tagada. Eelnimetatud eelduse tõttu, sõltumata suutlikkusest, avaldub, et riik riivab igal juhul inimese vabadusi. Siiski avaldus üldiselt mõnetine hegellik positsioon, mille kohaselt sideandmete säilitamine ja riigi poolsed kohustused erasektorile aitavad tagada lisaks turvalisusele ka privaatsust.

Teine uurimisküsimus uuris küberruumi arenemise loogikat ning selle mõju traditsioonilisele õiguskaitseasutuste tööle. Leiti, et võrreldes füüsilise maailmaga on digitaalmaailmale omane teatav anarhilisus ehk väheses reguleeritus. Seda arusaama kinnitasid ka enamik küsitlusele vastanud ametnikest, kes ühtlasi leidsid, et suurem eripärasid arvestav reguleeritus on vajalik. Seda selgitab, et virtuaalruumi areng ja haldamine toimunud valdavalt uuele avalikule haldusele omases stiilis ehk erasektori poolt. Ühtlasi peegeldub NPM asjaolus, et suurenenud nii erasektori roll kui kodanike endi vastutus küberruumis turvalisuse tagamisel. Seevastu praktikas on inimeste turvalisuse tagamine jätkuvalt riigi kohustus. Selle ülesande täitmine küberruumis on keerulisem, sest riigi traditsioonilise jõumonopoli rakendamine avaldub virtuaalmaailmas erinevalt, sest küberkuritegevuse lahendamisel ollakse sõltuvuses erasektori ettevõtete ja teiste riikide koostöövalmidusest. Teisisõnu avalduvad küberruumis riigi jaoks praktilised probleemid – suutmata kurjategijaid tuvastada ning kuritegevust tervikuna vajalikul määral tõkestada, ei paku riik inimestele ette nähtud kaitset.

Kolmandaks uuriti, kuidas Hobbesi ja Hegeli teooriate omavaheline kõrvutamine aitab mõista Euroopa Liidu õiguse konfliktsust privaatsust ja turvalisust puudutavate valdkondade kujundamisel. Järeldati, et probleemi on võimalik selgitada kahe fundamentaalselt erineva riigifilosoofia kokkupõrke abil. Seni hobbesilike loomuseisundiga sarnasusi omavat küberruumi on osutunud vajalikuks senisest enam reguleerida. Seda nähakse aga nullsummana, mitte õigusriikliku regulatiivse sekkumisena, mille tõttu on avaldunud probleem privaatsuse võimaliku säilimise ees. See avaldub selgelt, kuivõrd hobbesilik vabadus ja NPM eeldavad minimaalset riigivõimu sekkumist ja reguleeritust. Seevastu Euroopa Liit on lähiminevikus paljud valdkonnad ühiste eesmärkide nimel reguleerinud, et lisaks vabaduspõhisele keskkonnale oleks tagatud ka turvalisus ja õiguskesksus. Seega ei

avalduks õiguse kaudu turvalisuse kujundamine hegellikus eetilises riigis mitte piiranguna, vaid eeltingimusena ohutu ja turvalise küberruumi saavutamiseks.

Lõpetuseks käsitleti hobbesilikku ja hegellikku paradigmat Euroopa Liidu Kohtu sideandmete säilitamist puudutavate kohtuotsuste taustal. Uurimistöö argumenteerib, et privaatsuse ja turvalisuse konflikti aitab seletada aastakümneid Euroopas kehtinud õigusriikluse mõnetine torpedeerimine individuaalseid õiguseid rõhutava suundumuse poolt. Nii küberkuritegevus kui küberruum on andmepõhised. Seega on ka küberkuritegevuse vastane võitlus, mis arusaadavalt, kuid paratamatult, on tekitanud uusi muresid privaatsuse kaitse osas. Uurimistöö järeldab, et Euroopa Liidu Kohtu poolne sideandmete direktiivi tühistamine 2014. aastal ning üldine sideandmete säilitamise keelamine 2016. aastal, olles selgelt kantud individuaalsete vabaduste tugevdamise soovist, aitas tegelikkuses kaasa ebakindla keskkonna tekkimisele, mis tervikvaates pole avaldanud positiivset mõju inimeste privaatsusele ega turvalisusele. Nii turvalisuse kui privaatsuse kaitse jätkuv tagamine oleks eeldanud võimalikku tasakaalustamist ehk kaitsemeetmete suurendamist – säilitatavate andmete hulga ja ajaperioodi piiramist ning rangemate järelevalvemeetmete sätestamist.

Analüüsi põhjal ei ole uurimistöö tulemusel võimalik privaatsuse ja turvalisuse olemuslikku vastuolu kinnitada ega ümber lükata. Siiski argumenteerib uurimistöö, et privaatsust ja turvalisust ei pea mõtestama üksteisele vastanduvatena, vaid näiteks tugevalt üksteist mõjutavatena. Väärtuste omavaheline suhe sõltub aga sellest, kuidas inimesed oma individuaalset vabadust mõtestavad ja tõlgendavad ning millest nad vaba olla soovivad. Mõnetise kirjandusliku ebaselguse tõttu on seega hädavajalik täiendavalt uurida, kuidas inimesed kaasaegses ühiskonnas vabadusi tunnetavad. Olles vaba riigivõimust, võib osutuda inimeste vabale tahtele piiravaks ebakindel ja ohtlik keskkond, mida nii küberruumi kui läbikukkunud riikide näitel ilmestatud on. Püüdes argumenteerida euroopaliku õigusriigi eeldusliku eetilisuse vaatest, siis riiki ja selle seaduseid aktsepteerides ning riigivõimu usaldades on võimalik mõtestada vabadust inimeste ohu ning igapäevaellu ebavajaliku ja põhjendamatu sekkumise puudumise kaudu. Selline eetiline eeldus on põhjuseks, miks on võimalik mõtestada privaatsust ja turvalisust mitte vastandlikena, vaid üksteist mõjutavatena.

Summary

The thesis studied the trade-off concept between privacy and security in the context of cybercrime and metadata retention by the internet service providers. Is evident that people in modern society require both but the specific nature of technology has raised doubts about the state's deployment of various technologies. Without doubt, the unethical use of technology can lead to negative consequences for the society as a whole. Cybercrime has proven to be one of the most obvious examples of such implication.

The thesis builds on two significantly different state philosophies – the Hobbesian compromise based social contract and the Hegelian rule of law model but also on their completely different interpretation of liberty. Furthermore, it was analyzed, whether New Public Management, which has been previously related to Hobbes, and Continental European public management could be used to explain the trade-off conflict between privacy and security.

First, the problem was established in the context of technological era. Contemporary relationship between privacy and security and thorough overview of cybercrime was presented. A study among Estonian civil servants involved in security policy making was carried out and the results confirmed the assumption that privacy could indeed have negative implications on security. As opposed to several articles analyzed for this paper, it is argued that (surveillance) technology in itself has no intrusive implications but dependent on how these security technologies are being used.

To understand the privacy security dilemma, five research questions were presented. First, the survey participants had various understandings of this relationship. Still, the vast majority of respondents were of the opinion, that privacy and security are essentially not diametric. Furthermore, most of the officials agreed that the infringement of privacy does not necessarily result in the decrease of liberty. Similarly, it emerged that most of the participants did not consider the collection or processing of their data on justified purpose by the state as a decrease in their liberty. Therefore, it can be concluded that a certain degree of trust regarding the accountability of state was present. A slight contradiction became evident regarding the state action – if use of technology is deemed fundamentally wicked, it

matters not, if safeguards and supervision are enhanced – the baseline formula is always towards the negative impact on privacy. Further, it was found, that the state infringes ones' freedom if unable to provide protection. Therefore, it would appear, that whether able or unable to protect its citizens, state would always infringe one's freedom. Nevertheless, the general opinion was somewhat Hegelian, that metadata retention and cybersecurity obligations imposed on private entities can help to provide both, security as well as privacy.

