Sisekaitseakadeemia

Sisejulgeoleku instituut

Marit Laats

PIIRIÜLESTE JÄLITUSTOIMINGUTE LÄBIVIIMINE DIGITAALKESKKONNAS

Magistritöö

Juhendaja:

Tanel Järvet, MA

Tallinn 2017

SISEKAITSEAKADEEMIA MAGISTRITÖÖ ANNOTATSIOON

Sisejulgeoleku instituut	Kaitsmise kuu ja aasta: juuni 2017

Töö pealkiri eesti keeles: Piiriüleste jälitustoimingute läbiviimine digitaalkeskkonnas
Töö pealkiri võõrkeeles: Cross-Border Surveillance Activities Carried out in the Digital Enviroment
Lühikokkuvõte: Töö on kirjutatud eesti keeles, eesti- ja inglise keelse kokkuvõttega. Töö koos lisadega on esitatud 82-l leheküljel, millest töö põhiosa moodustab 80 lehekülge. Andmete illustreerimiseks on kasutatud 1 joonist ja 16 tabelit.

Magistritöö eesmärk on välja selgitada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohad ja esitada uurimispõhiselt rakendusettepanekuid nende lahendamiseks. Magistritöö eesmärgi saavutamiseks ja uurimisülesannete täitmiseks kasutati uurimisstrateegiana võrdlevat juhtumiuuringut, mille käigus viidi läbi dokumendianalüüsi, milles analüüsiti Euroopa Inimõiguste Kohtu, Euroopa Liidu Kohtu ja Eesti kohtute otsuseid. Dokumendianalüüsi täiendamiseks ja edasiarendamiseks viidi läbi poolstruktureeritud ekspertintervjuud. Kogutud arvamusi võrreldi omavahel ja kõrvutati teoreetiliste seisukohtadega ja dokumendianalüüsi tulemustega, mille põhjal tehti ettepanekuid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohtade lahendamiseks.

Uurimistöös jõuti järeldusele, et suurimad probleemid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise regulatsioonis on EL-i õiguse ebapiisav ülevõtmine, riigisisese õiguse kohaldamata jätmine vastavalt uutele reeglitele, riigisisese õiguse vastuolu või õiguslikult reguleerimata olukord. Samuti õigusabipalvete süsteemi mittesobivus digitaaltõendite kogumiseks, digitaalkeskkonnas „asukoha puudumise“ võimalus ja menetlejate IT alase teadlikkuse puudulikkus.

Magistritöös läbi viidud uuringu tulemusena tehakse ettepanekuid, mis aitaksid lahendada digitaalkeskkonnas piiriüleste jälitustoimingute probleemkohti.

Lisad: Ekspertintervjuude küsimustik, Nvivo11 väljavõte koodipuust

Võtmesõnad: piiriülene kuritegevus, jälitustoiming, piiriülesed jälitustoimingud, rahvusvaheline koostöö, digitaaltõend, jälitustoimingud digitaalkeskkonnas, inimõigused.

Võõrkeelsed võtmesõnad: cross-border crime, surveillance, cross-border surveillance, transnational cooperation, digital evidence, digital surveillance, human rights.

Magistritöö seos riiklike arengukavade ja prioriteetidega: Siseministeerium valitsemisala arengukava 2014-2017; Siseturvalisuse arengukava 2015-2020; Välisministeeriumi arengukava 2015-2018, Küberjulgeoleku strateegia 2014-2017.

Säilitamise koht:

Töö autor: Marit Laats

Olen koostanud magistritöö iseseisvalt. Kõik magistritöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujalt allikatest saadud info on nõuetekohaselt viidatud. Olen nõus oma magistritöö avaldamisega elektroonilises keskkonnas.

Allkiri:

Vastab magistritöö nõuetele

Juhendaja: Tanel Järvet Allkiri: (allkirjastatud digitaalselt)

Kaitsmisele lubatud

Sisejulgeoleku instituudi
juhataja: Ivo Juurvee Allkiri:

SISUKORD

MÕISTETE JA LÜHENDITE LOETELU

24/7 – arvutikuritegevusevastane ööpäeva ringne rahvusvaheline kiirkoostöö võrgustik (Arvutikuritegevusevastane konventsioon, 2004)

EIK – Euroopa Inimõiguste Kohus

EIÕK – Euroopa Inimõiguste ja põhivabaduste kaitse konventsioon

EK – Euroopa Liidu Kohus

EL – Euroopa Liit

ESS – elektroonilise side seadus

JIT - Ühised uurimisrühmad (inglise keeles *Joint Investigation Teams*)

JSB – Ühine järelevalveasutus (inglise keeles *Joint Supervisory Body*)

ISP – Internetiteenusepakkujad (inglise keeles *Internet Service Provider*)

IT – Infotehnoloogia, käesolevas töös peetakse selle all silmas ka kommunikatsioonitehnoloogiat.

KrMS – kriminaalmenetluse seadustik

MTA – Maksu- ja Tolliamet

PPA – Politsei- ja Piirivalveamet

PS – Eesti Vabariigi põhiseadus

„Asukoha puudumine“ (inglise keeles *loss of location*) – pilveandmetöötlusega tulemusel andmete täpse aukoha teadmise puudumine (Spoenle, 2010)

Küberkuritegevus - kuriteod, mis on pandud toime elektrooniliste sidevõrkude ja infosüsteemide abil või selliste võrkude või süsteemide vastu. (Euroopa Liidu Teataja, 2007)

Piiriülene kuritegevus - illegaalne käitumine, mille tegu, vahend või tagajärg ulatub teise riigi jurisdiktsiooni ning mille tõkestamiseks või avastamiseks on vaja riikidevahelist koostööd (Ering, 2011; Euroopa Liidu Teataja, 2009a; Passas, 2002; Porter, 1996; Saar, et al., 2003 põhjal magistritöö autori koostatud).

Pilvandmetöötlus - (inglise keeles *cloud computing*) korral pilveteenuse kasutaja salvestab, varundab või töötleb andmeid serverites, millele kasutajal on interneti vahendusel juurdepääs spetsiaalse tarkvara abil. Tarkvara kasutusliideseks on reeglina veebilehitseja (Parm, 2014) (nt Google või Outlook).

Pilveteenus – pilvetehnoloogia poolt võimaldatav pilves (interentis) kasutatav teenus (nt e-postiteenus, suhtlusvõrgud, tekstitöötlusvahendid, ajaplaneerijad, kalendrid, dokumentide failihaldusüsteemid). (Parm, 2014)

TOR – browser - tarkvara, mis kaitseb kasutajat "põrgatades" ühendust ringi hajutatud releede võrgus, mida juhivad vabatahtlikud üle maailma. Selle eesmärgiks on ennetada, et keegi saaks vaadelda isiku interneti ühendust tema külastatud veebilehekülgede kaudu. Samuti ei lase see isiku külastatud veebilehtedel tuvastada isiku füüsilist asukohta ja võimaldab pääseda ligi blokeeritud veebilehtedele. (The Tor Project, 2016)

Ultima ratio – viimne vahend

SISSEJUHATUS

Tehnoloogia kiire areng, pakub uusi võimalusi majanduskasvuks ja muudab oluliselt inimeste omavahelist suhtlemist. Nende muutustega kaasnevad ka uued julgeolekuprobleemid. Üha rohkem valmistab muret küberkuritegevus, järjest keerukamaks on muutumas inimkaubandus, uusi vorme võtab piiriülene organiseeritud kuritegevus ja endiselt ohustab julgeolekut terrorism. Euroopa Liit (edaspidi EL) on seisukohal, et julgeoleku tagamiseks peab kasutama tehnoloogilisi uuendusi ja teadussaavutusi (nt EL'i programm Horisont 2020), sest need aitavad kuritegevusega kaasnevaid ohte kõrvaldada. (Euroopa Komisjon, 2014)

Tänapäeval liigub suurem osa infost internetti kasutades ja telefoni teel vestluse käigus (Euroopa Liidu Nõukogu, 2016), seetõttu peab arvestama, et jälitustoiminguid peab läbi viima digitaalkeskkonnas. Tänapäeval, kiiresti muutuvas maailmas, on õiguskaitseorganitel üha suuremaks probleemiks kuritegevus digitaalses keskkonnas – internetis, kuid sellealane ettevalmistus ametnikel puudus. Eestis lisati alles paar aastat tagasi digitaaltõendi käsitlemise õpe politseinike õppekavasse. (Sisekaitseakadeemia, 2013)

Jälitustoimingute läbiviimise eesmärk on julgeoleku tagamine riigis (Lott, 2015), mille täitmiseks läheb aina rohkem vaja rahvusvahelist koostööd (Euroopa Komisjon, 2010). Vaieldamatult on rahvusvaheline koostöö vajalik, kuid oluline küsimus on õige lahenduse leidmine igal konkreetsel juhul, kui ühel pool on kaalukausil riigi rahvusvahelised kohustused ja teisel pool üksikisiku õigused. See, milles mingeid järeleandmisi aga teha ei tohi, on kriminaalmenetluse kvaliteet. See tähendab tõendite head kvaliteeti, põhiõiguste austamist, juriidilist korrektsust, menetluste läbimõeldust, aga ka jälitustoimingute läbiviijate professionaalsust. (Perling, 2014)

Käesolev magistritöö on **aktuaalne**, sest kiire virtuaalmaailma arenguga on ka kuritegevus laienenud küberruumi, mille tõttu on jälitustoimingute teostamise puhul äärmiselt oluline rahvusvaheline koostöö (Justiitsministeerium, 2010). Kaasaegne tehnoloogia on oluliselt laiendanud ka jälitustoimingute läbiviimiseks võimalusi, kust kohast saada andmeid inimese ja tema käitumise kohta (Lõhmus, 2016a). Samuti näitavad digitaalkeskkonnas leitavatele tõenditele süvenemist 2013. aastal sõlmitud Tallinna Tehnikaülikooli (edaspidi TTÜ) ja Politsei- ja Piirivalveameti (edaspidi PPA) koolituskokkulepe (Hurt, 2013) ning 2014. aastal Tallinnas toimunud *CyberCrime*

konverents, mille raames avati ka TTÜ küberkriminalistika ja küberjulgeoleku keskus (Keevallik, 2014).

Kuritegevuse liikumist digitaalkeskkonda on arvesse võetud ka siseturvalisuse arengukava loomisel, mis toob raskete ja organiseeritud kuritegevusega võitluse oluliste probleemidena välja sisejulgeoleku asutuste koostöö puudulikkuse, kriminaaljälituse ebapiisava tehnilise võimekuse ja küberkuritegevusega võitlemise vahendite ja oskuste ning küberkriminalistika võimekuse puudumise (Siseministeerium, 2015). Samuti näeb küberjulgeoleku arengukava ette küberkuritegevuse vastase võitluse tõhustamist (Majandus- ja Kommunikatsiooniministeerium, 2014). Rahvusvahelise koostöö edendamise vajalikkust rõhutavad ka justiits- ja välisministeerium (Justiitsiministeerium, 2010; Siseministeerium, 2013; Välisministeerium, 2014). Lisaks Eesti siseturvalisuse arengukavadele prioritiseerib võitlust küberkuritegevuse vastu ka Euroopa julgeoleku tegevuskava. (Euroopa Liidu Teataja, 2015)

Riigipiiride valvamise muudab komplitseerituks ka Schengeni õigusruumiga liitumine 2004. aastal, mis avas Eesti riigipiirid (Schengen Facility vahendite kasutamise kord, 2011). See võimaldab ka kurjategijatele kergema liikuvuse riikide vahel, mistõttu peab olema tagatud õiguskaitseorganite võimekus ka Eesti riigi territooriumilt väljaspool asuva kurjategija teo avastamiseks. Rahvusvahelisel tasandil on küberküsimuste arutelu viimastel aastatel märkimisväärselt elavnenud. Raske on leida riiki, kellele lokkav ning organiseeruv küberkuritegevus, küberruumis toimuvad võimuvastased meeleavaldused või mõnedes riikides interneti kasutamisele kehtestatud piirangud probleeme ei tekitaks. (Tikk-Ringas, 2012)

Jälitustoimingud on alati olnud kuritegevuse vastase võitluse oluline osa (Kergandberg, et al., 2004, lk 67). Teisalt on jälitustoimingud kollisioonis inimõigustega, mis reguleerivad inimese ja riigi vahelisi suhteid ning on arengus nagu ühiskonnad ja riigidki, mistõttu tuleb neid käsitleda kooskõlas arengutega maailmas (Inimõiguste Instituut, 2012). See tähendab, et oluline on inimõiguste kaitse ka digitaalkeskkonnas. Seda tõestab Euroopa Kohtu praktika, mis on tühistanud varasemaid direktiive seoses liiga invasiivsa inimõiguste riivega. (Digital Rights Irelang ja Seitlinger jt. EKo, 2014)

Käesolev magistritöö on **uudne**, sest magistritöös keskendutakse digitaalkeskkonnas läbiviidavatele piiriülestele jälitustoimingutele. Selle valdkonna puudusi ja arenemist on välja toonud mitmed erinevad riiklikud arengukavad ja strateegiad (Justiitsministeerium, 2010; Majandus- ja Kommunikatsiooniministeerium, 2014; Siseministeerium, 2015; Välisministeerium, 2014). Kuigi

erinevatest jälitustoimingutest on kirjutatud mitmeid uurimistöid, ei ole keskendutud ei piiriülesele ega digitaalaspektile. (Krevald, 2013; Linask, 2014; Madisson, 2015). Samuti ei ole varasemalt uuritud jälitusametnike enda hinnanguid jälitusalase rahvusvahelise koostöö probleemidele. Jälitusalast rahvusvahelist koostööd on põgusalt oma uurimistöö raames käsitlenud Mari-Liis Tamme (2016), kui analüüsis ühise uurimisrühma (JIT) toimimist ja Mariana London (2011) analüüsides EL'i politsei koostöö raamotsuste ülevõtmise täitmist. Seetõttu on oluline leida vastus **uurimisprobleemile,** milliseid tõrkeid ja takistusi esineb piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas ning kuidas neid lahendada?

Magistritöö uuringuga soovitakse leida vastused järgmistele **uurimisküsimustele:**

1) Milliseid õiguslikke probleeme esineb piiriülestel jälitustoimingutel digitaalkeskkonnas?
2) Milliseid takistusi esineb praktikas digitaalkeskkonnas jälitustoimingute läbiviimisel?
3) Kuidas lahendada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevaid probleemkohti?

Magistritöö **eesmärgiks** on välja selgitada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohad ja esitada uurimispõhiselt rakendusettepanekuid nende lahendamiseks.

Eesmärgi saavutamiseks püstitatakse järgmised **uurimisülesanded**:

1) Analüüsida teoreetilisi ja õiguslikke aluseid piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas, selgitamaks välja levinumad probleemid.
2) Välja selgitada dokumendianalüüsi ja ekspertintervjuudega, milliseid tõrkeid ja takistusi esineb piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas.
3) Välja töötada ettepanekud ja soovitused digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevate probleemide lahendamiseks.

Magistritöö on kvalitatiivne uurimus (Creswelli, 2003, p. 18), mille **uurimisstrateegiana** kasutatakse võrdlevat juhtumiuuringut (Flick, 2009). Juhtumiuuringu käigus viiakse andmete kogumiseks läbi dokumendianalüüs (Flick, 2009, p. 259; Flick, 2011, p. 123) ja poolstruktureeritud ekspertintervjuud (Flick, 2009, p. 156; Simons, 2009, p. 43). Juhtumiuuringu dokumendianalüüsiga analüüsitakse Euroopa Inimõiguste Kohtu (edaspidi EIK), Euroopa Liidu Kohtu (EK), ja Eesti Vabariigi kohtute lahendeid ning selgitatakse välja piiriüleste jälitustoimingute probleemkohad.

Ekspertintervjuu küsimustiku koostamise aluseks on magistritööst tulenevad teoreetilised põhiseisukohad ja dokumendianalüüsi tulemused digitaalkeskkonnas piiriüleste jälitustoimingute rakendusprobleemide kohta. **Valimiks** (Teddlie & Yu, 2007, p 77) on PPA uurijad (jälitusametnikud), Maksu- ja Tolliameti (edaspidi MTA) uurija, Riigiprokuratuuri abiprokurör ja pangaliidu rahapesu tõkestamise ekspert, kes oma töökohustustest tulenevalt puutuvad kokku jälitustoimingute läbiviimisega digitaalkeskkonnas ja rahvusvahelise koostööga. **Analüüsimeetodina** kasutatakse andmete kvalitatiivset sisuanalüüsi. Andmete tõlgendamiseks salvestused kõigepealt transkribeeritakse (Flick, 2009, p. 299) ning seejärel tehakse Nvivo11 programmi vahendusel transkriptsioonide sisuanalüüs (Flick, 2009, pp. 323-325).

Magistritöö koosneb kahest peatükist. Töö esimeses peatükis analüüsitakse teoreetilisi käsitlusi jälitustoimingute läbiviimisest ja uuritakse rahvusvahelise koostöö ja digitaalkeskkonna mõjureid piiriüleste jälitustoimingute läbiviimisel. Töö teises peatükis kirjeldatakse empiirilise uuringu metoodikat ja selgitatakse välja rakendusprobleemid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel. Samuti esitatakse magistritöö põhilised järeldused ja tehakse rakendusettepanekuid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevate probleemide lahendamiseks.

Käesolev magistritöö annab panuse piiriülese jälitusalase koostöö edendamisele digitaalkeskkonnas, mille tõttu on oluline, et magistritöö oleks kättesaadav kõigile ega vajaks juurdepääsu piirangut.

1. PIIRIÜLESTE JÄLITUSTOIMINGUTE TEOREETILISED JA ÕIGUSLIKUD ALUSED

Magistritöö esimeses peatükis analüüsitakse teoreetilisi käsitlusi jälitustoimingute läbiviimisest ja uuritakse piiriüleste jälitustoimingute läbiviimisel rahvusvahelise koostöö ja digitaalkeskkonna mõjureid. Esimene alapeatükk keskendub jälitusteooriatele ja nende muutustele seoses digitaalmaailma arenguga. Teine alapeatükk selgitab välja piiriüleste jälitustoimingute läbiviimise õigusliku aluse ja korralduse. Digitaalkeskkonnas läbiviidavaid jälitustoiminguid fookustab kolmas alapeatükk, milles tuuakse välja jälitustoimingute erisused digitaalkeskkonnas ning olulisemad takistused selles valdkonnas.

1.1. Piiriüleste jälitustoimingute teoreetilised lähtekohad

Jälitus on olnud minevikus, on praegu ja on ka tulevikus Euroopa ühiskonna julgeoleku tagamise osa (Lipartito, 2010; Ross, 2007), mille tõttu peetakse oluliseks selle analüüsimist (Brands & Schwanen, 2014; Brunton & Nissenbaum, 2013; Clarke, 1988; Deleuze, 1992; Foucault, 2002; Galic, et al., 2017; Haggerty, 2006; Haggerty & Ericson, 2000; Lyon, 2007; Schofield, 2009; Wood, 2007; Zuboff, 2015). Kaasaegne tehnoloogia on oluliselt laiendanud ka jälitustoimingute läbiviimiseks võimalusi (Lõhmus, 2016a), mille tõttu on jälituse teoritiseerimine pidanud selle kõrval arenema. Galic, et al. (2017) jaotavad jälituse teooriad kolme kategooriasse: arhitektuurilised teooriad, infrastuktuurilised teooriad ja uus konseptualiseerimine. Käesoleva magistritöö autori hinnangul sobivad need kolm kategooriat jälitustoimingute teooriate analüüsimiseks, et anda ülevaade, kuidas on ühiskonna, ka jälitustoimingute, digitaliseerumine mõjutanud jälitusteooriaid. Nimetatud kategooriad aitavad anda parema ülevaate jälitusteooria ekspertide seisukohtadest.

Arhitektuurilise kategooria alla kuulub Bentham'i „*The Panopticon"* idee vanglast, kus läbipaistvate seintega kongide keskmeks on pime torn, mida vangid näevad ja teavad, et neid jälgitakse, kuid ei tea täpsemalt, mis hetkel ja keda (Schofield, 2009, lk 70-94). Foucault (2002, lk 70) arendas Bentham'i ideed edasi ja tema kontseptsiooni kohaselt panoptika „kirjeldab jälitustegevust kui kõike nägevat järelevaatajat", mistõttu jälitustegevuse võimalikkus on sama oluline kui jälitustegevus ise. Magistritöö autori hinnangul kriminaalmenetluse raames

digitaalkeskkonnas läbiviidavate jälitustoimingute puhul panoptika kehtib, kuna digitaalkeskkonna võimalused annavad õiguskaitseasutustele oluliselt suuremad võimalused jälitustoimingute läbiviimiseks. Samas ei kehti täielikult Foucaulti kontseptsioon, kuna jälitustoimingu eesmärk on isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest (Kriminaalmenetluse seadustik, 2016), mis tähendab, et on oluline inimese teadmatus tema suhtes jälitustoimingu läbiviimise kohta. Foucault' (2002) teooria on autori hinnangul sobilik pigem preventatiivsel eesmärgil, mitte kuritegude lahendamiseks. Kuna panoptika teooriat peetakse jälitustegevuse teooria aluseks siis järgnevad teooriad arendavad seda edasi (Lyon, 2007) või üritavad seda ümber lükata (Haggerty, 2006; Wood, 2007).

Infrastuktuuriliste jälitusteooria puhul on jälitustegevus, sh ka -toimingud näiliselt võrgustatud ja peamiselt toetuvad pigem digitaal- kui füüsilisele tehnoloogiale. (Galic, et al., 2017) Digitaaltehnoloogiad võimaldavad inimesi jälgida pikema vahemaa tagant, mistõttu antud teooria keskendub enim sellele, kuidas mitte ainult kriitiliselt analüüsida kaasagsete võrkude võimustruktuure ja kuidas jälitustoimingud võimendavad või mõnikord ka õõnestavad neid, vaid kuidas minna mööda enesedistsipliini panoptilisest efektist (Deleuze, 1992; Haggerty & Ericson, 2000; Zuboff, 2015). Kõik, mis inimene internetis teeb jätab jälje (Liiv, 2014), mis panoptilise teooria (Focault, 2002) kohaselt peaks mõjutama inimesi seaduskuulekamalt käituma, samas digitaalkeskkonna areng võimaldab kurjategijatel nii tegutseda, et nende jälgede leidmine on oluliselt raskendatud kui just mitte võimatu.

Jälitusteooria uue konspetsiooni loomisel on lähtutud kahest eelnevast teooriast. Ühiskonna digitaliseerumisega koosneb tänapäeval jälitustoimingute läbiviimine nii digitaalkeskkonna kui ka füüsilise keskkonna jälgimisega. (Galic, et al, 2017) Kahe viimase aastakümnega on võimalusd jälitustoimingute läbiviimiseks oluliselt arenenud ja uued võimalused nagu digitaalkeskkonnas andmete kogumine (inglise keeles *dataveillance)* (Clarke, 1988) on lisandunud videokaamerate kaudu jälgimisele, mitte asendanud neid. Seetõttu on tänapäeval aktuaalne ka panoptiline teooria, kuigi Focault'i konseptsioon selle teooria kohta on tänapäeva jälitusvõimalustega muutunud. (Galic, et al, 2017)

Tehnoloogia areng pole ainult avardanud võimalusi jälitustoimingute läbiviimiseks vaid inimesed saavad ka ise valida, kui palju ja kergelt nende kohta infot koguda saab. On inimesi, kes teadlikult väldivad tänavatel videokaameraid (Brands & Schwanen, 2014), või kasutavad programme, mis annavad märku kui tema arvuti süsteemi üritatakse kaugligipääsuga siseneda või programme, mis

annavad vaatlejale vale infot (Brunton & Nissenbaum, 2013). Samuti on kättesaadavad ka „asukoha puudumist“ võimaldavad pilveteenused ja anonümiseerimise programmid (Osula, 2017).

Foucault’ (2002) filosoofilise lähenemisega jälituse teoritiseerimisele on kooskõlas Lyon (2007), mis kohandab panoptika kontseptsiooni tänapäeva digitaliseeritud maailma. Deleuze (1992), Haggerty ja Ericson (2000) ning Zuboff (2015) seevastu keskenduvad jälitustoimingute läbiviimisel digitaaltehnoloogia kasutamisele üritades kõrvale jätta füüsilise jälgimise, samas kui Galic, et al. (2017) nendivad, et ühiskonna digitaliseerumisega peab jälitustoiminguid läbi viima nii digitaalkeskkonnas kui ka füüsilises keskkonnas.

Jälitustoimingute läbiviimisel tehnoloogia kasutamise ühe aspektina toovad French & Smith (2016) välja „jälituse kehastumise“ („*surveillance – embodiment“*), see tähendab, et jälitustehnoloogiad ja -süsteemid muudavad üha rohkem inimesi informatsiooni objektideks. Lyon (2001, lk 15) nimetas järelevalve ühiskonna tõusu kehade kadumise põhjuseks. Sellest tingituna teostavad õiguskaitseasutused jälitustoiminguid mitte enam füüsiliste kehade peal, vaid nende andmestatud („*datafied“)* signatuuride peal (Lyon, 2001, lk 15), mis tähendab, et tõendeid kogutakse digitaalkeskkonnas.

Gandy (1989), Marx (1988) ja Lyon (2007) toovad välja, et kuigi jälitustoimingule allutatu võib olla olemuselt ühiskonnale ohtlik, kuna on kuriteo toime pannud, siis on ka nende puhul tegemist enamaga kui lihtsalt andmete kogumiga. French & Browne (2014) lisavad, et kuigi jälgitavad võivad olla ohtlikud, tuleb arvestada, et digitaalkeskkonna eripära tõttu võib muutuda nende õigus privaatsusele haavatavamaks. Nt kui teostatakse jälitustoiminguid isiku pilvekontol, kus on ühes koos kõik tema kontaktid, emailid, kalender jne, siis võib sõltuvalt isiku tehnika kasutamise rohkusest, saada tema kohta tunduvalt rohkem infot kui reaalmaailmas isikut jälgides.

Lisaks jälitatavale saavad jälitustoimingute läbiviimisel rikutud ka kolmandate isikute põhiõigused (Õiguskantsler, 2015), kellega jälitatav suhtleb. Seetõttu peetakse jälitustoiminguid ka vajalikuks kurjuseks („*necessary evil“*), kuna tegemist on toiminguga, mis on ühest küljest kasulik ja teisest küljest ohtlik turvalisuse tagamiseks ühiskonnas (Reiner, 2000). Samas toovad Barnard-Wills ja Wells (2012) välja, et kuigi varasemalt on vajaliku kurjuse mõiste jälitustoimingute kirjeldamiseks sobinud, siis tänapäeval teabepõhise politseitöö arenguga see enam ei kehti, kuna üha enam pannakse rõhku kuritegude ennetamisele.

Käesoleva magistritöö autor nõustub pigem väitega, et jälitustoimingute läbiviimise näol on tegemist vajalikku kurjusega, mille puhul on oluline leida tasakaal isikute põhiõiguste ja

õiguskaitseasutuste tegevuse vahel (Laos, 2008a, lk 10). Samal seisukohal on ka Bhatt (2006) ja Ross (2007), et riigi kohus on tagada selline reguleeritud süsteem, mis ühest küljest kaitseks põhiõigusi, kuid teisest küljest annaks politseile piisavalt võimalusi kuritegude ennetamiseks ja avastamiseks. Selleks on vajalik järelevalve teostamine (Wills & Vermeulen, 2011).

Kuna jälituse üks põhilisemaid olemuslikke tunnuseid on salajasus (Kergandberg, 2000), sest tegemist on informatsiooni kogumisega viisil, millega sekkutakse isiku õiguste ja vabaduste kasutamisse varjatult, s.o isiku teadmata, ja eesmärgiga varjata isiku eest tema kohta andmete töötlemist (Laos, 2008a), siis olukorras, kus isik ei ole oma põhiõigusi riivavast jälitustoimingust teadlik, on praktiliselt välistatud võimalus kasutada kohtusse pöördumise põhiõigust, mistõttu peab jälitustoimingutest teavitamise süsteem ja selle üle teostatav järelevalve olema piisavalt tõhusad, vältimaks õigusest üleastumisi ja omavoli (Rondel, 2016). Eestis on kontroll jälitustoimingute üle toimunud valikuliselt jälitustoimikute põhjal, hõlmates kõikide jälitusasutuste ja ringkonnaprokuratuuride tegevust ning nende tulemusena on korraldatud mitmeid koolitusi nii prokuröridele kui ka uurimisasutuste töötajatele, et tutvustada enamlevinud probleeme ja tagada ühtlasem praktika. (Ploom, 2016)

Piiriüleste kuritegudega võitlemiseks on vaja rahvusvahelist koostööd (Euroopa Komisjon, 2010). Klassikalistest rahvusvahelise koostöö julgeoleku teooriatest sobib käesoleva tööga enim liberalistlik institutsionalism, kuna Eesti kuulumine EL'i tähendab, et selle institutsiooniline ülesehitus (Jupille & Caporaso, 1999) kehtib ka Eesti riigile ning Euroopa Kohtu varasema direktiivi tühistamine inimõiguste kaitse tugevdamiseks (Digital Rights Irelang ja Seitlinger jt. EKo, 2014) näitab EL'i liberalistlikku lähenemist (Hoye & Monaghan, 2015). Liberaalsed institutsionalistid suhtuvad riikidesse kui egoistidesse, mille tõttu ei saa kokkuleppeid hierarhiliselt täita ja riikidevaheline koostöö toimib ainult siis, kui kõik osapooled saavad sellest kasu. (Keohane, Martin, 1995) Selline suhtumine tekitab aga probleeme piiriüleste jälitustoimingute läbiviimisel - kui üks riik palub teisel jälitustoiminguid läbi viia, siis võib kasu saaja olla palve esitanud riik. Samas usuvad liberaalsed institutsionalistid, et rahvusvahelised institutsioonid ja organisatsioonid (EL, NATO) võivad suurendada ja abistada rahvusvahelist koostööd (Jackson & Sorensen, 2015).

Eeltoodust nähtub, et tehnoloogia arenguga on nii jälitustoimingute läbiviimine kui ka jälituseteooria arenenud. Autor on seisukohal, et panoptiline lähenemine (Focault, 2002) ja selle enesedistsipliini efekt võib panna keskmiste moraalinormidega inimese seaduskuulelikumalt käituma, kuid organiseeritud kuritegelik grupp, kartes, et neid võidakse jälgida, otsib pigem teise võimaluse oma tegevusega jätkamiseks, nt anonümiseerimisvõrgud. Jälitustoimingute läbiviimise

näol on tegemist vajalikku kurjusega (Reiner, 2000), mille puhul on oluline leida tasakaal isikute põhiõiguste ja õiguskaitseasutuste tegevuse vahel (Laos, 2008a, lk 10). Digitaalkeskkonna piiride puudumise tõttu on vaja piiriüleste jälitustoimingute läbiviimiseks rahvusvahelist koostööd ning seda lihtsustavate organisatsioonide vajalikkust iseloomustab enim liberalistlik institutsionalismile kohane lähenemine.