Second research question studied the development of cyber space and its implications on traditional law enforcement. It was found that in comparison to the physical world, cyber space can be characterized by relative anarchism, i.e. absence of regulation. The latter became evident also from the respondents answers, where the need for further regulation, although with certain specifies, was clearly stated. This can be explained by the fact that cyber space has been mainly developed by private entities, similarly to the NPM logic. In addition, both the private sector as well as private individuals have gained increased responsibility for ensuring security in the digital space, which again applies to NPM. Although the state has an obligation to provide security in the physical and in the cyber space, fulfilling the task in the latter is becoming increasingly complex. Namely, states are lacking the necessary capabilities to carry out their traditional monopoly of power in the borderless cyber space where they are dependent on the aforementioned private entities but also on other states. In other words, such situation could give rise to a certain set of issues – the state's inability to detect and fight cyber criminals will result in the failure to meet its obligation to protect its citizens.

Third, it was analyzed, how the privacy-security conflict could be explained in respect to the European Union law, when analyzed through the Hobbesian and Hegelian theories. It was concluded, that the conflict could indeed be explained through the impact of fundamentally different logic of state and freedom. Cyberspace, having similar characteristics to the Hobbesian natural law theory, has increased the pressure by the states to establish more regulations. This, however, is seen as a trade-off, not rule of law based intervention, and has created serious concerns from the privacy protection perspective. This is evident, because Hobbesian liberty and NPM are explained through minimal state interference and regulation. In the past, however, the EU has regulated many areas in order to achieve common goals

and in addition to secure the area of freedom, provide security and justice. Therefore, if placed into the Hegelian ethical state perspective, regulations would not appear as restrictions of individual liberty but as preconditions for safe and secure cyberspace.

Finally, Hobbesian and Hegelian paradigms were analyzed regarding the EU case law and data retention. It was concluded that strong orientation towards individual liberties could be undermining the strong and central rule of law principle, which dominated the Continental Europe law system for many decades. As cybercrime and cyberspace are data-centric, the fight against crime is also depending on data, which, understandably, yet unavoidably, has created new concerns about privacy protection. This paper concludes, that although the rulings of the European Court of Justice, which invalidated the data retention directive in 2014 and forbade general data retention in 2016 were clearly driven by the desire to protect the individual liberty of EU citizens, in their apparent unclarity, led to an unstable legal environment, which has had a positive impact neither on the EU citizens' privacy nor their security. The enhancement of both privacy and security could have been achieved through the implementation of stronger safeguards – the limitation of retained data, time and increased supervision.

On the basis of the present analysis it is not possible to confirm or disprove, whether privacy and security are essentially conflicting values. Nevertheless, it is argued, that privacy and security may not be perceived as opposites but in strong relation to one-another. Such relation, however, is dependent on how people conceptualize and understand their personal liberty and from what they wish to be free from. Due to confusing literature on this, it should be certainly researched more thoroughly, how contemporary citizens perceive freedom. If freed from the state power, the free will of individuals may become restricted by the uncertain and dangerous environment, as can be illustrated with the examples of cyberspace and failed states. Yet, from the European rule of law based ethic state perspective, if accepting the state, its laws, and having trust in the state's activities, it is possible to conceptualize freedom as being free from danger and inappropriate intrusion by the state. Such ethical assumption would give an opportunity to think of privacy and security not as of opposites but as values, which, depending on circumstances, impact or complement each other.

Kasutatud kirjandus

Aas, Krista & Gross, Oskar (2021) „Andmed on Digitaalse Maailma DNA.“ *Postimees, 11. märts.* https://leht.postimees.ee/7198609/krista-aas-oskar-gross-andmed-on-digitaalse-maailma-dna (külastatud 11.03.2021)

Abercrombie, Nicholas; Turner Bryan S. & Hill, Stephen (2015) *Sovereign Individuals of Capitalism* [1986]. London & New York: Routlege.

Abrams, Lawrence (2020) „Sodinokibi Ransomware Data Leaks Now Sold on Hacker Forums.“ *Bleeping Computer*, 19. märts. https://www.bleepingcomputer.com/news/security/sodinokibi-ransomware-data-leaks-now-sold-on-hacker-forums/ (külastatud 03.04.2020)

Akers, Ronald L. (1990) „Rational Choice, Deterrence, and Social Learning Theory in Criminology: The Path Not Taken.“ *Journal of Criminal Law and Criminology* 81(3): 653–676.

Allen, Julia H. (2000) „State of the Practice of Intrusion Detection Technologies.“ *Carnegie Mellon University. Software Engineering Institute*. Report number: CMU/SEI-99-TR-028 https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=13543 (külastatud 12.05.2021)

Anderson, David Q. C. (2015) *A Question of Trust – Report of the Investigatory Powers Review. Independent Reviewer of Terrorism Legislation.* https://terrorismlegislationreviewer.independent.gov.uk/a-question-of-trust-reportof-the-investigatory-powers-review (külastatud 20.02.2021)

Aquilina, Kevin (2010) „Public security versus privacy in technology law: a balancing act?“ *Computer Law & Security Review* 26(2): 130–143.

Balboni, Paolo & Pelino, Enrico (2013) „Law Enforcement Agencies' Activities in the Could Environment: a European Legal Perspective.“ *Information & Communications Technology Law* 22(2): 165–190.

Barker, Ernest (1962) *Social contract: Essays by Locke, Hume and Rousseau*. New York: Oxford University Press.

Barlow, John P. (1996) „A Declaration of the Independence of Cyberspace.“ Electronic Frontier Foundation. https://www.eff.org/cyberspace-independence (külastatud 16.05.2021)

Bauman, Zygmunt; Bigo, Didier; Esteves, Paulo; Guild, Elspeth; Jabri, Vivienne; Lyon, David & Walker, R. B. J. (2014) „After Snowden: Rethinking the Impact of Surveillance.“ *International Political Sociology* 8(2): 121–144.

Beebe, Nicole L. & Clark, Jan G. (2004) „A Hierarchical, Objectives-Based Framework for the Digital Investigations Process." Digital Forensics Research Workshop (DFRWS), Baltimore, 2004. https://dfrws.org/presentation/a-hierarchical-objectives-based-framework-for-the-digital-investigations-process/ (külastatud 12.05.2021)

Bellanova, Rocco & González Fuster, Gloria (2013) „Politics of disappearance: Scanners and (unobserved) bodies as mediators of security practices." *International Political Sociology* 7(2): 188–209.

Berman, Jerry & Mulligan, Norman (1999) „Privacy in the Digital Age: Work in Progress." *Nova Law Review* 23(2): 551-582.

Birch, David (2009) „Victorian Values: Politicians and the Public Incorrectly See Security and Privacy as Opposites." *Information Security Technical Report* 14(3): 143–145.

Blackstone, Bethany; Giles, Michael W. & Vining, Richard L (2008) „The Supreme Court in American Democracy: Unraveling the Linkages between Public Opinion and Judicial Decision Making." *The Journal of politics* 70(2): 293-306.

Blažič, Borka J. & Klobučar, Tomaž (2020) „Removing the Barriers in Cross-Border Crime Investigation by Gathering e-evidence in an Interconnected Society." *Information & Communications Technology Law* 29(1): 66–81.

Blažič, Borka J. & Klobučar, Tomaž (2020) „Removing the Barriers in Cross-Border Crime Investigation by Gathering e-evidence in an Interconnected Society." *Information & Communications Technology Law* 29(1): 66–81.

Blauberger, Michael & Schmidt, Susanne K. (2017) „The European Court of Justice and its Political Impact." *West European Politics* 40(4): 907–918.