1.2. Piiriüleste jälitustoimingute läbiviimise õiguslik alus ja korraldus

Piiriülese kuritegevuse mõistet ei ole üheselt defineeritud. Erinevates uurimustes ja õigusaktides on käsitletud piiriülest kuritegevust erinevalt nii mõiste seletamisena kui ka lihtsalt kuritegude loeteluna (Ering, 2011; Euroopa Liidu Teataja, 2009a; Passas, 2002; Porter, 1996; Saar, et al., 2003). Näiteks on käsitletud piiriülest kuritegevust kui käitumist, millega rünnatakse kindlaid legaalselt kaitstud huvisid, mis on sätestatud rohkem kui ühes riigis (jurisdiktsioonis) ning mille rikkumine on karistatav kriminaalkorras rohkem kui ühes riigis (Passas, 2002). Samas TPÜ Rahvusvaheliste ja Sotsiaaluuringute Instituudi uuringus on rahvusvahelise koostöö kontekstis piiriülene kuritegevus igasugune kuritegevus, mille tõkestamiseks või avastamiseks taotleb riik teiselt riigilt teatud toimingute tegemist (Saar, et al., 2003).

Piiriülese kuritegevuse mõiste seletamist on käsitletud ka lihtsalt kuritegude loetelu koostamisena (Euroopa Liidu Teataja, 2009a; Ering, 2011). Näiteks EL'i Lissaboni leping artikkel 69b sätestab, et piiriülesteks kuritegudeks loetakse narkokuriteod, ebaseaduslik relvakaubandus, rahapesu, korruptsioon, maksevahendi võltsimine, arvutikuriteod ning organiseeritud kuritegevus. Samuti on võimalik olenevalt kujunenud olukorrast nõukogul pärast Euroopa Parlamendilt nõusoleku saamist vastu võtta otsustus täiendavate kuriteoliikide lisamiseks loetelule. (Euroopa Liidu Teataja, 2009a)

Võmalik on ka selgitada piiriülest kuritegevust nii mõiste seletamise kui kuritegude loetlemise kaudu nagu teeb seda Ering (2011, pp. 73-80) väites, et „*piiriülene kuritegevus on valik kuriteokoosseise, mille puhul toimepanija ja tagajärg ulatuvad üle territoriaalpiiri. Sellisteks tegudeks võib pidada inimkaubandust, rahapesu, narkokaubandust, relvasmuugeldamist ja -kaubandust, piiriülest terrorismi, nafta illegaalset kaubandust (oil bunkering), teemantide ebaseaduslikku kaubandust, korruptsiooni, äripettust.*"

Üldiselt mõiste seletamine kuriteo koosseisude järgi on keeruline, sest kuriteo koosseise võidakse ajaga dekriminaliseerida või ühes maailmaarenguga ja kriiside tekkimisega võivad muutuda ka

kuritegevusega võitlemise prioriteedid, näiteks digitaalkeskkonna arenguga on muutunud prioriteetseks võitlus küberkuritegevusega (Euroopa Liidu Nõukogu, 2016)

Samuti võivad muutuda kuriteo uurimise võimalused. 1996. aastal iseloomustati piiriülest kuritegevust kui tegu, mille puhul rikkuja ületab politsei volituse piiri, et panna toime kuritegu või rikkumine, mis eeldab politsei poolt uurimise läbiviimiseks riigipiiri ületamist. (Porter, 1996) Selline seletus on täielikult välja jätnud digitaalkeskkonna võimalused nii kuritegude toimepanemise kui ka nende ärahoidmise ja tõkestamise osas, kuna sellel ajal ei olnud veel see laialt levinud ning kättesaadav võimalus.

Eeltoodust lähtudes käsitleb käesoleva magistritöö autor piiriülest kuritegevust kui illegaalset käitumist, mille tegu, vahend või tagajärg ulatub teise riigi jurisdiktsiooni ning mille tõkestamiseks või avastamiseks on vaja riikidevahelist koostööd.

Piiriülene koostöö on oma olemuselt väga mitmetahuline valdkond, milles igal osapoolel on oma huvid, soovid, vajadused, nõudmised ja ka koostööst tulenevad eeldused (Tüür, 2001). Politseikoostöö ja õigusalase koostöö läbiviimise edukus seisneb seejuures selleks kasutatavates meetmetes, st kuritegevusega võitlemiseks on vaja modernseid ja sobivaid vahendeid omavaid institutsioone, ilma milleta oleks riik võimetu efektiivselt kuritegevusele vastu astuma (Bocaniala & Bocaniala, 2012).

Kahe viimase aastakümne jooksul majanduse globaliseerumisega on piiriülene kuritegevus seniolematult kõrge, kuna kriminaalid on omaks võtnud uued võimalused tehnoloogia arengus, mille tõttu on kuritegusid raske tuvastada ja takistada. (Council on Foreign Relations, 2013) Piiriülene kuritegevus moodustab hinnanguliselt 3,6% maailmamajandusest (UNODC, 2011). Selleks, et piiriülese kuritegevusega efektiivselt võidelda, on vaja parandada rahvusvahelise koostöö tõhusust, mida näeb ette ka Euroopa Komisjon muutuva maailma ohtudele ja probleemidele reageerimise arendamisel. (Euroopa Komisjon, 2010)

Selleks, et Eesti muutuva maailmaga kaasas käiks, töötatakse välja arengukavasid. Eesti Vabariigi Siseministeerium on oma arengukavas (Siseministeerium, 2013) seadnud aastatel 2014-2017 oluliseks prioriteediks just rahvusvahelise koostöö arendamise ning menetluse sujuvamaks muutmise läbi riikidevaheliste kokkulepete, rahvusvaheliste konventsioonide ja riikliku seadusandluse. Samuti rõhutatakse organiseeritud ja piiriülese kuritegevuse vastase võitluse juures rahvusvaheliste organisatsioonide politsei- ja tollikoostöö instrumentide kasutamist ja arendamist (Justiitsministeerium, 2010). Sellisteks koostöö instrumentideks on näiteks ühised uurimisrühmad

(edaspidi JIT) (Euroopa Liidu Nõukogu, 2015; Tamme 2016), teabe ja jälitusteabe vahetamine ja uurimismäärus (Ploom, 2010). Sellisteks instrumentideks võib pidada ka rahvusvahelisi programme koostöö edendamiseks (Arvutikuritegevusevastane konventsioon, 2004). Digitaalkeskkonnas piiriülese kuritegevuse vastu võitlemiseks on loodud näiteks 24/7 kiirkoostöövõrgustik (täpsemalt käesoleva magistritöö teooria kolmandas osas). (vt joonis 1.)

Rahvusvaheline koostöö toimib vastastikkuse tunnustamise põhimõttel (*principle of mutual recognition)* (Vernimmen-Van Tiggelen & Surano, 2008) ning seda on peetud ka Euroopa õigusruumi nurgakiviks (Euroopa Liidu Teataja, 2005a). Selle põhimõtte kohaselt tunnustatakse ja täidetakse ühe liikmesriigi poolt tehtud tõendite kogumise otsuseid teise riigi poolt ilma täiendavate eeltingimusteta ja viivitamata. Varasemalt toimis rahvusvaheline koostöö ja väljaspool EL'i toimib siiani vastastikkuse, topeltkaristatavuse vältimise ja spetsiaalsuse põhimõttel, kuid Amsterdami lepingu sõlmimisega on EL'is kohaldamisel vastastikkuse tunnustamise põhimõte. (Nilsson, 2006) Kirjeldatud kujul vastastikkuse tunnustamise põhimõtte järgimine peaks võimaldama fundamentaalsete õiguste, riikide õigussüsteemide ja liikmesriikide traditsioonide ühtlustamist, mille eesmärgiks on turvalisuse tagamine (Bindar, 2010). Selle alla kuulub ka võitlus rahvusvahelise organiseeritud kuritegevusega. (Riigikogu, 2008).

Eestis on kriminaalasjades rahvusvaheline koostöö reguleeritud kriminaalmenetlusseadustiku (edaspidi KrMS) 19 peatükis. Antud peatükk ei defineeri rahvusvahelise koostöö mõistet, vaid sätestab selle tegevuste kaudu (Kriminaalmenetluse seadustik, 2016). Käesolevas töös keskendub autor antud loetelust riikide vastastikkusele abile kriminaalasjades. Väljaspool EL'i toimub rahvusvaheline koostöö lepingute alusel ja piires. (Kriminaalmenetluse seadustik, 2016) Iga riigiga, millega soovitakse kriminaalasjade raames koostööd teha, peab eelnevalt olema sõlmitud koostöö leping, mille piires on võimalik saada õigusabi. Näiteks on Eestil tihe koostöö USA'ga tänu toimivale õigusabilepingule. (Eesti Vabariigi Valitsuse ja Ameerika Ühendriikide valitsuse vahelise lepingu vastastikusest õigusabist kriminaalasjades muutmise kokkuleppe ratifitseerimise seadus, 2006)

Euroopa Liidus on rahvusvahelise koostöö aluseks lepingud – Maastrichti (Euroopa Liidu Teataja, 1992), Amsterdami (Euroopa Liidu Teataja, 1997), Nice'i (Euroopa Liidu Teataja, 2001), Lissaboni (Euroopa Liidu Teataja, 2009a) lepingud - mis on järk-järgult loonud ühise õigusraamistiku justiits- ja siseküsimustes. Lisaks lepingutele on olulisel kohal kolm Euroopa Ülemkogu programmi, millega on paika pandud ELi peamised prioriteedid ja suunad õigusalases koostöös kriminaalasjades (London, 2011). Nendeks on Tampere (Euroopa Parlament, 1999), Haagi

(Euroopa Liidu Teataja, 2005b) ja Stockholmi (Euroopa Liidu Teataja, 2010a) programmid. Kui õigusalase rahvusvahelise koostöö vaatest oli Tampere programm loodud vastastikkuse tunnustamise põhimõtte kasutuselevõtmise juurutamise eesmärgil (Raba, 2002) ja Haagi programm tugines eelkõige õiguskaitseasutuste koostöö tugevdamisele (Euroopa Liidu Teataja, 2005b), siis Stockholmi programmi eesmärgiks oli kodanike huvid ja vajadused, eelkõige aga põhiõiguste ja –vabaduste ning isikupuutumatuse austamine samas tagades ka turvalisuse (Euroopa Liidu Teataja, 2010a). Stockholmi programmi tulemusel suurenenud õiguskaitsealane ja jälitusalane koostöö on osutunud oluliseks vahendiks, et reageerida ühistele ohtudele, nagu inimkaubandus, terrorism, küberkuritegevus ja korruptsioon. (Euroopa Komisjon, 2014)

Koostöö tagamiseks on EL loonud erinevaid ameteid ja koostöömeetmeid. Jälitustoimingutega on nendest enim seotud koostöö organisatsioonid Eurojust ja Europol (Euroopa Liit, 2015). Koostöö tõhusamaks läbiviimiseks on loodud ka erinevaid koostööinstrumente (Bindar, 2010; Parkin, 2012), millest olulisimaks antud töö kontekstis võib pidada JIT (Euroopa Liidu Teataja, 2000) ning erinevaid raamotsuseid ja direktiive (Arvutikuritegevusevastane konventsioon, 2004; Euroopa Liidu Nõukogu, 2015; Euroopa Liidu Teataja, 2006; Euroopa Liidu Teataja, 2014).

EL'i loodud koostöö organisatsioonidest on nii Eurojust kui ka Europol asutatud liikmesriikide koostöö tõhustamiseks võitluses rahvusvahelise kuritegevusega (Bindar, 2010; Parkin, 2012). Eurojust moodustati 2002. aastal Euroopa Nõukogu otsusega (Euroopa Liidu Teataja, 2002a) kui juriidilisest isikust EL asutus, kus iga liikmesriiki esindab üks liige ning, mille eesmärgiks on raskete kuritegude vastu võitlemiseks ergutada, parandada ja arendada liikmesriikide pädevate õigusasutuste vahelist koordineerimist ja koostööd. 2008. aastast on liikmesriikidel õigus osaleda ühistes uurimisrühmades, mis on seotud nende enda liikmesriigiga, sealhulgas õigus osaleda uurimisrühmade moodustamises (Euroopa Liidu Teataja, 2008a).

Euroopa Politseiamet (Europol) loodi Maastrichti lepingu jõustumise järgselt Europoli konventsiooniga (Euroopa Liidu Teataja, 2009b), et parandada liikmesriikide vahelise koostöö raames liikmesriikide pädevate ametiasutuste tõhusust ja koostööd terrorismi, ebaseadusliku uimastiäri ja muude raskete organiseeritud, rahvusvaheliste kuritegude ärahoidmiseks ning nende vastu võitlemiseks. Europolil on õigus aastast 2002 osaleda Europoli pädevuses uuritavate kuritegude puhul ühistes uurimisrühmades. (Euroopa Liidu Teataja, 2009b)

Kuna ka piiriüleste jälitustoimingute puhul on tegemist oluliselt inimõigusi riivava valdkonnaga (Kergandberg, 2000; Laos, 2008b; Rondel, 2016), on vajalik selle järelevalve. Europolil ja

Eurojustil lubatakse isikuandmeid töödelda, salvestada ja edastada nende volituste piires (Euroopa Liidu Teataja, 2008a, 2009b), mille tõttu peaks nende meetmete üle teostama järelevalvet. EL'is on selleks mitteparlamentaarsed, Europoli ja Eurojusti ühised järelevalveorganid (edaspidi JSBd). JSB on kohane järelevalvemehhanism kontrollimaks isikuandmete kasutamist politseikoostöö organisatsioonide poolt, omades juurdepääsu kõikidele failidele ja ruumidele, mis on seotud isikuandmete töötlemisega ja neil on head võimalused selleks, et tagada, et parandatakse kõik menetlused, mis rikuvad andmekaitse-eeskirju, mille tõttu ei pea EP nende tegevusi dubleerima. (Wills & Vermeulen, 2011)

Rahvusvahelise koostöö tõhusus sõltub otseselt koostöö instrumentide toimimisest (Bindar, 2010; Parkin, 2012). Üheks selliseks instrumendiks on ühine uurimisrühm (Euroopa Liidu Teataja, 2002b). Europoli ja Eurojusti kaudu saab luua ühiseid uurimisrühmasid (Euroopa Liidu Teataja, 2000, 2008a) rahvusvahelise koostöö abil kuritegude lahendamiseks juhul, kui tegemist on kuritegeliku ühendusega ning kuriteoga on seotud vähemalt kaks riiki. Eesti Vabariigis on kuritegelik ühendus defineeritud karistusseadustiku § 255 lg-s 1 (Karistusseadustik, 2016), mille kohaselt on kuritegelik ühendus kolmest või enamast isikust koosnev püsiv isikutevaheline ülesannete jaotusega ühendus, mille tegevus on suunatud esimese astme või raskemate teise astme kuritegude (min 3 aastat vangistust) toimepanemisele.

Rahvusvahelist koostööd läheb vaja ka selliste kuritegude lahendamisel, mille puhul ei ole tegemist kuritegeliku ühendusega ega loodud JIT'd. Sel juhul pöördutakse teise riigi poole õigusabipalvega jälitustoiming läbi viia (Euroopa Liidu Teataja, 2000), mille kord ja läbiviimise võimalused on sätestatud Euroopa Liidu liikmesriikide vahelises kriminaalasjades vastastikuse õigusabi konventsioonis. Antud konventsiooni 3. jaotises on lahti seletatud ka, millised on piiriülese tehnilise sidevahendi pealtkuulamise võimalused (Euroopa Liidu Teataja, 2000).

Juba vastastikuse õigusabi konventsioonis (Euroopa Liidu Teataja, 2000) on käsitletud ühiseid uurimisrühmasid, kuid kuna selle konventsiooni ratifitseerimine lükkus edasi ja vahepeal toimusid 11.09.2001 terrorirünnakud USAs, siis peale seda tehti ühiste uurimisrühmade raamotsuse loomise ettepanek (Rijken, 2006). 2002 võttiski Euroopa Nõukogu vastu raamotsuse ühiste uurimisrühmade kohta. (Euroopa Liidu Teataja, 2002b)

Ühiseid uurimisrühmasid on mõttekas koostada, kui kahes või enamas riigis tuleb paralleeslelt teostada suurel hulgal menetlustoiminguid, mis tavalise õigusabi tingimustes tähendaks iga toimingu tegemiseks õigusabitaotluse esitamist (Raba, 2002). JIT eeliseks võrreldes tavalise

rahvusvahelise koostööga saab pidada võimalust vahetult jagada teavet uurimisrühma liikmete vahel, võimalust olla menetlustomingute tegemise juures, võimalust arendada koostööd eri riikide praktikute vahel ja Europoli/Eurojusti kaasamise võimalust (Council of the European Union, 2011). Lisaks aja ja ressursi kokkuhoiule, mis kuluks õigusabiplavete esitamisele, on uurimisrühma eeliseks vahetu informatsiooni vahetus ning saadud ja vahetatavat teavet tohib kasutada eelkõige uurimisrühma eesmärgi saavutamiseks. (Ploom, 2010)

Piiriüleste jälitustoimingute läbiviimise tõhustamiseks väljaspool JIT on üheks olulisimaks instrumendiks teabe ja jälitusteabe vahetamise raamotsus (Euroopa Liidu Teataja, 2006), mis töötati välja EL'i terrorismivastase strateegia raames ja millega püütakse kindlat liiki teabe ja jälitusteabe puhul tagada õiguskaitseasutuste kiire EL - sisene vahetamine kriminaalmenetluse või jälitusmenetluse läbiviimiseks. Raamotsus on inkorporeeritud Eesti kriminaalmenetlusseadustiku 9. jaotises. (Kriminaalmenetluse seadustik, 2016) Oluline on antud raamotsuse juures asjaolu, et teabe ja jälitusteabega peetakse silmas juba olemasolevat teavet ja jälitusteavet (Euroopa Liidu Teataja, 2006) ehk seda, mida ei pea koguma. Kui käsitletav raamotsus kohustab liikmesriike vahetama teavet ja jälitusteavet, siis EL liikmesriikide vaheline juba olemasolevate ja otseselt kättesaadavate tõendite kogumine kriminaalmeneluses kasutamise eesmärgil põhineb hoopis Euroopa tõendikogumismääruse raamotsusel (Euroopa Liidu Teataja, 2008b).

Kuigi tõendikogumismäärus on loodud menetluse kiirendamiseks, ei saa seda siiski kasutada digitaalkeskkonnas jälitustoimingute läbiviimiseks, sest artikkel 4 seab tõendi kogumisele piirangud - ei saa läbi viia teabe kogumist reaalajas. (Euroopa Liidu Teataja, 2008b) Siiski on antud raamotsusega võimalik digitaalkeskkonnas jälitustoimingute käigus kogutud infot edastada, kui näiteks jälitustoimingute käigus saadakse infot teise riigi jurisdiktsioonis toime pandud või planeeritava kuriteo kohta, siis on info saanud riigil võimalus omaalgatuslikult kogutud info edastada teisele riigile kuriteo lahendamiseks või ennetamiseks (Euroopa Liidu Teataja, 2008b). Kui tõendikogumismääruse kaudu saab edastada nagu nimigi ütleb – tõendeid siis teabe- ja jälitusteabe vahetamise raamotsuse raames edastatakse informatsiooni. Kui soovitakse saadud teavet kasutada tõendina, peab selleks taotlema info edastanud riigi luba. (Euroopa Liidu Teataja, 2006)

Õigusalase koostöö edendamiseks on 2014. aastal vastu võetud direktiiv 2014/41/EL (Euroopa Liidu Teataja, 2014), mis käsitleb Euroopa uurimismäärust kriminaalasjades. Uurimismääruses sisalduva vastastikuse tunnustamise põhimõtte eesmärgiks on paremini toimiv liikmesriikidevaheline koostöö, kuid paraku ei paku see lahendust digitaalsete tõendite ajakriitilise

hankimise vajadusele, sest näeb taotluste puhul ette kuni 90-päevase vastamisaja. Uurimismääruses on käsitletud esemete, dokumentide ja andmete kogumist kriminaalmenetluses kasutamise eesmärgil, mis hõlmab võimalikult suurel määral igat liiki tõendeid, sisaldab täitmise tähtaegu ja piirab võimalikult suurel määral keeldumise aluseid. See peaks oluliselt hõlbustama rahvusvahelist koostööd. ELTL artikkel 87 lõike 2 (Euroopa Liidu Teataja, 2014) kohaselt võetakse politseikoostööga seotult vastu meetmeid seoses andmete haldamisega, personaliga ja organiseeritud kuritegevuse raskete vormide avastamisega seotud ühiste uurimismeetoditega. Kuigi Eesti oli antud määruse üks algataja, ei ole seda senini Eesti õigusesse üle võetud, sõltumata sellest, et see on seatud siseriiklikes tegevuskavades eesmärgiks. (Vabariigi Valitsus, 2011)

Kuigi EL töötab selle suunas, et kriminaalkoostöö piiriüleste jälitustoimingute läbiviimiseks oleks ühtlane ja sujuv (Euroopa Liit, 2015) (vt tabel 1), võib probleeme tekitada, kui EL'i regulatsioone sisustatakse siseriiklikult erinevalt või riikide õiguskord ise on väga erinev (Tamme, 2016). Selleks, et rahvusvaheline koostöö toimiks, peab toimima EL'is ühtne menetluspraktika ja püüdlemine samade eesmärkide poole (Euroopa Liidu Teataja, 2005b). Ka Euroopa Parlament on kritiseerinud (Euroopa Parlament, 2014; Euroopa Parlament, 2015) koostöö õigusliku raamistiku puudusi seoses sellega, et raamistik ei taga liikmesriikidele optimaalseid tulemusi ega isikute õiguste täielikku kaitset. EL-i õiguse rakendamisel ilmnenud probleemid võivad märku anda erinevatest vajakajäämistest (Mikli, 2015), milleks võivad olla nii EL-i õiguse ebapiisav ülevõtmine, riigisisese õiguse kohaldamata jätmine vastavalt uutele reeglitele, riigisisese õiguse vastuolu või õiguslikult reguleerimata olukord. Samuti on Euroopa Liidu Nõukogu (2014) uurimisrühm kokkuvõtvalt nentinud, et õigusabitaotluste süsteem on üldiselt ebaefektiivne ning digitaalsete tõendite saamiseks lausa sobimatu, takistades riigi võitlust kuritegevusega, mille menetlemiseks on vajalikud piiriülesed digitaalsed tõendid.

Eeltoodule tuginedes võib väita, et EL on loonud mitmeid erinevaid direktiive ja raamotsuseid sujuvama rahvusvahelise koostöö tagamiseks, kuid riikide endapoolne EL'i regulatsioonide erinev siseriiklik sisustamine ja kohaldamata jätmine raskendavad oluliselt rahvusvahelist koostööd. Samuti ei ole kehtiv õigusabipalvete süsteem tõendite kogumiseks digitaalkeskkonnas nende ajakriitilisuse tõttu.

Tabel 1. Rahvusvahelise koostöö elemendid (Arvutikuritegevuse vastane konventsiooni, 2004; Euroopa Liidu Nõukogu, 2015; Euroopa Liidu Teataja, 2000, 2004, 2005a, 2006, 2014, 2015 põhjal magistritöö autori koostatud)

RAHVUSVAHELINE KOOSTÖÖ DIGITAALKESKKONNAS

	Koostöö vorm		Eesti kontaktasutus	Võimaldab
Organisatsioonide kaudu	Europol		Eesti kontaktametnik Haagis; kontaktasutuseks Eestis on Keskkriminaalpolitsei	• Andmete ja teabe analüüs • Hõlbustab riikidevahelist teabevahetust • Võimalus osaleda uurimisrühmades
	Eurojust		Eesti riigi esindaja prokurör Haagis; kontaktasutuseks Eestis on Riigiprokuratuur	• Koordineerib, arendab ja parendab liikmesriikide vahelist koostööd • Õigusabitaotlustele vastamine • Rahastab JIT'e ja muid operatiivtööga seotud
Riikidevaheline koostöö	Kokkulepped	EL's	Justiitsministeerium kriminaalpoliitika osakonna rahvusvahelise justiitskoostöö talitus.	• Õigusabi (Kriminaalasjades vastastikuse abistamise Euroopa konventsioon) • Õigusabi otse riikidevaheliste lepingutega nt Soome, Läti, Leedu
		Kolmandate riikidega		• Õigusabi otse riikidevaheliste lepingutega nt Ukraina Vene Föderatsioon, USA
	Vastastikkuse tunnustamise põhimõte – tõendite kogumise otsuste vastastikune tunnustamine.		-	• Ühe EL liikmesriigi poolt tunnustatakse ja täidetakse ilma täiendavate eeltingimusteta teise EL liikmesriigi poolt tehtud otsuseid • Väljaspool EL'i toimib vastastikkuse, topeltkaristatavuse vältimise ja spetsiaalsuse põhimõte
Koostööinstrumendid	24/7 (Arvutikuritegevuse vastane konventsioon, 2001; Eesti 2004; rahvusvahelised lepingud)		SPOC (*Sirene Point of Contact*)	• Kiire hetkeolukorra fikseerimine • Operatiivne infovahetus • Koostöö ka väljaspool EL'i • Koostöö interneti teenuse pakkujatega
	Ühine uurimisrühm (EN raamotsus, 2002/465/JSK) Eesti, 2008		• Riigiprokuratuur • Eurojusti Eesti liige	• Operatiivne info edastus • Kiire koostöö
	Euroopa uurimismäärus (EPN direktiiv, 2014/41/EL)		Pole inkorporeeritud	• Seab tähtajad õigusabipalvetele vastamiseks • Edastamiseks võimalik kasutada kõiki kanaleid (Eurojust, õigusalase koostöö võrgustik vms. • Ühtne tõendite hankimise kord
	Teabe ja jälitusteabe vahetamise raamotsus (EN raamotsus, 2008; Eesti 2015)		PPA; (MTA ise oma pädevuse piires)	• Juba olemasoleva teabe ja jälitusteabe vahetamine • Omaalgatuslik teabe edastus

1.3. Jälitustoimingud digitaalkeskkonnas

Kuigi tänapäeval on võimalik iga kuriteo puhul leida olulist infot digitaalkeskkonnas, on küberkuritegevus selline kuriteo liik, mida pole võimalik menetleda digitaaltõendeid kogumata. Küberkuritegevust peetakse selliseks kuritegevuse vormiks, mis paneb proovile politsei võimekuse mitmel tasandil. (Leppänen, et al, 2016) Reaalmaailma rikkumised (sellised teod, mille lahendamiseks politsei organisatsioon algupäraselt loodi) on tavaliselt üks-ühele kuriteod, mis on seotud kindla asukohaga ja kurjategija on nähtav avalikkusele, mistõttu on risk saada tuvastatud. (Brenner, 2007) Paraku, enamik küberkuritegevuse jälgi on nähtavad ainult professionaalidele ja nii kurjategijad kui ka kannatanud võivad olla laiali üle maailma (Nhan & Huey, 2011).

Infotehnoloogia (edaspidi IT) ja kuritegevus on järjest tihedamalt omavahelises seoses (Lõhmus, 2016a) , mille tõttu peaks ka õiguskaitseorganitel olema sellealane profesionaalne väljaõppe. Paraku alles paar aastat tagasi ei olnud antud teemat politseinike õppekavadesse üldse lülitatud ja tänasel päeval on see osa väga pinnapealne (Sisekaitseakadeemia, 2013), mistõttu tulevased ametnikud ei saa koolist vajalikke erialaseid teadmisi. Kuna ttänapäeval liigub suurem osa infost interneti vahendusel, on see laiendanud kurjategijate võimalusi (Euroopa Liidu Teataja, 2007). Samuti on võimalik digitaalkeskkonnast leida kuritegude lahendamiseks ja ennetamiseks vajalikke tõendeid ja informatsiooni, milleks on oluline suurendada õiguskaitseorganite sellealast väljaõpet (Owsley, 2016). Eestis on politseiametnikele kasutamiseks loodud infotehnoloogia kuritegude menetlemise käsiraamat, mille eesmärk on hõlbustada IT abil toimepandud kuritegude kohtueelset menetlemist ja digitaalsete tõendite kogumist. IT kasutamine kurjategijate poolt ühest küljest hõlbustab kuritegude toimepanemist, teisalt aga jäävad enamasti maha jäljed. (Politsei - ja Piirivalveamet, 2011) Kuna internet ei tunne riigipiire (Euroopa Liidu Nõukogu, 2016), on vaja just eriti digitaalkeskkonnas tõendite leidmiseks teha rahvusvahelist koostööd teiste riikidega (Euroopa Komisjon, 2010).

Digitaalsete tõendite kogumise, käitlemise ja esitamise reeglid peavad toetama kriminaalmenetluse efektiivsust ja vältima nii menetlejate kui menetlussubjektide asjatut koormamist bürokraatiaga (Tehver, 2016). Digitaalsed tõendid saab jagada kaheks: tõendid andmekandjal (nt SIM-kaardid, mälupulgad, kõvakettad jne) ja tõendid arvutivõrkudes. (Politsei - ja Piirivalveamet, 2011) Käesoleva töö raames keskendub autor sellistele jälitustoimingutele, mille eesmärgiks on leida tõendeid arvutivõrkudes, eriti internetis toimuva tegevuse kohta. Näiteks on võimalik tuvastada võrguseadmetes või serverites salvestatud logide abil isikute tegevust arvutivõrkudes, mille

lõpptulemusena on võimalik jõuda juba kahtlustatava arvutini, millest seejärel on võimalik leida kuriteo lahendamiseks vajalikke tõendeid (Politsei - ja Piirivalveamet, 2011).

Üks põhi probleeme antud valdkonnas kriminaalõigusega on vajadus teada täpset kuriteo toimepanemise asukohta ja aega ning kurjategijate asukohta kuriteo toimepanemisel, mis digitaalkeskkonnas ei ole aga üldsegi mitte nii kindel just küberruumi leviku tõttu, mis raskendab õiguskaitseasutustel digitaaltõendeid koguda ja talletada (Velasco, et al, 2016). Samuti on digitaalkeskkonna eeliseks kuritegude toimepanemisel tehnoloogia võimalus ja vahendid varjata oma identiteeti (Osula, 2017). See muudab õiguskaitseorganitel väga keeruliseks tõendada kriminaalmenetluse käigus kuriteo tehiolud (Velasco, et al, 2016).