Blauberger, Michael; Heindlmaier, Anita; Kramer, Dion; Martinsen, Dorte Sindbjerg; Thierry, Jessica Sampson; Schenk, Angelika & Werner, Benjamin (2018) „ECJ Judges Read the Morning Papers. Explaining the Turnaround of European Citizenship Jurisprudence." *Journal of European Public Policy* 25(10): 1422–1441.

Borchardt, Klaus D. (2016) *Liidu õiguse ABC.* Luksemburg: Euroopa Liidu Väljaannete Talitus.

Bowyer, Kevin W. (2004) "Face Recognition Technology: Security Versus Privacy." *IEEE Technology and Society Magazine* 23(1): 9–20.

Britz, Marije T. (2013) *Computer Forensics and Cyber Crime: an Introduction*. Clemson University, 3rd edition.

Budak, Jelena; Rahj, Edo & Recher, Vedran (2017) „Citizens' Privacy Concerns: Does National Culture Matter?" Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 36–51.

Bug, Mathias & Bukow, Sebastian U. (2017) „Civil Liberties vs. Security: Why Citizens Accept or Reject Digital Security Measures.“ *German Politics* 26(2): 292–313.

Broadhurst, Roderic; Grabosky, Peter; Alazab, Mamoun & Chon, Steve (2014) „Organizations and Cyber Crime: An Analysis of the Nature of Groups Engaged in Cyber Crime.“ *International Journal of Cyber Criminology* 8(1): 1–20.

Button, Mark (2020) „The “New” Private Security Industry, the Private Policing of Cyberspace and the Regulatory Questions.“ *Journal of Contemporary Criminal Justice* 36(1): 39-55.

Burgess, Peter J. (2008) „Security After Privacy: The Transformation of Personal Data in the Age of Terror.“ *International Peace Research Institute,* Oslo (PRIO), policy brief 5: 1–4. https://www.academia.edu/12239471/Security_after_privacy (külastatud 01.05.2021)

Burt, Tom (2020) „Microsoft report shows increasing sophistication of cyber threats.“ 29. september. https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/ (külastatud 16.05.2021)

Brown, S. D. Cameron (2015) „Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice“ International Journal of Cyber Criminology 9(1): 55-119.

Camp, Jean & Chien, Y. T. (2000) „The Internet as Public Space: Concepts, Issues, and Implications in Public Policy.“ *ACM SIGCAS Computers and Society* 30:3.

Campell, Carlos I. (2021) „Authorities have taken down the dark web’s largest illegal marketplace“ The Verge, 12. jaanuar. https://www.theverge.com/2021/1/12/22227929/darkmarket-shutdown-europol-worlds-largest-illegal-marketplace (külastatud 16.01.2021)

Castells, Manuel (2000) *Information Age: Rise of the Network Society*. Maiden: Blackwell.

Caš, Johann; Bellanova, Rocco; Peter, Burgess J.; Friedewald, Michael & Peissl, Walter (2017) „Surveillance, Privacy and Security.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 7-12.

Caruana, Mireille M. (2019) „The Reform of the EU Data Protection Framework in the Context of the Police and Criminal Justice Sector: Harmonisation, Scope, Oversight and Enforcement.“ *International Review of Law, Computers & Technology* 33(3): 249-270.

Chapell, Allison T; Monk-Turner, Elizabeth & Payne, Brian K. (2010) „Broken Windows or Window Breakers: The Influence of Physical and Social Disorder on Quality of Life.“ Justice Quarterly 28(3): 522-540.

Choo, Kim-Kwang R. (2011) „The Cyber Threat Landscape: Challenges and Future Research Directions.“ *Computers & Security* 30(8): 719-731.

Chowdhury, Nupur & Wessel, Ramses A. (2012) „Conceptualising Multilevel Regulation in the EU: A Legal Translation of Multilevel Governance?“ *European Law Journal* 18(3): 335–357.

Chrismas, Billy (2017) „The Link Between American Gun Culture and White Supremacy Undermines Conservative Arguments for Gun Rights But Not Classical Liberal Arguments.“ *Libertarianism*. https://www.libertarianism.org/columns/second-amendment-me-gun-control-thee (külastatud 09.05.2021)

Clark, Tom S. (2009) „The Separation of Powers, Court Curbing, and Judicial Legitimacy.“ *American Journal of Political Science* 53(4): 971–989.

Curran, James (2009) „Reinterpreting Internet History.“ Raamatus *Handbook of Internet Crime*, toim. Jewkes, Yvonne & Yar, Majid. USA & Canada: Willan Publishing, 17–37.

Davidoff, Sherri & Ham, Jonathan (2012) *Network Forensics: Tracking Hackers through Cyberspace.* Pearson Education Inc.

Davies, Gareth (2016) „The European Union Legislature as an Agent of the European Court of Justice.“ *Journal of Common Market Studies* 54(4) 846–861.

De Hert, Paul (2005) „Balancing Security and Liberty Within the European Human Rights Framework. A Critical Reading of the Court's Case Law in the Light of Surveillance and Criminal Law Enforcement Strategies After 9/11.“ *Utrecht Law Review* 1(1): 68–96.

Denning, Dorothy E. & Baugh, William E. (1997) „Encryption and Evolving Technologies: Tools of Organized Crime and Terrorism.“ *Trends in Organized Crime* 3: 84–91.

Denning, Dorothy E. & Baugh, William E. (1999) „Hiding Crimes in Cyberspace.“ *Information, Communication & Society* 2(3): 251–276.

Dinant, Jean-Marc (2004) „The Long Way from Electronic Traces to Electronic Evidence.“ *International Review of Law, Computers and Technology* 18(2): 173-183.

Dratwa, Jim, ed. (2014) „Ethics of Security and Surveillance Technologies.“ *Opinion no. 28 of the European Group on ethics in science and new technologies*. Brussels. https://ec.europa.eu/info/publications/ege-opinions_en (külastatud 01.05.2021)

Drechsler, Wolfgang (2005) „The Re-Emergence of "Weberian" Public Administration after the Fall of New Public Management: The Central and Eastern European Perspective.“ *Halduskultuur* 6: 94–108.

Drozdova, Jekaterina (2001) „Civil Liberties and Security in Cyberspace.“ Raamatus *The Transnational Dimension of Cyber Crime and Terrorism*, toim Sofaer, Abraham D. & Goodman, Seymout D. Stanford: Hoover Institution Press, 183-220.

Drewer, Daniel & Miladinova, Vesela (2017) „The BIG DATA Challenge: Impact and Opportunity of Large Quantities of Information Under the Europol Regulation.“ *Computer Law & Security Review* 33(3): 298-308.

Dunn, William N. & Miller, Dawid Y. (2007) „A Critique of the New Public Management and the Neo-Weberian State: Advancing a Critical Theory of Administrative Reform.“ Public Organization Review 7(4): 345–378.

Duquette, David A. „Hegel: Social and Political Thought“ *Internet Encyclopedia of Philosophy*. https://iep.utm.edu/hegelsoc/ (külastatud 21.02.2021)

Dyde, Samuel W. (1894) „Hegel's Conception of Freedom.“ *The Philosophical Review* 3(6): 655–671.

Eck, John E. & Gersh, Jeffrey H. (2000) „Drug Trafficking as a Cottage Industry.“ *Crime Prevention Studies* 11: 241–271.

Eckes, Christina & Knstandinides, Theodore, eds. (2011) *Crime Within the Area of Freedom, Security and Justice: A European Public Order*. USA, New York: Cambridge University Press.