„Asukoha puudumine“ digitaalkeskkonnas andmete kogumisel on järjest suuremaks probleemiks jälitustoimingute läbiviimisel (Osula, 2017). Üha enam kasutatav andmesäilitus võimalus pilveteenus ja pilvandmetöötlus annavad õiguskaitseorganitele ühest küljest hea võimaluse tõendeid omandada, kuna kasutades erinevaid pilveteenuseid on kõik andmed ühes kohas koos. Samas „asukoha puudumine“ takistab oluliselt andmete kättesaadavust. (Euroopa Liidu Nõukogu, 2010) Pilves asuvaid andmeid liigutatakse pidevalt ühest serverist teise ja seda ka riigipiiride üleselt. Samuti võidakse pilves olevaid andmeid peegeldada turvalisuse ja kättesaadavuse huvides ja seetõttu võivad need olla mitmes erinevas asukohas korraga, seda nii ühe riigi piires kui ka erinevates riikides. Selle ja andmete puhverdamise tõttu ei pruugi ka pilveteenuse pakkuja teada, kus soovitud andmed täpselt asuvad. (Schwerha, 2010) See raskendab oluliselt pilvest informatsiooni kättesaamist.

Teisena raskendab õiguskaitseorganitel digitaalkeskkonnas jälitustoimingute läbiviimisel andmete kogumist isiku ja asukoha anonüümsust võimaldav võrguteenus TOR (Osula, 2017). TOR võrku ei kasuta sugugi mitte ainult kurjategijad, kes kasutavad TOR võrku mitte ainult omavaheliseks suhtluseks vaid ka kuritegude toimepanemiseks kasutades selleks võrgu anonüümsust pakkuvaid omadusi. TOR võrku kasutavad ka isikud, kes soovivad internetis rohkem oma privaatsust kaitsta, mis on nende põhiõigus. Samuti kasutavad TOR võrku erinevate riikide õiguskaitseorganid - TOR võrk loodigi Ameerika Ühendriikide mereväe poolt eesmärgiga kaitsta valitsuse tasandil suhtlust. (Minarik & Osula, 2016) Just eelpool nimetatud omadused muudavad TOR võrgu populaarseks anonümiseerimise vahendiks, kuid samas takistab see jälitustoimingute läbiviimist digitaalkeskkonnas.

Lisaks eeltoodud digitaalkeskkonna võimalustele, mis raskendavad jälitustoimingute läbiviimist, on veel digitaaltõendite üks omadus see, et nad on kergesti kaduvad. Nt on olemas digitaalseid tõendeid, mis võivad kaduda väga kiiresti – internetiliikluse salvestised, mis võidakse üle kirjutada päevade või isegi tundidega, see tähendab, et tõendite säilimise ja puutumatuse tagamiseks peab tegutsema viivitamatult (Politsei - ja Piirivalveamet, 2011) ning sellistes olukordades võib vastastikkuse õigusabi süsteem ja muud käesoleva töö peatükis 1.2. kirjeldatud meetmed, olla liiga aeglased ja vananenud (Osula, 2015, Euroopa Liidu Nõukogu, 2014). Selle probleemi lahendamiseks on loodud rahvusvaheline kiirkoostöövõrk 24/7 (Department of Justice, 2007). Kiirkoostöövõrgu aluseks on riikidevahelised õigusabilepingud, mis Eesti Vabariigis kuuluvad Justiitsministeeriumi kriminaalpoliitika osakonna rahvusvahelise justiitskoostöö talituse haldusalasse (Justiitsministeerium, 2016). Kuigi programmis osalejad on erinevad riigid üle maailma, on EL'i siseselt sama programm sisse kirjutatud ka Budapesti arvutikuritegevusevastase konventsiooni artiklisse 35 (Arvutikuritegevusevastane konventsioon, 2004).

Kiiremaks informatsiooni saamiseks annab võimaluse ka arvutikuritegevusevastase konventsiooni artikkel 32b (2004), mis võimaldab otse ühendust võtta teenuse pakkujaga, kellelt otse andmeid saada eeldamata riigi keskset rolli, eriti vajalik on selline võimalus, kui ei ole teada, millises riigis informatsioon asub. Näiteks saab tuua kui uurija kasutab kahtlustatava arvutis või telefonis olevat otseühendust või uurija kasutab seaduslikult saadud sisenemisparoole pilve teenusesse. (UNODC, 2013). Selline võimalus kiirendab küll oluliselt kriminaalmenetluseks vajaliku informatsiooni saamist, kuid seab küsimuse alla teise riigi suveräänsuse rikkumise (Osula, 2015). Samas Euroopa Komisjoni poolt 2016. aastal esitatud raport, mis käsitleb kriminaalõiguse parendamist küberruumis, tõi välja teenuse pakkujaga tõhusama koostöö loomise (Euroopa Komisjon, 2016).

Tõendite kogumiseks on vaja läbi viia erinevaid toiminguid sh ka jälitustoiminguid. Oluline on vahet teha luure, teabehanke ja jälitustoimingute vahel (Heldna, 2016). Käesolevas töös uuritakse ainult selliseid jälitustoiminguid, mida viiakse läbi digitaalkeskkonnas ja mida on võimalik läbi viia ka piiriüleselt.

Jälitus on praegu ja on olnud ka minevikus kaasaegse Euroopa ühiskonna julgeoleku tagamise osa (Lipartito, 2010). Tehnoloogia arengu ja selle kaasamisega jälitustoimingute läbiviimisesse ei ole tegemist sugugi ühepoolse suhtega vaid keerulise, kontekstist sõltuva sotsiaalse, poliitilise, ajaloolise ja tehnoloogilise dünaamikaga, mis mõjutab jälitustoimingute praktikat (Goos, et al, 2015). Vastavalt KrMS § 126^1 lg-le 1 on jälitustoiming isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest, ning

kõik jälitustoimingud on ammendavalt loetletud KrMS 3[1] peatükis (Kriminaalmenetluse seadustik, 2016). Tänapäeval on toimunud tehnoloogia ja informaatika vallas suured arengud (Euroopa Komisjon, 2014). Nende arengute tagajärjel on muutunud olulisel määral kuritegude kvaliteet ja toimepanemise viis, mille tõttu peab arenema ka õiguskaitseasutuste taktika ja vahendid kuritegude avastamisel (Lõhmus, 2016a).

Kriminaalmenetluse seadustik ei too välja eritingimusi digitaalkeskkonnas jälitustoimingute läbiviimiseks, kuid toob välja jälitustoimingu läbiviimise arvutisüsteemi sisenemise kaudu, kui see on vajalik jälitustoimingu eesmärgi saavutamiseks (Kriminaalmenetluse seadustik, 2016). Arvutisüsteemi kaudu teistesse mujal asuvates arvutisüsteemides läbiotsimist nimetatakse kaugläbiotsimiseks (Osula, 2017). Samas kui jälitustoiminguid teostatakse *online* tegevuse kohta, on tegemist pealtkuulamisega. Pealtkuulamine on üks klassikalisemaid jälitustoiminguid. Rahvusvaheliselt on surve sõnumite saladuse piiramiseks seotud eelkõige terrorismi ja piiriüleste kuritegude ohuga. Samas hõlbustab kommunikatsiooni pealtkuulamine või – vaatamine ka muude kuritegude uurimist, mistõttu jälitusasutuste huvi sellise jälgimismeetodi vastu on suur. (Lõhmus, 2014, lk 325) Võrgu pealtkuulamine on jälitustoiming, mida kasutatakse informatsiooni kogumiseks, näiteks on võimalik näha kasutajate omavahelist suhtlust, paroole, uurida, millega nad tegelevad ja mis intensiivsusega. (Laaneoks, 2010) Praegu ei ole Eesti õigusnormides täpselt eristatud, mille puhul on tegemist kaugläbiotsimisega ja millal tegemist võrgu pealtkuulamisega. Seetõttu tuleks kehtiv jälitustoimingu regulatsioon üle vaadata - läbiotsimist ja pealtkuulamist võimaldavate menetlustoimingute kasutamine tuleks selgemalt eristada (Osula, 2017).

Samuti ei näe kehtiv KrMS § 126^{10} ette kohustuslikke nõudeid jälitustoimingute dokumenteerimiseks selles osas, mis puudutab digitaalandmete kogumise protsessi ning andmete autentsuse ja terviklikkuse tagamise meetmete kirjeldamist (Tehver, 2016). See muudab võimatuks hinnata hiljem kogutud tõendite usaldusväärsust (Ginter, et.al, 2013). Selle lahendamiseks peaks olema digitaalse teabe kogumisel KrMS-is dokumenteerimise nõue (Tehver, 2016).

Digitaalkeskkonnas on võimalik teostada jälitustoiminguid interneti keskkonna infrastuktuuris ennast sinna nähtamatult sisse disainides. Sellisesse tegevusse on võimalik kaasata ka teisi (nt interneti teenuse pakkuja (edaspidi ISP) (Hallinan, 2015). Ühest küljest loob selline tegevus meeletu jälituse potentsiaali ja võimalused informatsiooni kogumiseks ja töötlemiseks. Teisest küljest on tegemist ilmselgelt liiga invasiivse inimõiguste rikkumisega. (Stranburg, 2007)

Piiriüleste jälitustoimingute puhul peab arvestama ka teise riigi õiguskorraga, mis võib Eesti riigi omast erineda. Näiteks pealtkuulamine ja varjatud jälgimine on Saksamaal ja Soomes detailsem kui Eestis ning mõlemad toimingud hargnevad n-ö omakorda erinevateks toiminguteks (telekommunikatsioonivahendite pealtkuulamine, asukoha kuulamine eravalduses (k.a kodus) ja asukoha kuulamine avalikus kohas), mis on sätestatud eriparagrahvides. Seega iga toiminguliigi puhul on detailiseeritud lisaks kahtlustatavale ka kolmandate isikute suhtes toimingute teostamise lubatavust ning teatud intensiivsete toimingute eriliikide puhul, mida Eestis eristatud pole, mittelubatavust. (Linask, 2014)

Viimast probleemi iseloomustab ka näide, mil USA konstitutsioon lubab teabevahetust pealt kuulata ilma kohtu loata, kui sõnumi vahetaja sellega nõustub. Saksamaal sõnumi saladuse põhiseaduslik kaitse säilib seni, kuni kõik suhtluse osalised pealtkuulamiseks nõusolekut ei anna. (Schwartz, 2002) Ka Eesti põhiseaduse §-i 43 (2015), mis kaitseb kõiki suhtlusosalisi, tuleb tõlgendada sarnaselt Saksa põhiseaduspraktikaga. (Lõhmus, 2008)

Jälistustoimingute, ka digitaalkeskkonnas ja piiiriüleste kuritegude puhul, on läbi aegade üheks suurimaks probleemiks olnud jälituse ja inimõiguste vaheline kollisioon (Reiner, 2006). Euroopa Liidu eduka toimimise üheks aluseks on Euroopa Liidu põhiõiguste harta, mille artikkel 7 ja 8 lähevad aga jälitustoimingu olemusega vastuollu. (Euroopa Liidu Teataja, 2010b)

Kuna jälitustoimingud on oluliselt inimõigusi riivavad tegevused (Kergandberg, 2000; Laos, 2008a; Rondel, 2016), siis tuleb nende läbiviimisel arvestada kolme olulise põhiõiguste dokumendiga: Eesti Vabariigi põhiseadusega (2015), Euroopa Inimõiguste ja põhivabaduste kaitse konventsiooniga (edaspidi EIÕK) (1996) ja Euroopa Liidu põhiõiguste hartaga (2010b). Selline olukord raskendab orienteerumist eri dokumentides ja mõjub mõneti häirivalt õigusselgusele. Ehkki riik loovutab üha enam pädevusi rahvusvahelistele organisatsioonidele, jääb põhiõiguste reaalne kaitse endiselt riigi asutuste, eriti kohtute ülesandeks. (Lõhmus, 2010)

Eesti Vabariigi põhiseaduse kohaselt Eesti Vabariik rajatud vabadusele, õigusele, õiglusele ning muuhulgas ka sisemise ja välise rahu tagamisele (Eesti Vabariigi põhiseadus, 2015). Peamine põhiseaduslik probleem riigi jaoks sisemise ja välise rahu tagamisel seisnebki tasakaalu leidmises isikute põhiõiguste ning julgeoleku eest vastutavate riigiasutuste tegevuse tõhususe vahel. (Laos, 2008b, lk 10-35). Avalik võim riivab privaatsust kõige laiemalt, sügavamalt ja tõsisemalt jälitustoimingute läbiviimisel ja teeb seda samal ajal vähemalt kahel rindel: esiteks mingit konkreetset privaatsusega hõlmatavat valdkonda riivates ja teiseks tegevuse salajasusega

põhiõiguste riive vaidlustamist raskendades (kui mitte öelda välistades) (Kergandberg, 2005). Jälitustoimingu salajasuse tõttu ei saa isik oma põhiõiguste riivest teada, mis välistab selle riive lubatavuse ja proportsionaalsuse vaidlustamise võimaluse ja seetõttu kujutab see endast põhiseadus § 15-s (2015) sätestatud põhiõiguse riivet. (Kergandberg & Sillaots, 2006)

Pärast USA, Ühendkuningriigi ja paari teise Euroopa Liidu liikmesriigi massilise interneti luure avalikuks tulekut varasem teooria, et parandades küberturvalisust on ka privaatsus kaitstud, enam ei toimiks (Argomaniz, 2015). Eeldati, et võimaldades küberturvalisuse eest vastutavatel ametkondadel suuremat ligipääsu isikuandmetele (nt IP aadress) hõlbustaks see väidetavalt nende tööd ennetades arvutisüsteemi vastaste kuritegude toimepanemist (Bowden, 2013). Oluline on tähele panna, et selline jälitus mõjutab otseselt EIÕK art 8, mis käsitleb igaühe õigust era- ja perekonnaelu puutumatust (Brown and Korff, 2009). 2013. aasta aprillis hoiatas Ühinenud Rahvaste Organisatsiooni (ÜRO) väljendusvabaduse eriraportöör (United Nations, 2011), et valitsused laiendades küberjälitust ja kogudes privaatseid isikuandmeid sekkuvad eneseväljendus ja privaatsus õigustesse, millega ohustavad demokraatliku ühiskonna põhitalasid. See on kindlasti üks teguritest, mis mõjutas EK'd võtma vastu kohtuotsuse muutmaks andmete säilitamise direktiivi. (Argomaniz, 2015)

Kuigi EL suurendab inimõiguste kaitset, ei tunne Eestis elavad inimesed, et nende põhiõigusi liigselt riivatakse (Inimõiguste Instituut, 2014). Eestis 959 inimese seas läbi viidud ja 2014. aasta lõpus avaldatud Inimõiguste Instituudi ja Tartu Ülikooli ühise uuringu „Privaatsusõigus inimõigusena ja igapäevatehnoloogiad" tulemused näitasid, et mure isikuandmete kaitstuse pärast on ületähtsustatud (41% küsitlusel osalenutest). 61% küsitletutest nõustus väitega, et riigil peab olema suurem õigus julgeoleku tagamise eesmärgil töödelda isikuandmeid. Üldiselt peeti üsna samaväärselt probleemiks seda, kui inimese nõusolekuta pääsevad andmetele ligi või koguvad andmeid riik, eraettevõtted või teised inimesed. (Inimõiguste Instituut, 2014)

Ühest küljest tundub antud uuringu tulemuste põhjal, et ei tajuta, et hästi informeeritud avalik võim võiks sattuda vaenulike jõudude kätte. Informatsiooni omamisega kaasneb võim, mille kuritarvitamine võib kujutada endas tõsist ohtu nii indiviidile kui ka Eesti riigile tervikuna. (Davies, 2014) Pruulmann-Vengerfeldt (2014) põhjendas uuringu tulemusi eestlaste ajalooga, kuna kõige leplikumad riigi poolse privaatsuse rikkumisega on vanem generatsioon, kes on üles kasvanud harjumusega, et naaber, sõber, töökaaslane ja isegi pere liige võib tema igast tegevusest KGB'le teada anda. Teine grupp, kes enim lepib privaatsuse rikkumisega on noored, kes on infoühiskonnas üles kasvanud ja on leppinud olukorraga, kus iga liigutus internetis jätab jälje ja kontrollivad ka

seda, mida nad postitavad ning seetõttu on noored need, kes tunnetavad, et neil pole midagi varjata. (Pruulmann-Vengerfeldt, 2014)

2016. aasta sügisel viidi taaskord läbi samalaadne küsitlus selgitamaks välja, mil määral on muutunud inimeste suhtumine jälitustoimingute eesmärgil inimõigustest loobumine, kuid tulemused ei olnud märkimisväärselt muutunud. (Turu-uuringute AS, 2016) Võib - olla selleks, et Eesti inimesed oma privaatsusest rohkem hoolima hakkaks, peaks toimuma Eestis Snowden'i sarnane skandaal. Nimelt avaldasid 2013. aasta juuni alguses mitmed erinevad meedia väljaanded – *New York Times, The Guardian* jne *US National Security Agency* (NSA) ja mõnede teiste luure agentuuride massilise rahva jälgimise. Salajased luuredokumendid avaldas meediale NSA allüksuse töötaja Edward Snowden. (Wright & Kreissl, 2015)

Käesoleva töö autor asub seisukohale, et inimesed ei taju, et nende privaatsusõigust liigselt riivatakse ja sellest tuleneb ka kergekäeline privaatsusesse sekkumisse suhtumine. Kuna riigi poolt on tagatud kontroll jälitusasutuste tegevuse üle (Rondel, 2016) ja on läbiviidud koolitusi ühtlasema praktika saamiseks (Ploom, 2016), võib järeldada, et Eesti tegeleb aktiivselt tasakaalu leidmisega inimeste põhiõiguste ja julgeoleku tagamise vahel.