Eddy, Melissa & Perlroth, Nicole (2020) „Cyber Attack Suspected in German Woman's Death“ *The New York Times,* 18. september. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html (külastatud 16.01.2021)

Eesti Vabariigi Põhiseadus. https://www.riigiteataja.ee/akt/115052015002 (külastatud 10.05.2020)

Eneman, Marie; Gillespie, Alisdair A. Brend, Stahl C. (2010) „Technology and Sexual Abuse: A Critical Review of an Internet Grooming Case.“ Conference: Proceedings of the International Conference on Information Systems, 144. https://aisel.aisnet.org/icis2010_submissions/144 (külastatud 04.01.2021)

Eoyang, Mieke; Peters, Allison; Mehta, Ishan & Gaskew, Brandon (2018) „To Catch a Hacker: Toward a Comprehensive Strategy to Identify, Pursue and Punish Malicious Cyber Actors.“ Third Way Report. 29. oktoober. https://www.thirdway.org/report/to-catch-a-hacker-toward-a-comprehensive-strategy-to-identify-pursue-and-punish-malicious-cyber-actors (külastatud 12.05.2021)

Eriksson, Johan & Giacomello, Giampiero (2006) „The Information Revolution, Security, and International Relations: (IR) Relevant Theory?“ *International Political Science Review* 27(3): 221–244.

Esposti, Sara D.; Pavone, Vincenzo & Santiago-Gómez, Elvira (2017) „Aligning Security and Privacy: The Case of Deep Packet Inspection“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 72–90.

Eurobaromeeter 2017. „European's attitudes toward's security.“ Summary – nr 464b. https://europa.eu/eurobarometer/surveys/detail/1569 (külastatud 15.05.2021)

Eurobaromeeter 2019. „European's Attitudes Towards Cyber Security." Summary – nr 499. https://europa.eu/eurobarometer/surveys/detail/2249 (külastatud 15.05.2021)

Europol (2018) *Common Challenges in Combating Cybercrime.* *https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime* (külastatud 20.09.2020)

Europol (2019) *Cyber-Telecom Crime Report*. https://www.europol.europa.eu/publications-documents/cyber-telecom-crime-report-2019 (külastatud 11.04.2021)

Europol & Eurojust (2019) *First Report on the Observatory Function on Encryption.* https://www.eurojust.europa.eu/first-europoleurojust-report-encryption-observatory-function (külastatud 05.01.2021)

Europol (2020) *Internet Organized Crime Threat Assessment (IOCTA).* https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020 (külastatud 01.05.2020)

Euroopa Inimõiguste Kohtu Suurkoja otsus (1985) kohtuasjas 8978/80, *X ja Y vs Holland.*

Euroopa Inimõiguste Kohtu Suurkoja otsus (1992) kohtuasjas 72/1991/324/396, *Niemetz vs Saksamaa*.

Euroopa Inimõiguste Kohtu Suurkoja otsus (2002) kohtuasjas 2346/02, *Pretty vs Ühendkuningriik*.

Euroopa Inimõiguste Kohtu Suurkoja otsus (2007) kohtuasjas 6339/05, *Evans vs Ühendkuningriik*.

Euroopa Inimõiguste Kohtu Suurkoha otsus (2008) kohtuasjas 2872/02, *K.U vs Soome.*

Euroopa Kohtu Suurkoja otsus (2014) liidetud kohtuasjades C 293/12 ja C 594/12, *Digital Rights Ireland jt*.

Euroopa Kohtu Suurkoja otsus (2016) Liidetud kohtuasjades C-203/15 ja C-698/15, *Tele2 Sverige AB ja Watson jt*.

Euroopa Kohtu Suurkoja otsus (2018) kohtuasjas C-207/16, *Ministerio Fiscal*.

Euroopa Kohtu Suurkoja otsus (2020) Liidetud kohtuasjades C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net jt*.

Euroopa Kohtu Suurkoja otsus (2021) kohtuasjas C-746/18, *H. K. vs Prokuratuur*.

Fairfield, Joshua A. T. & Engel, Christoph (2015) „Privacy as a Public Good." *Duke Law Journal* 65(3): 385–457.

Farmer, Lindsay (2014) „Criminal Law as a Security Project." *Criminology and Criminal Justice* 14(4): 399–404.

Friedewald, Michael Peter, Burgess J.; Caš, Johann; Bellanova, Rocco & Peissl, Walter toim. (2017) *Surveillance, Privacy and Security: Citizens' Perspectives*. London & New York: Routledge.

Galetta, Antonella & De Hert, Paul (2014) „Complementing the Surveillance Law Principles of the ECtHR with its Environmental Law Principles: An Integrated Technology Approach to a Human Rights Framework for Surveillance." *Utrecht Law Review* 10(1): 55–75.

Galetta, Antonella (2013) „The Changing Nature of the Presumption of Innocence in Today's Surveillance Societies: Rewrite Human Rights or Regulate the Use of Surveillance Technologies?" *European Journal of Law and Technology* 4(2): https://ejlt.org/index.php/ejlt/article/view/221/377 (külastatud 15.05.2021)

Garcia, Blake E. & Geva, Nehemia (2016). „Security Versus Liberty in the Context of Counterterrorism: An Experimental Approach. *Terrorism and Political Violence* 28(1): 30-48.

Gatlan, Sergiu (2020) „Buchbinder Car Renter Exposes Info of Over 3 Million Customers." *Bleeping Computer*, 23. jaanuar. https://www.bleepingcomputer.com/news/security/buchbinder-car-renter-exposes-info-of-over-3-million-customers/ (külastatud 16.05.2021)

Gellert, Raphael & Serge, Gutwirth (2013) „The Legal Construction of Privacy and Data Protection." *Computer Law & Security Review* 29(5): 1–15.

Gerry QC, Felicity; Muraszkiewicz, Julia; Vavoula, Niovi (2016) „The Role of Technology in the Fight Against Human Trafficking: Reflections on Privacy and Data Protection Concerns" *Computer Law & Security Review* 32(2), 205–217.

Giacomello, Giampiero (2005) *National Governments and Control of the Internet: A Digital Challenge*. USA & Kanada: Routledge.

Goldstein, Herman (1977) *Policing a Free Society*. Cambridge & Massachusetts: Ballinger.

Gonzales Fuster, Gloria & Gutwirth, Serge (2013) „Opening Up Personal Data Protection: A Conceptual Controversy." *Computer Law & Security Review* 29(5): 531–539.

Grabosky, Peter (2007) „The Internet, Technology and Organized Crime." *Asian Journal of Criminology* 2: 145–161.

Greenwald, Glenn (2014) *No place to hide: Edward Snowden, the NSA, and the U.S. surveillance State.* New York: Metropolitan Books.

Haker, Hille (2015) „The New Culture of Security and Surveillance." *Political Sciences and Public Affairs* 3(1): 1–6.

Hayes, Ben; Jeandespoz, Julien; Ragazzi, Francesco; Simon, Stephanie & Mitsilegas, Valsamis (2015) „The law enforcement challenges of cybercrime: are we really playing

catch up?“ Study for the LIBE Committee. Directorate General for Internal Policies. European Union, Brussels. https://www.europarl.europa.eu/thinktank/en/document.html?reference=IPOL_STU(2015)536471 (külastatud 12.12.2020)

Hearfield, Ryan; Loukas, George; Budimir, Sanja; Bezemskij, Anatlij; Fontaine, Johnny R. J.; Filippoupolitis, Avgoustinos & Roesch, Etienne (2018) „A Taxonomy of Cyber-Physical Threats and Impact in the Smart Home.“ *Computers & Security* 78: 398–428.

Henriquez, Maria (2019) „The top 12 data breaches of 2019.“ *Security Magazine*, 05. detsember. https://www.securitymagazine.com/articles/91366-the-top-12-data-breaches-of-2019 (külastatud 18.03.2020)

Hildebrandt, Mireille (2013) „Balance or Trade-off? Online Security Technologies and Fundamental Rights.“ *Philosophy and Technology* 26(4): 357–379.

Hinduja, Sameer (2004) „Theory and Policy in Online Privacy.“ *Knowledge, Technology & Policy* 17(1): 38-58.