Siiski on digitaalkeskkonnas jälitustoimingute läbiviimisel probleemiks rahvusvahelise koostöö aeganõudvus, mis raskendab tõendite õigeaegset kogumist. Eeltoodust lähtub, et digitaaltõendite omaduste tõttu, milleks on kiire hävinemine ja riigipiiride puudumine, on oluline nende kiire kogumine, kuid rahvusvahelise koostöö aeganõudvus seab ohtu võimaluse saada vajalikku informatsiooni enne selle hävinemist. Samuti on probleemiks „asukoha puudumine" võimaldavad tehnoloogiad, nagu pilvetehnoloogia ja TOR võrk. Järjest rohkem on vaja jälitustoiminguid läbi viia digitaalkeskkonda kasutades ja seetõttu on suurenenud ka rahvusvahelise koostöö vajadus. Kriminaalmenetluse seadustikus on aga jälitustoimingud reguleeritud digitaalkeskkonda väga üldiselt käsitledes „arvutivõrgu sisenemise kaudu". Selline piitilus on autori hinnangul liiga üldine. Lisaks on digitaalkeskkonna pideva arengu tõttu oluline ka menetlejate IT-teadlikkuse tõstmine.

2. PIIRIÜLESTE JÄLITUSTOIMINGUTE RAKENDUSPROBLEEMID DIGITAALKESKKONNAS

2.1. Metoodika ja valim

Käesolevas magistritöös on tegemist **kvalitatiivse uuringuga** Creswelli (2003, p. 18) käsitluses, mis põhinevad individuaalsetel kogemustel. Magistritöö **uurimisstrateegiana** kasutatakse võrdlevat juhtumiuuringut (*„case study"*) (Laherand, 2008; Flick, 2009, p. 134), milleks kasutatakse Flick`i (2009, p. 259) poolt välja toodud lähenemist, vaadeldes töö eesmärgi saavutamiseks teaduslikke ja õiguslikke dokumente ning hinnates neid digitaalkeskkonnas jälitusalase rahvusvahelise koostöö kontekstis. Seejuures peab arvestama, et dokumendid võivad olla osaliselt kättesaamatud või piiratud ligipääsuga (Flick, 2009, p. 259; Flick, 2011, p. 123). Juhtumiuuringu eesmärgiks on konkreetsete juhtumite kirjeldamine ja põhjuslike seoste väljaselgitamine (Flick, 2009, p. 134), mille tulemusel on võimalik hinnata valitud teemat põhjalikult (Yin, 2009, p. 4) ja pakkuda rakenduslikke lahendusi. Käesoleva magistritöö raames uuritud juhtumite, so kohtute otsused on kättesaadavad, kuid jälitusalane dokumentatsioon on olulises osas piiratud ligipääsuga, eriti selles osas, mis puudutab konkreetseid menetlusi rahvusvahelise koostöö rakendamisel.

Uurimisinstrumentide kasutamisel on autor lähtunud töö esimeses osas välja toodud probleemidest, milleks on EL regulatsioonide erinev siseriiklik sisustamine, digitaalsete tõendite ajakriitilisus, õigusabipalve süsteemi mitte sobivus digitaaltõendite kogumiseks ja „asukoha puudumine". Eeltoodust tulenevalt valiti dokumendianalüüsi jaoks nii EIK, EK kui ka Eesti Vabariigi kohtute lahendid, mis toovad autori hinnangul digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohad esile. Samuti koostati ja esitati ekspertintervjuude küsimused selliselt, mis võimaldasid intervjueeritavatel anda hinnang digitaalkeskkonnas piiriüleste jälitustoimingute probleemide põhjuste kohta ning tuua omapoolseid ettepanekuid probleemide lahendamiseks.

Juhtumiuuringu täiendamiseks ja edasiarenduseks (Simons, 2009, p. 64) viis autor läbi **poolstruktureeritud ekspertintervjuud**. Intervjueeritavate leidmiseks kasutas autor eesmärgistatud valimit, millega lähtutakse uuritavate valikul uurimisülesannetest ja eraldatakse kindlaksmääratud mahuga populatsioonist liikmeid eesmärgipäraselt selliselt, et tegemist oleks ekspertidega, kes oskavad analüüsitavast teemast parimal võimalikul viisil rääkida. (Teddlie & Yu,

2007, p 77) Ekspertintervjuu küsimustiku koostamise aluseks on magistritööst tulenevad teoreetilised põhiseisukohad ja dokumendianalüüsi tulemused digitaalkeskkonnas piiriüleste jälitustoimingute rakendusprobleemide kohta.

Eelnimetatust lähtudes tugines autor valimi koostamisel teadmisele, et EV's käib rahvusvaheline koostöö reeglina läbi keskkriminaalpolitsei. **Valimisse** kuulusid Politsei- ja Piirivalveameti uurijad (jälitusametnikud), ja Maksu- ja Tolliameti uurija, Riigiprokuratuuri abiprokurör ja pangaliidu rahapesu tõkestamise toimkonna juht, kes oma töökohustustest tulenevalt puutuvad või on puutunud kokku tõendite kogumisega digitaalkeskkonnast ja rahvusvahelise koostööga.

Lähtudes sisendist, et intervjueeritavate igapäevatöö ülesanded peavad seonduma jälitusalase rahvusvahelise koostööga digitaalkeskkonnas, kuulus valimisse 9 isikut. Intervjueeritavad olid valitud võimalikult erineva taustaga, et saaks hinnata esile tulevaid probleeme võimalikult objektiivselt. Seejuures on uuringu teemat valdavate ekspertide arv Eestis oluliselt piiratud, kuna on vähe neid, kes kõigi kolme aspektiga – digitaalkeskkond, jälitustoimingud ja rahvusvaheline koostöö – kokku puutuks, mistõttu saavutas autor valimi koostamisel optimaalseima võimaliku tulemuse. Autori hinnangul oli eesmärgistatud valim sobilik uuringu eesmärgi saavutamiseks, kuna see võimaldas parimal viisil saada vastused püstitatud uurimisküsimustele.

Kuna uuring viidi läbi Politsei- ja Piirivalveametis töötavate jälitusametnikega, pöördus autor 28.11.2016 uuringu läbiviimise nõusoleku saamiseks Politsei- ja Piirivalveameti poole. 12.12.2016 andis Politsei- ja Piirivalveamet uuringu korraldamiseks nõusoleku reg.nr 1.1-14/322-2.

Intervjuude uurimisküsimuste (vt lisa 1) koostamise aluseks olid magistritööst tulenevad teoreetilised põhiseisukohad ja juhtumiuuringus kohtulahendite analüüsi tulemused piiriülese digitaalkeskkonnas läbiviidatavate jälitustoimingute rakendusprobleemide kohta. Tulemuste parimaks saavutamiseks viidi ekspertintervjuud läbi poolstruktureeritult (Flick, 2009, p. 156; Simons, 2009, p. 43), mis annab rohkem informatsiooni kui näiteks standardiseeritud intervjuud (Flick 2009, p. 150), samas võimaldab see uurijal vestlust piirata läbimõeldud küsimustikuga (Mahoney, 1997).

Intervjuud viidi läbi ajavahemikul 15.02.2017-23.02.2017. Intervjuude keskmiseks pikkuseks oli 54:59 minutit. Kõikide intervjueeritavatega võeti ühendust kas e-maili või telefoni teel, milles tutvustati uuringu eesmärki ja intervjuu iseloomu. 7 intervjuud 9-st viidi läbi intervjueeritavate tööruumides ning lindistati helikandjale. Üks viidi läbi intervjueeritava kodus ja üks Sisekaitseakadeemias. Kõikidele intervjueeritavatele selgitati enne intervjuuga alustamist võimalust

tagada nende anonüümsus. Kuna mõned intervjueeritavad on ka varasemalt avalikkuse ees sõna võtnud, siis nemad ei pidanud anonüümsust oluliseks. Samas on intervjueeritavate seas neli jälitusametnikku, kelle tööülesannetest lähtuvalt on oluline tagada nende anonüümsus. Samuti avaldas kaks intervjueeritavat soovi, et nende ametikohad ei oleks detailselt avaldatud, vaid ameti täpsusega. Uuringu ja järelduste teadusliku usaldusväärsuse tagamiseks peab magistritöö olema võimalikult läbipaistev ja metodoloogiliselt selge (Koch, Niesz & McCarthy, 2014), selle tõttu tõi autor välja (tabel 1) võimalikult täpsed andmed intervjueeritavate ja intervjuude läbiviimise kohta. Intervjuud andnud ekspertide eristamiseks kasutab autor tähelis-numbrilist kombinatsiooni, mis on tuletatud intervjuu läbiviimise järjekorrast – I1 (intervjuu 1), I2 (intervjuu 2), I3 (intervjuu 3) jne.

Tabel 2. Uuringu intervjuude toimumise kronoloogia (magistritöö autori koostatud uurijapäeviku alusel)

Intervjueeritava (nimi) ja kood	**Positsioon**	**Töötamise valdkond**	**Intervjuu läbiviimise viis ja koht**	**Intervjuu toimumise aeg**	**Intervjuu kestvus**
Reemo Salupõld (I1)	Spetsialist	Politsei- ja Piirivalveamet	Suuline, Tallinn, SKA	15.02.2017	48:48
Hannes Kelt (I2)	Juht	Politsei- ja Piirivalveamet, Põhja Prefektuur, Kriminaalbüroo	Suuline, Tallinn, Põhja Prefektuur	15.02.2017	39:04
Aivar Paul (I3)	Juht	Pangaliidu rahapesu tõkestamise toimkonna juht	Suuline, Tallinn, LHV Pank	16.02.2017	1:07:00
Robert Laid (I4)	Juht	Riigiprokuratuur, süüdistusosakond, abiprokurör	Suuline, Tallinn, Riigiprokuratuur	16.02.2017	41:08
Anonüümne 1 (I5)	Spetsialist	Politsei- ja Piirivalveamet, Põhja Prefektuur, Kriminaalbüroo	Suuline, Tallinn, Intervjueeritava kodus	16.02.2017	1:47:23
Maria-Elisabeth Kool (I6)	Juht	Politsei- ja Piirivalveamet, teabehaldus- ja menetlusosakond	Suuline, Tallinn, keskkriminaalpolitsei	21.02.2017	1:00:23
Anonüümne 2 (I7)	Spetsialist	Maksu- ja Tolliamet	Suuline, Tallinn, MTA	21.02.2017	57:00
Anonüümne 3 (I8)	Spetsialist	Politsei- ja Piirivalveamet, Põhja Prefektuur, Kriminaalbüroo	Suuline, Tallinn, Põhja Prefektuur	21.03.3017	44:02
Anonüümne 4 (I9)	Spetsialist	Politsei- ja Piirivalveamet, Põhja Prefektuur, Kriminaalbüroo	Suuline, Tallinn, Põhja Prefektuur	23.03.2017	30:00

Uuringu käigus kogutud andmed transkribeeriti ja dokumenteeriti ning seejärel teostati kvalitatiivse andmeanalüüsi programmi Nvivo11 vahendusel transkriptsioonide kvalitatiivne sisuanalüüs (Flick,

2009, pp. 323-325). Sisuanalüüsi läbiviimiseks rakendati intervjuude avatud kodeerimist (Flick, 2009, p. 309). Selleks loodi uurimisküsimuste alusel kategooriad ja kategooriate alla koondati neid iseloomustavad koodid. Kodeerimise järgselt kasutati analüüsimiseks Nvivo11 võimalusi, et välja selgitada ekspertide arvamuste sarnasused, erinevused ja muu oluline. Pärast märksõnade grupeerimist ja esialgset kodeerimist ning uurimisküsimuste võrdlust moodustus kõikidest märksõnadest 12 koodi kolme kategooria alla. Intervjuudest moodustunud koodipuu on toodud käesoleva uurimistöö lisas (lisa 2).

Seejärel teostati tekstide kvalitatiivne sisuanalüüs (Bazealy & Jackson, 2013), mille käigus käsitleti intervjuudest välja võetud tekste koodide lõikes ning võrreldi ja analüüsiti andmeanalüüsi programmiga NVivo11 intervjueeritavate seisukohti. Väljatoodud erinevuste ja sarnasuste kontrollimiseks koodi lõikes tehti NVivo11 programmiga eraldi päringuid.

Uuringu kolmandas etapis esitati analüüsi tulemused kategooriate kaupa. Koodid on välja toodud intervjueeritavate seisukohtade olulisuse järjekorras, enim väljatoodud hinnangud eespool. Läbiviidud intervjuud võimaldasid kinnitada eelneva dokumendianalüüsi tulemusi digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise rakendusprobleemide kohta ning pakkusid täiendava käsitlusvõimaluse. Kuna viidi läbi kvalitatiivne uurimus, siis said vastajad avatumalt oma arvamust avaldada ja vajadusel põhjendada ning näidetega illustreerida. Seetõttu on autor seisukohal, et antud lähenemisviis võimaldas parimal võimalikul viisil lahendada töös püstitatud probleemi ja jõuda eesmärgini, milleks on välja selgitada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohad ja esitada uurimispõhiselt rakendusettepanekuid nende lahendamiseks. Dokumendianalüüsi ja ekspertintervjuude tulemusi on analüüsitud järgnevas alapeatükis.

2.2. Jälitustoimingute rakendusprobleemid digitaalkeskkonnas

Käesoleva töö esimeses peatükis selgitas autor digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise õiguslikku raamistikku ja analüüsis digitaalkeskkonnas läbiviidavate jälitustoimingute iseärasusi. Sünteesi käigus saadi vastus esimesele uurimisküsimusele, so EL'i õiguse ebapiisav ülevõtmine, riigisisese õiguse kohaldamata jätmine vastavalt uutele reeglitele, õigusabipalve süsteemi mitte sobimine digitaaltõendite ajakriitilisuse tõttu ning „asukoha puudumine". Magistritöö teooria osas ilmnenud õiguslike probleemide paremaks mõistmiseks analüüsib töö autor

EIK, EK ja Eesti Vabariigi kohtu otsuseid. Dokumendianalüüsi tulemuste täiendamiseks ja edasiarenduseks on autor analüüsinud ja võrdluseks toonud ekspertide seisukohad selliste rakendusprobleemide kohta.

Euroopa Inimõiguste Kohtu, Euroopa Liidu Kohtu ja Eesti Vabariigi kohtu otsuste analüüs

Dokumendianalüüsi kasutab autor täiendava vahendina intervjuudele, tuvastamaks ühisosa kohtute seisukohtadest nähtuvate probleemide ning digitaalkeskkonnas piiriüleseid jälitustoiminguid läbiviivate isikute hinnangute vahel. Dokumentide otsimiseks kasutas autor Euroopa Inimõiguste Kohtu ja ametlike võrguväljaannete Euroopa Liidu Teataja, Riigi Teataja andmebaase ning otsingumootorit Google.

Üheks keerulisimaks probleemiks jälitustoimingute puhul on kolmandate isikute õigused (käesolev töö, lk 12), kui jälitusluba on antud telefoninumbrile, mida kasutab suurem isikute ring. Riigikohus aktsepteeris sellisel juhul loa andmist, kus kahtlustatav kasutas telefoninumbrit ainult ühel korral ja ülejäänud aja kasutasid seda teised isikud (Andres Sarapuu ja Jüri Oidekivi kriminaalasi KarS § 184 lg 2 p 1, 2 ning Ervin Kurmi kriminaalasi KarS § 184, lg 1 järgi, 2011). Selline lai ja selgelt piiritlemata luba võib anda võimaluse salajase pealtkuulamise kuritarvitamiseks ja nn „õngitsemiseks“. Kruusamäe ja Timo (2013) leidsid, et peab vältima olukordi, kus kolmandate isikute kõned muutuvad iseseisvalt jälitustoimingule allutatuks, et vältida olukorda, kus salajase pealtkuulamise aluseks olevat kohtu luba pole võimalik kriminaaltoimikusse võtta põhjusel, et sellega sanktsioneeriti jälitustoimingu tegemine üheaegselt mitme isiku suhtes, kellest osa pole konkreetse kriminaalmenetlusse kaasatud, tuleks koostada nõuetekohane luba iga salajase pealtkuulamisele allutatud isiku kohta eraldi. (Andrei Pavlištšuki kriminaalasi KarS § 164 järgi, 2012)

Selline seisukoht ühtib pigem liberaalse teooriaga, mis peab oluliseks inimõiguste kaitset. Samas on magistritöö autor seisukohal, et kuigi antud kaasuste puhul on tegemist telefoniside pealtkuulamisega, kehtivad samad põhimõtted ka võrgu pealtkuulamisele (käesolev töö, lk 13).

Märkimisväärne on ka hiljutisest Riigikohtu otsusest tulenev seisukoht, et email on PS § 43 mõttes kommunikatsiooniprotsessis selle ärasaatmisest kuni saajani jõudmiseni ehk sõnumi teeloleku ajal, mil sõnum on isiku mõjusfäärist väljas ning ta ei saa seda kolmandate isikute eest kaitsta (Ivor Onksioni kriminaalasi KarS § 137 lg 1 ja § 156 lg 1 järgi, Priit Toobali kriminaalasi KarS § 137 lg 1 – § 22 lg 2, § 156 lg 1 – § 22 lg 2, § 344 lg 1 järgi ja Lauri Laasi kriminaalasi KarS § 137 lg 1 –

§ 22 lg 2, § 156 lg 1 – § 22 lg 2 järgi 2015). Riigikohtu hinnangul oleks juba isiku mõjusfääri jõudnud e-kirjale ligipääsemiseks nõutav kohtu luba arvutisse sisenemiseks (Kriminaalmenetluse seadustik, 2016) liiga range (Lõhmus, 2016b). Seetõttu võib salvestatud andmetele ligipääsu kvalifitseerida, kui jälitustoimingute kasutamine on õigustatud, KrMS § 126^5 alusel. Seega on vajalik „asja", mis antud kaasuse puhul oli Google server, läbivaatamiseks prokuröri luba (Ivor Onksioni kriminaalasi KarS § 137 lg 1 ja § 156 lg 1 järgi, Priit Toobali kriminaalasi KarS § 137 lg 1 – § 22 lg 2, § 156 lg 1 – § 22 lg 2, § 344 lg 1 järgi ja Lauri Laasi kriminaalasi KarS § 137 lg 1 – § 22 lg 2, § 156 lg 1 – § 22 lg 2 järgi 2015). See tähendab, et kui isik on e-maili kätte saanud, loetakse kommunikatsiooniprotsess lõppenuks ja õiguskaitseametnik vajab sellele ligipääsuks prokuröri, mitte kohtuniku luba (käesolev töö, lk 25). Täpsustamata on, kas prokuröri loast piisab, kui läbivaadatavad andmed asuvad teise riigi territooriumil.

Eeltoodud Riigikohtu seisukoht ei ühti EIK omaga, kuna viimane loeb nii sõnumite sisu kui ka edastamise protsessi iseloomustavad andmed sõnumite saladuse kaitsealasse, ehk andmed helistaja ja vastuvõtja numbri, kõne aja ja kestvuse kohta on telekommunikatsiooni osa (Malone *vs.* Ühendkuningriik, EIKo, 1984; Copland *vs.* Ühendkuningriik, EIKo, 2007). Samuti on EIK praktika järgi korrespondentsi mõistega kaetud lisaks edastamise protsessis olevatele sõnumitele ka saatmiseks ette valmistatud ja kohale jõudnud sõnumid (Wieser ja Bicos Beteiligungen GmGH *vs*. Austria, EIKo, 2007). Ilmselt tuleneb siin erinev lähenemine asjaolust, et PS § 43 (2015) räägib sõnumist, mida edastatakse üldkasutataval teel ehk rõhk on edastavatel sõnumitel, mitte mis tahes sõnumitel. Selles osas sarnaneb Eesti sõnumite saladuse kaitseala pigem USA omaga, mistõttu ei ole kindel, et EIK sellist tõlgendust tunnustab kui ta peaks analüüsima Eesti seaduste vastavust EIÕK'le (Lõhmus, 2014, lk 331-333). Selline Eesti Riigikohtu ja EIK seisukohtade erinevus on näide sellest, kuidas siseriiklik õigus võib olla vastuolus EL'i omaga. Selleks, et rahvusvaheline koostöö toimiks, peab toimima ühtne menetluspraktika ja püüdlemine samade eesmärkide poole (käesolev töö, lk 20).

Euroopa Kohus on viimaste aastatega vastu võtnud paar digitaalkeskkonna jälitust mõjutavat kohtuotsust. Kõige olulisemaks võib pidada Seitlinger ja Digital Rights Ireland kaasust (EKo, 2014), milles kohus kuulutas andmete säilitamise direktiivi 2006/24/EÜ tagasiulatuvalt õigustühiseks. Oma otsuses tugines kohus argumentidele, et direktiivis ei ole defineeritud raske kuritegevuse mõistet, muutes nii avaliku huvi kaitse ja põhiõiguse rikkumise proportsionaalsuse hindamise võimatuks. Direktiivis ei olnud kehtestatud ka kindlat korda, mille järgi andmete üleandmine luureasutustele peaks toimuma ning ei eristatud andmesubjekte, kelle suhtes esineb

mõistlik kahtlus, nendest, kellel puudub igasugune side kuritegevusega. Samuti ei nähtud direktiivis andmesubjektidele ette piisavaid tagatisi ja õiguskaitsevahendeid andmete kuritarvitamise puhuks ja lisaks ei olnud ettenähtud andmete säilitamise periood põhjendatud. (Digital Rights Ireland ja Seitlinger jt. EKo, 2014)

Eestis toimub andmete säilitamine elektroonilise side seaduse (2004) (edaspidi ESS) alusel, mille järgi on nii telefoni- ja mobiiltelefoniteenuse ning telefonivõrgu ja mobiiltelefonivõrgu teenuse osutaja kui ka Interneti-ühenduse, elektronposti ja interneti-telefoni teenuse osutaja kohustatud säilitama andmeid üks aasta alates side toimumise ajast. Mõnedes riikides nagu Austrias, Sloveenias, Slovakkias, Poolas, Rumeenias, Ühendkuningriigis, Bulgaarias, Belgias ning Hollandis tunnistasid kõrgeima astme kohtud andmete säilitamise põhiseadusvastaseks (FRA, 2015). Selline erinev riikidesisene praktika, mil igal riigil on erinevad tähtajad andmete säilitamiseks, kui see üldse toimub, raskendab autori hinnangul oluliselt rahvusvahelist koostööd piiriüleste jälitustoimingute läbiviimisel (käesolev töö, lk 20).

Andmete säilitamise direktiivi kehtetust on kasutatud argumendina Eesti Vabariigi kohtus (nr 3-1-1-51-14). Antud asjas väitis kaitsja, et elektroonilise side metaandmete säilitamise tulemusena saadud informatsioon ei kuulu kriminaalmenetluses lubatavate tõendite hulka. Riigikohtu kriminaalkolleegium aga rõhutas samuti, et andmete säilitamine kui selline, ei ole ebaproportsionaalne riive ning direktiivi kehtetus ei too vältimatult kaasa riigisisese regulatsiooni kehtetust, kuna direktiivi eesmärke silmas pidades on liikmesriigi seadusandjal riigisisese regulatsiooni kujundamisel teatud ulatuses kaalutlusõigus. Seega ei toonud EK otsus kaasa kogutud tõendite kehtetust. (Ruve Veski, Jaanus Lauri, Tõnu Schasmini ja Roland Feodorovi kriminaalasi KarS § 212 lg 1 järgi, 2015)

Pärast *Digital Rights Ireland*'i kaasust, kui sideandmete säilitamise direktiiv kehtetuks muudeti, otsustasid mõned riigid suurendada siseriiklikult andmete säilitamist. Selle kohta tegi EK 2016. aasta detsembris otsuse liidetud kohtuasjas C-203/15 ja C-698/15 (Tele2 Sverige AB ja Secretary of State for the Home Department jt. EKo, 2016), milles käsitleti EL'i liikmesriikide siseriiklikku õiguskorda, mis nägi ette abonentide ja registreeritud kasutajate liiklusandmete säilitamise kohustuse. Euroopa Kohus viitas oma otsuses, et selline kord läheb vastuollu Euroopa Liidu põhiõiguste harta (Euroopa Liidu Teataja, 2010b) artiklitega 7, 8 ja 11, kuna see näeb ette kuritegevuse vastu võitlemise eesmärgil kõiki elektroonilise side vahendeid puudutava kohustuse säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik

liiklusandmed ja asukohaandmed. (Tele2 Sverige AB ja Secretary of State for the Home Department jt. EKo, 2016) Praegu kohustab Eesti seadus sideettevõtteid säilitama suurt hulka andmeid. Näiteks peavad mobiilifirmad aastaks ajaks säilitama helistaja ning vastuvõtja numbri koos nime ja aadressiga, andmed kõne alguse ja lõpu aja kohta, kõne geograafilised andmed ning teabe ka kasutatud telefoni kui seadme kohta. (Elektroonilise side seadus, 2004)

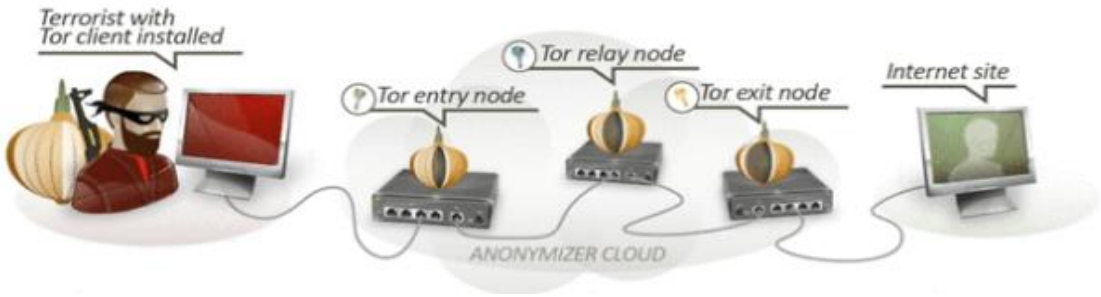
2016. aasta aprillis võtsid Euroopa Parlament ja Nõukogu vastu isikuandmete kaitse üldmääruse, mis hakkab kehtima 25.05.2018, kui saab läbi kahe aastane üleminekuperiood, kuna tegemist on regulatsiooniga, ei ole vaja liikmesriikide valitsustel see eraldi vastu võtta. Määruse eesmärk on suurendada ja ühtlustada isikuandmete kaitset Euroopa Liidu piires. Kuigi määruses ei ole määratud andmete säilitamise tähtaegu, on selge, et eelnevalt analüüsitud kohtuotsuste valguses hakatakse Eestis hetkel kehtivaid õigusnorme muutma. (Euroopa Liidu Teataja, 2016)

EK lahendite ja uute määruste analüüsimisel on keskne koht inimõiguste maksimaalsel kaitsel, mis viitab liberalistlikule lähenemisele. (käesolev töö, lk 13).

Digitaalkeskkonnas toimepandud kuritegude puhul sai eelmisel aastal palju meediakajastust Mart Pirita kaasus. M. Piritat süüdistati, et ta sisestas ilma seadusliku aluse ja volituseta Siseministeeriumi haldusala töötajate kaugligipääsu portaalides mõnede kasutajate kasutajatunnused ning ebaõiged paroolid, mille tulemusel nende kasutajakontod blokeerusid. Sellega oli Siseministeeriumi haldusala töötajate kaugligipääsu arvutisüsteemi toimimine häiritud. Oluline antud kaasuse puhul on asjaolu, et teo toimepanemiseks kasutati Tor anonümiseerimisvõrku ja Debian operatsioonisüsteemi ja selle võrgu anonüümsuse omaduse tõttu mõisteti M. Pirita ka õigeks. (Mart Pirita kriminaalasi KarS § 207 lg 1 järgi, 2016)

Tor võrk võimaldab anonüümsust oma töö põhimõtte poolest. Kohtuotsuses on lahti seletatud, et Tor on netikasutuse jälgede peitmise võrk, kus Tori kliendi andmeside toimub läbi projektiga ühinenute poolt selleks üles seatud serverite (vt joonis 1). Tori kliendi saadetud andmepakett liigub mööda suvaliselt valitud Tori võrgu serverite ahelat, millest viimane (ExitNode) teeb pöördumise lõplikku sihtkohta. Andmeside Tor võrgus on krüpteeritud ning selle ahela lülid, mida päring läbib, ei „näe“ tervet ahelat. Seetõttu ei ole Tor võrgu kaudu tehtud päringu puhul võimalik tuvastada päringu teekonda ja selle päringu teinud Tori kasutaja IP-aadressi. Eelnev ei tähenda, et kindlaks ei ole võimalik teha seda, et mingilt IP-aadressilt on kasutatud Tor võrku. Konkreetse IP-aadressi võrguliiklust jälgides on võimalik näha, et see suhtleb mõne Tor võrku kuuluva IP-aadressiga, kuid ei ole teada, kuhu päring Tor võrgus edasi liigub. (Mart Pirita kriminaalasi KarS § 207 lg 1 järgi,

2016) See tähendab, et kui teha kindlaks, et isik kasutas Tor võrku, ei saa kindlaks teha, mida ta selle vahendusel tegi, kuna samad logid on kõikidel samal ajal Tor-võrgu kasutajatel.