Hinchman, Lewis P. (1982) „Hegel's Theory of Crime and Punishment.“ *The Review of Politics* 44(4): 523–545.

Hobbes, Thomas (1996) *Leviathan* [1691]. Tuck, Richard toim. Cambridge: Cambridge University Press.

Jackson, Michael W. (1986) „Bureaucracy in Hegel's Political Theory.“ *Administration & Society* 18(2): 139–157.

Jackson, Robert H. (1993) *Quasi-States: Sovereignty, International Relations and the Third World*. Cambridge: Cambridge University Press.

Jasserand, Catherine (2018) „Law Enforcement Access to Personal Data Originally Collected by Private Parties: Missing Data Subjects’ Safeguards in Directive 2016/680?“ *Computer Law & Security Review* 34(1): 154–165.

Jewkes, Yvonne & Yar, Majid (2010) *Handbook of Internet Crime.* USA & Canada: Willan Publishing.

Kalev, Leif (2011) „Vabadus, Võrdsus ja Vendlus ning Liberaaldemokraatliku Riigi Üleilmastumine“ *Vikerkaar* http://www.vikerkaar.ee/archives/12522 (külastatud 21.01.2021)

Kao, Da-Yu & Wang, Shiuh-Jeng (2009) „The IP address and time in Cyber-Crime Investigation.“ *Policing: an International Journal of Police Strategies and Management* 32(2): 194-208.

Kolliarakis, Georgios (2017) „In Quest of Reflexivity: Towards an Anticipatory Governance Regime for Security.“ Raamatus *Surveillance, Privacy and Security: Citizens*

Perspectives, toim. Friedewald, Michael et al. London & New York: Routledge, 234–254.

KOMISJONI TEATIS EUROOPA PARLAMENDILE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE Euroopa julgeoleku tegevuskava. COM/2015/0185 final. https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52015DC0185

KOMISJONI TEATIS EUROOPA PARLAMENDILE, EUROOPA ÜLEMKOGULE, NÕUKOGULE, EUROOPA MAJANDUS- JA SOTSIAALKOMITEELE NING REGIOONIDE KOMITEELE ELi julgeolekuliidu strateegia kohta. COM/2020/605 final. https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52020DC0605

Krasner, Stephen D. (2004) „Sharing Sovereignty: New Institutions for Collapsed and Failing States." *International Security* 29(2): 85–120.

Laks, Liina (2020) „Eelnõu paneb andmeid koguma ja isikustab kõnekaardid." *Postimees, 2. november.* https://leht.postimees.ee/7099660/eelnou-paneb-andmeid-koguma-ja-isikustab-konekaardid (külastatud 16.05.2021)

Lambert, John (2020) „Important steps for customers to protect themselves from recent nation-state cyberattacks." 13. detsember. https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/ (külastatud 16.05.2021)

Lambert, John (2020) „Important steps for customers to protect themselves from recent nation-state cyberattacks." 13. detsember. https://blogs.microsoft.com/on-the-issues/2020/12/13/customers-protect-nation-state-cyberattacks/ (külastatud 16.05.2021)

Lewis, James A.; Zheng, Denise E.; & Carter, William A. (2017) „The Effect of Encryption on Lawful Access to Communications Data." *Centre for Strategic and International Studies*. https://www.csis.org/analysis/effect-encryption-lawful-access-communications-and-data (külastatud 12.05.2021)

Levy, Ian & Robinson, Crispin (2018) „Principles For a More Informed Exeptional Access Debate." *Lawfare* https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate (külastatud 20.03.18)

Liaropoulos, Andrew (2019) „In search of a Social Contract for Cybersecurity." Proceedings of the 18th European Conference on Cyber Warfare and Security, 4-5 July, University of Coimbra Portugal.

Liberatore, Angela (2007) „Balancing Security and Democracy, and the Role of Expertise: Biometrics Politics in the European Union." *European Journal on Criminal Policy and Research* 13(1): 109–137.

Lischka, Juliane A. (2016) „Explicit terror prevention versus vague civil liberty: how the UK broadcasting news (de)legitimatise online mass surveillance since Edward Snowden's revelations." *Information, Communication and Society* 20(5): 665–682.

Loideain, Nora N. (2015) „EU Law and Mass Internet Metadata Surveillance in the Post-Snowden Era.“ *Media and Communication* 3(2): 53–62.

Lukacs, Adrienn (2016) „What is Privacy? The History and Definition of Privacy.“ https://www.semanticscholar.org/paper/What-is-Privacy-The-History-and-Definition-of-Adrienn/430bfacbabb89c0033b6dcceddc18ba9bbc02c5f (külastatud 13.04.2021)

Lynskey, Orla (2019) “Criminal Justice Profiling and EU Data Protection Law: Precarious Protection from Predictive Policing.” *International Journal of Law in Context* 15(2): 162–176.

Lyon, David (2004) „Globalising surveillance. Comparative and sociological perspectives.“ *International Sociology* 19(2): 135–149.

Malik, Nikita (2018) „The Internet: To Regulate Or Not To Regulate?“ *Forbes* (7. september). https://www.forbes.com/sites/nikitamalik/2018/09/07/the-internet-to-regulate-or-not-to-regulate/?sh=69da686b1d16 (külastatud 03.12.2021)

Mann, Heather; Garcia-Rada, Ximena; Hornuf, Lars & Tafurt, Juan (2016) „What Deters Crime? Comparing the Effectiveness of Legal, Social, and Internal Sanctions Across Countries.“ *Frontiers in Psychology* 7: artikkel 85.

Marin, Luisa (2017) „The Deployment of Drone Technology in Border Surveillance: Between Techno-Securitization and Challenges to Privacy and Data Protection.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 107–122.

Meos, Indrek (2000) *Uusaja filosoofia: peatükke filosoofia ajaloost*. Tallinn: Koolibri.

Micheli, Marina; Christop, Lutz & Büchi, Moritz (2018) “Digital Footprints: An Emerging Dimension of Digital Inequality.” *Journal of Information, Communication and Ethics in Society* 16(3): 242–251.

Milaj, Jonida (2015) „Invalidation of Data Retention Directive – Extending the Proportionality Test.“ *Computer Law & Security Review* 31(5): 604–617.

Milaj, Jonida (2016) „Privacy, Surveillance, and the Proportionality Principle: The Need for a Method of Assessing Privacy Implications of Technologies Used for Surveillance.“ *International Review of Law, Computers & Technology* 30(3): 115–130.

Mitrou, Lilian (2007) „Communications Data Retention: A Pandora’s Box for Rights and Liberties?“ Raamatus *Digital Privacy: Theory, Technologies, and Practices*, toim. Aquisti, Alessandro; Gritzalis, Stefanos, Lambrinoudakis, Costos & di Vimercati, Sabrina. Auerbach Publications, 410–430.

Montpetit, Eric (2011) „Between Detachment and Responsiveness: Civil Servants in Europe and North America.“ *West European Politics* 34(6): 1250–1271.

Morgan, Steve (2019) „2019 Official Annual Cybercrime Report. Cybersecurity Ventures.“ Herjaveck Group. https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/ (külastatud: 20.03.2021)

Neocleous, Mark (2007) „Security, Liberty and the Myth of Balance: Towards a Critique of Security Politics.“ *Contemporary Political Theory* 6(2): 131–149.

Nurse, Jason R. C. (2018) „Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit.“ Raamatus *The Oxford Handbook of Cyberpsychology. Publisher: Oxford University Press*, toim. Atrill-Smith, Allison; Fullwood, Chris; Keep, Melanie & Kuss, Daria J.

Ochodek, Tomaś (2018) „The Interpretaton of the Charter of Fundamental Rights of the EU in Data Retention Cases: national implementation and possible changes of policy.“ *Acta Universitatis Carolinae – Iuridica* 4: 143-154.

O'Neil, Michael (2001) „Cybercrime Dilemma: Is it Possible to Guarantee Both Security and Privacy?“ *Brookings*: *https://www.brookings.edu/articles/cybercrime-dilemma-is-it-possible-to-guarantee-both-security-and-privacy/* (külastatud 01.05.2021)

Osborne, Stephen P. (2006) „The New Public Governance.“ *Public Management Review* 8(3): 377–87.

Ovsjannikov, Mihhail F. (1974) *Hegel*. Sarjast „Suuri mõtlejaid“. Tallinn: Eesti Raamat.

Owen, Taylor (2004) „Challenges and Opportunities For Defining and Measuring Human Security.“ *Human Rights, Human Security and Disarmament*, disarmament forum 3: 15–24.

Parti, Katalin (2011) „Actual Policing in Virtual Reality – A Cause of Moral Panic or a Justified Need?“ Raamatus *Virtual Reality*, toim. Kim, Jae-Jin. IntechOpen, 647-672.

Pau, Aivar (2020) „Valitsus tõukab Eesti mitme pika sammu võrra kontrollimisühiskonna poole – likvideeritakse isikustamata kõnekaardid ja suhtlusprogrammid lähevad võimu kontrolli alla.“ *Forte*, 19. oktoober. https://forte.delfi.ee/news/tarkvara/valitsus-toukab-eesti-mitme-pika-sammu-vorra-kontrollimisuhiskonna-poole-likvideeritakse-isikustamata-konekaardid-ja-suhtlusprogrammid-lahevad-voimu-k?id=91396045 (külastatud 16.05.2021)

Pavone, Vincenzo & Pereira-Puga, Manuel (2009) „The Privacy vs Security Dilemma in a Risk Society: Insights From the PRISE Project on the Public Perception of New Security technologies in Spain.“: 109–127

Pelczynski, Zbigniew, A. (1984) „*Political community and individual freedom in Hegel's philosophy of state*.“ https://www.marxists.org/reference/subject/philosophy/works/ot/pelczyns.htm (külastatud 20.02.2021)

Peters, Allison & Jordan, Amy (2020) „Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime“ *Journal of National Security Law and Policy*: 487–524. https://jnslp.com/2020/02/13/countering-the-cyber-enforcement-gap-strengthening-global-capacity-on-cybercrime/ (külastatud 12.05.2021)

Porcedda, Maria G. (2017) „The Manifold Significance of Citizens' Legal Recommendations on Privacy, Security and Surveillance.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 191.212.

Prokuratuur (2020) Aastaraamat. Küberkuritegevuse ökosüsteem on muutunud teenusepõhiseks. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2020/kuberkuritegevuse-okosusteem-muutunud-teenusepohiseks (külastatud 01.05.2021)

Queiroz, Regina (2018) „Individual Liberty and the Importance of the Concept of the People.“ Human & Social Sciences Communications 4: artikkel nr 99.

Rauhofer, Judith (2008) „Privacy is Dead, Get Over it! Information Privacy and the Dream of a Risk-free Society.“ *Information & Communications Technology Law* 17(3): 185–197.

Rauhofer, Judith (2008) „Privacy is Dead, Get Over it! Information Privacy and the Dream of a Risk-free Society.“ *Information & Communications Technology Law* 17(3): 185–197.

Rowe, Frantz (2020) „Contact Tracing Apps and Values Dilemmas: A Privacy Paradox in a Neoliberal World.“ *International Journal of Information Management* 55: 1–5.

Rubenfeld, Jed (2008) „The End of Privacy.“ *Faculty Scholarship Series*. 1552: https://digitalcommons.law.yale.edu/fss_papers/1552 (külastatud 01.05.2021)

Samier, Eugenie (2001) „Demandarinisation in the New Public Management: Examining Changing Administrative Authority from a Weberian Perspective.“ Raamatus *Max Webers herrschaftssoziologie: studien zu entstehung und wirkung*, toim. Hanke, Edith & Mommsen, Wolfgang J. Tübinger: Mohr/Siebeck, 235-263

Schmitt, Michael N. (2017) *Tallinn Manual 2.0.* Cambridge University Press.

Shamsi, Jawwad A.; Zeadally, Sherali; Sheikh, Fareha & Flowers, Angelyn (2016) „Attribution in Cyberspace: Techniques and Legal Implications.“ *Security and Communication Networks*. 9(15): 2886–2900.

Shaw, Carl K. Y. (1992) „Hegel's Theory of Modern Bureaucracy.“ *American Political Science Review* 86(2): 381–389.

Smith, Matthew & Green, Matthew (2016) „A Discussion of Surveillance Backdoors: Effectiveness, Collateral Damage, and Ethics.“ https://www.vr-elibrary.de/doi/abs/10.14220/9783737007627.131 (külastatud 19.04.2021)

Solove, Daniel J. (2008) „Data Mining and the Security-Liberty Debate.“ *The University of Chicago Law Review* 75(1): 343–362.

Solove, Daniel J. (2011) *Nothing to Hide: The False Tradeoff between Privacy and Security.* New Haven & London: Yale Univeristy Press.

Somody, Bernadette; Szabó, Máté Dániel & Székely, Iván (2017) „Moving Away From the Security-Privacy Trade-Off: The Use of the Test of Proportionality in Decision Support.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 155–176.

Spadafora, Anthony (2020) „Millions of Facebook users have data exposed online.“ *TechRadar*, 11. märts https://www.techradar.com/news/millions-more-facebook-users-have-their-data-exposed-online (külastatud 18.03.2020)

Stratton, Greg; Powell, Anastasia & Cameron, Robin (2016) „Crime and Justice in Digital Society: Towards a ‘Digital Criminology’?“ *International Journal for Crime, Justice and Social Democracy* 6(2): 17–33.

Strauß, Stefan (2017) „A Game of Hide-and-Seek? Unscrambling the Trade-Off Between Privacy and Security.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 255–272.

Strickland, Lee S. & Hunt, Laura E. (2005) „Technology, Security and Individual Privacy: New Tools, New Threats and the New Public Perceptions.” *Journal of the American Society for Information Science and Technology* 56(3): 221–234.

Sundquist, Matthew L. (2012) „Online Privacy Protection: Protecting Privacy, the Social Contract, and the Rule of Law in the Virtual World.“ *Regent University Law Review* 25: 153–183.

Szabados, Tamas (2015) „’Precedents’ in EU Law – The Problem of Overruling.“ *ELTE Law Journal.* https://eltelawjournal.hu/precedents-eu-law-problem-overruling/ (külastatud 06.02.2021)

Zanetti, Lisa A. & Adams, Guy B. (2000) „In Service of the Leviathan: Democracy, Ethics and the Potential for Administrative Evil in the New Public Management.“ *Administrative Theory & Praxis* 22(3): 534–554.

Zmudzinski, Adrian (2020) „Trident Crypto Fund data preach: 266, 000 passwords stolen.“ *Cointelegraph*, 06. märts. https://cointelegraph.com/news/trident-crypto-fund-data-breach-266-000-passwords-stolen (18.03.2020)

Tabansky, Lior (2012) „Cybercrime: A National Security Issue?“ *Military and Strategic Affairs* 4(3): 117–136.

Taylor, Nick (2014) „To Find the Needle Do You Deed the Whole Haystack? Global Surveillance and Principled Regulation.“ *The International Journal of Human Rights* 18(1): 45–67

Tehrani, Pardis M.; Manap, Nazura A. & Taji, Hossein (2013) „Cyber Terrorism Challenges: The Need for a Global Response to a Multi-Jurisdictional Crime.“ *Computer Law & Security Review* 29(3): 207–215.

Toomla, Rein toim. (1990) *Tekste poliitikateaduse klassikast*. Tartu: Tartu Ülikool.

Tracol, Xavier (2014) „Legislative Genesis and Judicial Death of a Directive: The European Court of Justice Invalidated the Data Retention Directive (2006/24/EC) Thereby Creating a Sustained Period of Legal Uncertainty About the Validity of National Laws which Enacted it.“ *Computer Law & Security Review* 30(6): 736–746.

Tracol, Xavier (2017) „The Judgment of the Grand Chamber Dated 21 December 2016 in the Two Joint Tele2 Sverige and Watson Cases: The Need for a Harmonised Legal Framework on the Retention of Data at EU Level.“ *Computer Law & Security Review* 33(4): 541–552.

Tsiftsoglou, Anna (2011) „Surveillance in Public Spaces as a Means of Protecting Security: Questions of Legitimacy and Policy“ Raamatus *Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices*, toim. Psygkas, Athanasios & Akrivopoulou, Christina. IGI Global, 93–102.

Van Brakel, Rosamunde & De Hert, Paul (2011) „Policing, Surveillance and Law in a Pre-crime Society: Understanding the Consequences of Technology Based Strategies.“ *Journal of Police Studies* 20(3): 163–192.

Van Der Broek, Ooms, Merel; Friedewald, Michael; van Lieshout, Marc & Rung, Sven (2017) „Privacy and Security: Citizens' Desires for an Equal Footing.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 15–35.

Van Lieshout, Marc; Friedewald, Michael; Wright, David & Gutwirth, Serge (2013) „Reconciling Privacy and Security.“ *Innovation: The European Journal of Social Science Research* 26(1/2): 119–132.

Vedaschi, Arianna & Lubello, Valerio (2015) „Data Retention and its Implications for the Fundamental Right to Privacy.“ *Tilburg Law Review* 20: 14–34.

Vermeersch, Hans & De Pauw, Evelien (2017) „The Acceptance of New Security Oriented Technologies: A 'framing' Experiment.“ Raamatus *Surveillance, Privacy and Security: Citizens Perspectives*, toim. Friedewald, Michael et al. London & New York: Routledge, 52–70.

Välisministeerium (2021) „Ülevaade Eesti Osalemistest Euroopa Liidu kohtu ja EFTA Kohtu Menetlustes Eesti vastu Algatatud Rikkumismenetlustest ja Projekti „EU PILOT“ Päringutest aastal 2020. https://vm.ee/et/euroopa-liidu-kohus (külastatud 20.03.2021)

Waiton, Stuart (2010) „The Politics of Surveillance: Big Brother on Prozac.“ *Surveillance & Society* 8(1): 61–84.

Waldron, Jeremy (2003) „Security and Liberty: The Image of Balance.“ *The Journal of Political Philosophy* 11(2): 191–210.

Walt, Stephen M. (1991) „The Renaissance of Security Studies.“ *International Studies Quarterly* 35(2): 211–239.

Wasik, Martin (2010) „The Emergence of Computer Law.“ Raamatus *Handbook of Internet Crime*, toim. Jewkes, Yvonne & Yar, Majid. USA & Canada: Willan Publishing, 395–412.

Wasserfallen, Fabio (2010) „The Judiciary as Legislator? How the European Court of Justice Shapes Policy-making in the European Union.“ *Journal of European Public Policy* 17(8): 1128–1146.

Wall, David S. (2010) „Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'.“ Raamatus *Handbook of Internet Crime*, toim. Jewkes, Yvonne & Yar, Majid. USA & Canada: Willan Publishing, 88–103.

Weimann, Gabriel (2016) „Going Dark: Terrorism on the Dark Web.“ *Studies in Conflict and Terrorism* 39(3): 195-206.

Wells, Helen & Wills, David (2009) „Individualism and Identity: Resistance to Speed Cameras in the UK.“ *Surveillance & Society* 6(3): 259–274.

Westin, Alan F. (2003) „Social and Political Dimensions of Privacy.“ *Journal of Social Issues* 59(2): 431–453.

Williams, Katherine S. (2010) „Transnational Developements in Internet Law.“ Raamatus *Handbook of Internet Crime*, toim. Jewkes, Yvonne & Yar, Majid. USA & Canada: Willan Publishing, 466–491.

Wolff, Jonathan (2005) *Sissejuhatus poliitikafilosoofiasse.* Tartu: Tartu Ülikooli kirjastus.

ÜHISTEATIS EUROOPA PARLAMENDILE JA NÕUKOGULE ELi küberturvalisuse strateegia digikümnendi jaoks. JOIN/2020/18 final. https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52020JC0018 (külastatud 19.12.2020)

Lisa 1. Ankeetküsimustik

I – Õiguskaitse muutumine ajas

Traditsiooniliselt on omanud jõumonopoli üksnes riik. Lähiminevikust leiab näiteid, mis ilmestavad õiguskaitse mõningat erastamist (Eestis näiteks plekimõlkimiste lahendamise delegeerimine kindlustusfirmadele). Seevastu on virtuaalne turvalisus osaliselt otseselt sõltuv erasektori poolt pakutaast turvatarkvarast. Eriti levinud on erasektori ja eradetektiivide kaasamine Ameerika Ühendriikides, kuivõrd ettevõtete hinnangul ei suuda riik küberruumis nende turvalisust ja ohutust tagada.

1. Demokraatlikus ühiskonnas on välja kujunenud, et kõikidel inimestel on nende õiguste rikkumise korral õigus riigi poolsele kaitsele. Kas Te nõustute selle kontseptsiooniga?

A) Jah B) Ei (selgitus):

2. Kas Teie hinnangul võib mõtestada kodanike õiguste kaitset kui igaühe õigusena, teenusena või millegi muuna? Vajadusel selgitage.

A) Õigus B) Teenus (selgitus):

3. Kas Teie hinnangul peaks riik tehnoloogia arengu ja küberkuritegevuse paljususe tingimustes vähem prioriseerima kergemaid rikkumisi? Võimalusel nimetage.

A) Jah B) Ei (selgitus):

4. Kas Teie oleksite valmis õiguskaitse, nt Politsei väljakutsete eest tasuma? Vajadusel selgitage.

A) Jah B) Ei (selgitus):

5. Kas Teie hinnangul oleks põhjendatud, et erasektori ettevõte saaks riiklike õiguskaitseorganitega (nt Politsei) analoogsed õigused ja kohustused (nt sunni kohaldamine, andmete analüüsimine kuritegude lahendamiseks, jälitusõigused jne)?

A) Jah B) Ei C) Üksnes teatud õigusrikkumiste osas

6. Kas erinevate tehnoloogiast tingitud ja ajas avalduvate uute ohtude osas tuleks Teie hinnangul pigem

A) Riigil kohaneda uute ohtudega, et võimaldada kodanikele nende õiguste kaitse sõltumata tingimustest.

B) Kodanikel tuleks eelkõige ise ohtudega kohaneda ja vastutada oma individuaalse heaolu eest.

(selgitus)

7. Milline nendest omadustest on Teile õiguskaitseasutuste tegevuste vaatest kõige olulisem? Reastage 4 - kõige olulisem, 3, 2, 1 - kõige vähem olulisem.

A) **Kiirus** (kuriteo lahendamiseks kuluv ajaline maht) ( )
B) **Suutlikkus** (võimalikkus igat liiki õigusrikkumist nii teoreetiliselt kui praktiliselt lahendada) ( )
C) **Tulemus** (suutlikkus tabada võimalikult palju õigusrikkujaid) ( )
D) **Õiglus** (igat ohvrit koheldakse võrdselt ning tagatakse võrdne õiguste kaitse) ( )

II – Õiguskaitseasutuste tegevus virtuaal- ehk küberruumis.

Isikute andmete kaitse vaatest on tehnoloogiaajastul avaldunud oluline probleem: küberkuritegevuse tõkestamine hõlmab endas ulatuslikku andmete analüüsi nii kurjategijate kui võimalike ohvrite tuvastamiseks. Seetõttu on domineeriv akadeemiline ning inimõiguste gruppide poolne väide, et riigi tegevus virtuaalruumis kuritegevust menetledes vähendab olulisel määral isikute privaatsust.

8. Kas Teie hinnangul on virtuaalruum võrreldes füüsilise maailmaga analoogselt reguleeritud?

A) Jah B) Ei (selgitus)

9. Kas Teie hinnangul peaks virtuaalruum võrreldes füüsilise maailmaga olema analoogselt reguleeritud?

A) Jah B) Ei (selgitus)

10. Kas Teie hinnangul on kurjategijatel võimalik tunda end turvalisemalt füüsilises või virtuaalses ruumis?

A) Füüsilises ruumis B) Virtuaalses ruumis

11. Kas Teie hinnangul peaksid õiguskaitseasutused olema suutelised tagama kaitse isiku õiguste rikkumisel virtuaalruumis samal määral kui füüsilises ruumis?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

12. Kas Teie hinnangul on õiguskaitseasutused suutelised tagama inimeste õiguste rikkumine virtuaalruumis samal määral kui füüsilises ruumis?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

13. Kas Teie hinnangul suudab riik virtuaalruumis toimuva kuritegevusega sammu pidada?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

14. Kas nõustute P. Burgessi (2008) iseloomustusega, et "privacy has metamorphosed from being the object of security to a very threat to security"? "Privaatsus on muutunud kaitsealusest väärtusest väärtuseks, mis turvalisust ohustab".

A) Nõustun B) Pigem nõustun D) Pigem ei Nõustu E) Ei nõustu

15. Kas Teie hinnangul sideandmete säilitamine sideettevõtete poolt (elektroonilise side seaduse § 1111) võimaldab õiguskaitseasutustel virtuaalruumis inimeste turvalisust tõhusamalt tagada?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

16. Kas Teie hinnangul sideandmete säilitamine sideettevõtete poolt vähendab automaatselt iga kliendi individuaalset privaatsust?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

17. Kas Teie hinnangul sideandmete säilitamine eraettevõtete poolt võimaldab õiguskaitseasutustel lisaks inimeste turvalisusele tagada ka inimeste privaatsust?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

18. Kas Teie hinnangul peaks riik õiguskaitseasutuste näol suutma senisest tõhusamalt tõkestada küberruumis toimuvat kuritegevust?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

19. Milline alljärgnevatest elementidest on Teile virtuaalkeskkonnas kõige enam tajutav? Reastage: 4 - enim tajutav, 3, 2, 1 - vähim tajutav.

A) **Anonüümsus ja privaatsus** ( )
B) **Tasuta ja piiramatu ligipääs informatsioonile** ( )
C) **Tegevusvabadus** ( )
D) **Ohutu keskkond** ( )

20. Riik sätestab seadusega ettevõtetele küberturbe miinimumreeglid. Millise väitega Te enim nõustute? Reastage: 4 - nõustun enim, 3, 2, 1 - nõustun vähimal määral.

A) Nõuete sätestamisega vähendab riik erasektori ettevõtlusvabadust ( )
B) Nõuete sätestamine võimaldab paremini kaitsta ettevõtte ja tema klientide turvalisust ( )
C) Nõuete sätestamine võimaldab paremini kaitsta ettevõtte ja tema klientide turvalisust ja privaatsust ( )
D) Nõuete sätestamine ei võimalda ühtegi eelnevat ( )

III – Individuaalsed õigused ja vabadused

Tehnoloogia arengut ja selle kasutamist eelkõige riikide poolt nii turvalisuse kui julgeoleku tagamisel on peetud üheks suurimaks ohuks inimeste põhiõiguste ja vabaduste säilimisele. Seetõttu on läbiv mehhanism poliitikate loomisel "tasakaalustamine" ehk erinevate asjaolude arvestamine ning "proportsionaalsus" ehk mingi poliitika põhjendatus (vajalikkus, eesmärgipärasus, mõõdukus) probleemi lahendamiseks.

21. Kas Teie hinnangul tähendab vabaduste (nt privaatsuse) riivamine vabaduste vähenemist?

A) Nõustun B) Pigem nõustun D) Pigem ei nõustu E) Ei nõustu

22. Mis vähendab Teie hinnangul enim Teie isiklikke õiguseid ja vabadusi?

A) Kui riik/seadus ei luba mul mingeid tegevusi teha

B) Kui riik/seadus ei võimalda ega loo mulle tingimusi mingite tegevuste tegemiseks

C) Kui ma ise ei suuda mingeid tegevusi teha

23. Kas Teie hinnangul seadused, maksud ja kohustused riigi ees pigem:

A) Vähendavad minu isiklikku vabadust

B) Piiravad minu isiklikku vabadust

C) Võimaldavad mulle läbi hüvede isikliku heaolu ja selle kvaliteedi

24. Kas Teie hinnangul vähendab teie isiklikku privaatsust enim:

A) Kui riik minu andmeid õiguspäraselt kogub

B) Kui riik minu andmeid õiguspäraselt töötleb

C) Õiguspärane kogumine ega töötlemine ei vähenda minu isiklikku privaatsust

25. Teie vastu on pandud toime pandud kuritegu. Kas Teie hinnangul rikub riik rohkem Teie õiguseid, kui:

A) Riik kuriteo lahendamiseks minu ja võimalike kahtlusaluste andmeid töötleb

B) Kui riik ei suuda õigusrikkujat tuvastada ega minu turvalisust tagada

26. Millise väitega Te rohkem nõustute?

A) Riigil on õigus sätestada isikuandmeid haldavatele ettevõtetele kohustused küberturbe meetmete rakendamiseks ja seeläbi ettevõtete turvalisuse ja toimepidevuse suurendamiseks.
B) Riigil on õigus sätestada isikuandmeid haldavatele ettevõtetele kohustused küberturbe meetmete rakendamiseks klientide andmete ja privaatsuse kaitsmiseks.
C) Väited ei ole sisuliselt erinevad.

27. Millise väitega Te rohkem nõustute?

A) Rendifirmast auto rentimisel on õigustatud isikuandmete registreerimine. Õnnetuse või kuriteo tingimustes on riigil õigus eraettevõttelt neid andmeid küsida.
B) Kõnekaardi ostmisel on õigustatud kõnekaardi sidumine konkreetse isikuga. Õnnetuse või kuriteo puhul on riigil õigus eraettevõttelt neid andmeid küsida.
C) Väited ei ole sisuliselt erinevad.

28. Millise väitega Te enim nõustute? Reastage: 4 - nõustute enim, 3, 2, 1 - nõustute vähimal määral.

A) Teie privaatsust vähendab enim, kui Teid eraisikute poolt füüsilises ruumis jälgitakse ja pealt kuulatakse ( )
B) Teie privaatsust vähendab enim, kui Teid riigi poolt füüsilises ruumis jälgitakse ja pealt kuulatakse ( )
C) Teie privaatsust vähendab enim, kui sideettevõtted Teie andmeid teenuse osutamisel säilitavad ( )
D) Teie privaatsust vähendab enim, kui virtuaalruumis on eraettevõtte andmelekke läbi saanud teada Teie isiklikud andmed, kasutajakontod ja paroolid ()

4.3. Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina

_____

(*autori nimi*)

(isikukood: _____)

annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose

_____

_____

_____,

(*lõputöö pealkiri*)

mille juhendaja on _____,

(*juhendaja nimi*)

1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace'is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

2. üldsusele kättesaadavaks tegemiseks ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace'i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni;

3. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile;

4. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus/Tallinnas/Narvas/Pärnus/Viljandis, _____ (*kuupäev*)

_____(*allkiri*)