Joonis 1. Tor – võrgu toimimise põhimõte (Estonian Cyber Security News Aggregator, 2016)

Nagu ka käesoleva töö teoorias (käesolev töö, lk 22) välja toodi, on viimane kaasus väga hea näide, kuidas digitaalkeskkond paneb õiguskaitse võimekuse proovile mitmel tasandil. Lisaks klassikalistele menetlustaktikatele ja meetoditele peab tänapäeva menetleja oskama tõendeid otsida ka digitaalkeskkonnast.

Dokumendianalüüsi tulemusena võib järeldada, et isikuandmete kaitse on EL'is suure tähelepanu all ja sellega seoses tehakse muudatusi, mis seavad rangemad nõuded jälitustoimingute läbiviimisele. Samuti on digitaalkeskkonna võimekuse kasvamisega laienenud võimalused kasutada digitaalkeskkonda kuritegude toimepanemisel, mistõttu on oluline, et ka menetlejate pädevus laieneks.

Ekspertintervjuude võrdlev analüüs

Magistritöös püstitatud uurimisküsimustele vastamiseks viidi läbi pooltstruktureeritud ekspertintervjuud. Intervjuude eesmärgiks oli koondada digitaalkeskkonnas läbiviidavate piiriüleste jälitustoimingutega tegelevate ametnike ja abiprokuröri seisukohad, võrrelda kogutud arvamusi ja analüüsida neid rahvusvahelise koostöö teooriast lähtudes, ning saada sisendeid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise parendamise ettepanekute tegemiseks.

Esimene kategooria **„Õiguslikud probleemid"** koosneb koodidest, millega vastati uurimisküsimusele nr 1: milliseid õiguslikke probleeme esineb piiriülestel jälitustoimingutel digitaalkeskkonnas? Teise uurimisküsimuse: milliseid takistusi esineb praktikas digitaalkeskkonnas jälitustoimingute läbiviimisel? Koodid koondati teise kategooriasse **„Praktilised nõrgad kohad"**. Kolmandasse kategooriasse **„Parendus - ettepanekud"** koondati koodid, mis vastasid kolmandale

uurimisküsimusele: kuidas lahendada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevaid probleemkohti?

Tabel 3. Uurimusküsimuste seos kategooriate ja koodidega (magistritöö autori koostatud magistritöö analüüsi põhjal NVivo11 programmiga)

1) Milliseid õiguslikke probleeme esineb piiriülestel jälitustoimingutel digitaalkeskkonnas?	2) Milliseid takistusi esineb praktikas digitaalkeskkonnas jälitustoimingute läbiviimisel?	3) Kuidas lahendada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevaid probleemkohti?
I kategooria **Õiguslikud probleemid**	**II kategooria** **Praktilised nõrgad kohad**	**III kategooria** **Parendusettepanekud**
Koodid Erinevate riikide õiguskord Õigusabipalved Kiirkoostöövõrk JIT Inimõiguste riive	Koodid Digitaalkeskkonna võimekus Pädevus Tutvused Sideohvitser Teise riigi motivatsioon	Koodid Õiguslikud parandusettepanekud Praktilised parandusettepanekud

Õiguslike probleemide kategooria alla kodeeriti digitaalkeskkonnas läbiviidavate jälitustoimingute õiguslikud probleemid – erinevate riikide erinev õiguskord, inimõiguste riive, JIT ning õigusabipalved. Õigusabipalvete alla tekkis eraldi kood kiirkoostöö võrgu jaoks. (vt tabel 3)

Esimese kategooria all avaldasid intervjueeritavad kõige enam arvamust **erinevate riikide õiguskorra** suhtes ning nenditi, et erinevate riikide erinev õiguskord tekitab probleeme. Riikide erineva õiguskorra juures võib probleeme tekitada nii siseriiklik erinev õiguskord (käesolev töö, lk 20) kui ka EL'i raamotsuste ning kohtu otsuste erinev tõlgendamine (käesolev töö, lk 20; 35). Siseriikliku õiguse sisustamise probleemid on seotud nii menetluspraktika kui ka teo kvalifitseerimisega. Näiteks toodi välja juhtumeid, kui sooviti õigusabi teiselt riigilt, kuid selles riigis polnud Eestis uuritav tegu üldsegi kuritegu. Või teises riigis ei ole võimalik toiminguid läbi viia sellisel määral või sellises mahus, nagu meil Eestis tehakse (käesolev töö, lk 34). Riikide erineva õiguskorra üheks mõjutajaks märgiti intervjuude käigus kultuuri. EL on koostöö tagamiseks loonud erinevaid meetmeid, et ühtlustada piiriüleste toimingute, sh jälitustoimingute läbiviimist (käesolev töö, lk 17).

Osa intervjueeritavatest tõi välja, et kuigi EL ühelt poolt üritab arendada kriminaalasjades rahvusvahelist koostööd, siis teiselt poolt võtab EK vastu otsuseid, mis pigem raskendavad kriminaalmenetlustes tõendite kogumist. Mitmed intervjueeritavad tõid välja andmete säilitamise kaasuse EK's, mida analüüsiti ka dokumendianalüüsi osas. Kohtuotsusega tühistati varasem direktiiv ja seati olulised piirangud andmete säilitamise tähtaegadele (käesolev töö, lk 34-36). Riigid

sisustasid seda siseriiklikult erinevalt, kui Eestis on näiteks võimalik sideettevõttel aasta vältel andmeid säilitada (käesolev töö, lk 35), siis mõnes teises riigis võib see ainult kuu olla. See seab olulised piirid teiste riikidega suhtlemisele ja koostööle.

Lisaks üldisele hinnangule saab välja tuua konkreetseid probleeme intervjueeritavate poolt esitatud kaasuste alusel: näiteks riikide erinevus kahju ulatuse käsitlemisel. Seda eriti kelmuste või narko kuritegude menetlemisel. Kõik kahju summat käsitlenud intervjueeritavad tõid välja, et on oluline vahe, millise riigiga koostööd teha. Sõltuvalt sellest, milline nende hinnangul kahju väärtus on. Antud probleemi osas tõid intervjueeritavad sarnaseid näiteid, kus Eestis võib olla kelmusega tekitatud kahju 5000€ suure kahju summa tõttu oluline asi, kuid suurriigi puhul nagu Saksamaa ei ole alla 10000 või 20000€ menetlus prioriteetne ja see mõjutab rahvusvahelise koostöö kvaliteeti. Tekib vastuolu rahvusvahelise koostöö ühe olulisima printsiibiga – vastastikkuse tunnustamise printsiibiga (käesolev töö, lk 16), kuna selle kohaselt peaks Saksamaa Eesti õigusabipalve täitma samasuguse kvaliteediga nagu ta teeks seda nende jaoks olulise kahju suuruse puhul. Kuna praegu see rahvusvahelise koostöö puhul nii ei toimi siis **võib liikmesriikide erinev kahju ulatuse käsitlemine mõjutada oluliselt vastastikkuse tunnustamise põhimõtte järgimist koostöö läbiviimisel**.

Intervjueeritavate sellist kokkuvõtvat seisukohta selgitab EL'i institutsiooniline ülesehitus, (käesolev töö, lk 13) mille kohaselt on liikmesriikidel võimalus oma institutsionaalset raamistikku reguleerida, mis hõlmab ka erinevat siseriiklikku reguleerimist. Liikmesriigid on neid võimalusi ka kasutanud. Arvestades nii intervjueeritavate seisukohti kui ka autori poolt käsitletud (käesolev töö, lk 20) problemaatikat seoses EL-i regulatsioonide rakendamisega, võib öelda, et EL-is ei ole tagatud ühtset süsteemi direktiivide rakendamisel ja ülevõtmisel.

Tabel 4. Tsitaadid ekspertintervjuudest kategooria „Õiguslikud probleemid" koodi erinevate riikide õiguskord kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, spetsialist	*"Ja siseriiklikud õigused on erinevad mingil määral, et paljudel näiteks ei võimalda, et mida meie Eestis teeme, teised ei saagi võib olla oma riigis teha üldse./.../ Võib öelda, et meie suured probleemid ei ole isegi nende väiksed probleemid."* (I1, 2017)
Riigiprokuratuur, juht	"*Kui me räägime kõige kuumemast ja seksikamast teemast praegu Euroopa Liidus, siis olukorras, kus Euroopa Kohus on 2014 teinud lahendi data preventioni osas, 2016 teinud uue lahendi, kus lisaks sellele, et varasem andmete säilitamise direktiiv on kehtetu./.../ ka riigisiseste seadusandluste osas on küsimus andmeside sideandmete säilitamises ja sellest muutunud õiguslikus raamistikus, kus ma ei tea enam, kas kõneeristusi on võimalik Euroopa Liidus üleüldse saada. Neid probleeme, on väga eri riikides ja eri mastist ja osades, mis annab meile Euroopa Kohus selle kandiku peal ise kätte probleemina."* (I4, 2017)

Kõik intervjueeritavad tõid olulise probleemina välja **õigusabipalvete** puhul riikidega suhtlemise ja taotluste rahuldamise ja ajamahukuse, samale järeldusele jõudis autor ka töö teooria osas (käesolev töö, lk 20). Õigusabipalvete probleemkohtadena märkisid PPA ametnikud riikide omavahelisi suhteid. Selleks, et rahvusvaheline koostöö toimiks, peab toimima EL'is ühtne menetluspraktika ja püüdlemine samade eesmärkide poole (käesolev töö, lk 20). Riigid, kellega on keeruline koostööd teha ei ole mitte ainult riigid väljaspool Euroopat, vaid ka EL liikmed, kes peaksid tegutsema samade direktiivide alusel, kuid praktikas see nii ei ole. Isegi naaberriikidega ei pruugi koostöö sujuda. Näitena tõi üks intervjueeritav välja juhtumi Leeduga, kus Leedus kuulati pealt ühte meest, mille käigus selgus, et ta peab plaani kaaslastega Eestisse tulla röövi toime panema. Eestile seda infot ei edastatud, vaid anti info planeerimise kohta, kui õigusabipalve kaudu oli palutud infot juba Eestis teo toimepannud röövlite kohta. Samad röövlid panid peale Eestis toime pandud röövi toime Soomes röövi katse ja Soome saatis Leedule mitu õigusabipalve taotlust. Kui röövlid olid kinni peetud ja ka Leedule teada antud, et röövlid käes, siis neli päeva hiljem saatis Leedu Soomele info, et nende isikute poolt plaanitakse toime panna rööv. Tegelikkuses oleks pidanud Leedu Eestile ja Soomele teabe ja jälitusteabe edastamise raamotsuse kohaselt omaalgatuslikult teada andma (käesolev töö lk 19) röövide toimepanemise plaanidest, et oleks saanud neid ennetada.

Õigusabipalvete aeganõudvuse probleemi käsitles enamus intervjueeritavatest. Õigusabipalveid võivad aeganõudvaks muuta, mitte ainult riikide suur töökoormus, mis tekitab lausa järjekorrad, vaid seda teeb ka näiteks erinevate riikide menetluskord (käesolev töö, lk 20). Näitena võib tuua, kui Soome poolt palutakse Eestis pealtkuulamine läbi viia. Kõigepealt peab Soome kohus andma loa jälitustoiming läbi viia ja seda saab seal anda maksimaalselt üheks kuuks, edasi pöördutakse Eesti poole, kus siis peab prokuratuur õigusabipalve üle vaatama, et see oleks korrektselt täidetud, millega siis pöördutakse Eesti kohtuniku poolt, kes peab jälitustoimingu läbiviimiseks loa andma. See kõik toimub enne, kui reaalselt saab toiminguid läbi viima hakata. Lisaks peab veel arvestama ülekuulamiste puhul, et kõik peab transkribeerima ja aega võtab veel ka tõlkimine, kuna Eestis peavad dokumendid olema eesti keeles ja Soomes soome keeles. Samuti tekitab aja probleeme asjaolu, et praegune õigusabi süsteem ei näe ette täitmise tähtaegu (käesolev töö, lk 19). Kuigi Euroopa uurimismäärus näeb ette õigusabipalvete tunnustamise tähtajad ei ole Eesti ja ka paljud teised riigid seda enda õigusesse inkorporeerinud. Riikide poolt raamotsuste erinev tõlgendamine või ülevõtmata jätmine toovad omakorda kaasa erinevaid probleeme (käesolev töö, lk 20).

Samuti tõid intervjueeritavad välja õigusabipalvete aeganõudvuse juures andmete säilitamise piirangu keerukuse (käesolev töö, lk 34-36). Pärast EK lahendeid andmete säilitamise kohta, kui

liikmesriigid lühendasid andmete säilitamise tähtaegu, tekkis probleem: kui andmeid säilitatakse ainult 3 kuud, kuid õigusabipalve võib aega võtta 6 kuud. Sellises olukorras ei saagi andmeid, kui ei kasutata otse kontakte või vastavaid koostöö programme.

Rahvusvahelise õigusabipalve süsteemi probleemid vastavad liberaalsete institutsionalistide käsitlusele, mille kohaselt rahvusvahelised institutsioonid nagu seda on ka EL võivad suurendada ja abistada rahvusvahelist koostööd (käesolev töö, lk 13), kuid ka EL ei suuda hõlmata kõikide liikmesriikide omavahelist suhtlust. Paraku on digitaaltõendid tihti just ajatundlikud, mistõttu õigusabipalvete aeganõudvus ja riikide omavahelised suhted takistavad ning piiravad oluliselt kiiret ja tõhusat koostööd (käesolev töö, lk 20; 24).

Tabel 5. Tsitaadid ekspertintervjuudest kategooria „Õiguslikud probleemid“ koodi õigusabipalved kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, spetsialist	*“Ma ütlengi, see ongi mille pärast paljud asjad kuhugi ei jõua või mõned asjad jäävad siis pimedaks, et lihtsalt on ammu teada, et millisest riigist saab informatsiooni ja millisest ei saa, et kust on võimalik edasi liikuda ja kus ei ole. Lisaks sellele, et tänapäeval on igasuguseid neid enda identiteedi varjamise vahendeid nii palju, et ma arvan, et paljud riigid ei saa ka nendes riikides endas asetsevatest serveritest või nendest teenusepakkujatest infot kätte tegelikult. Seal neid probleeme ikkagi on. /.../ Tänasel päeval kehtiv õigusabi süsteem seda kindlasti ei toeta. See on nii aeglaseks ja ajale jalgu jäänud. Ta mingite formaalsete päringute puhul toimib aga kui meil on operatiivselt vaja midagi teha siis selle kaudu ei ole võimalik seda teha tegelikult.”*(I1, 2017)
Pangaliit, juht	*“Rahvusvahelise koostöö on nii bürokraatlik ja aeganõudev, et küsidki mingeid andmeid ja saadki poole aasta pärast vastuse, siis tegelikult sellest vastusest selgub, et sul on vaja veel kolme muusse riiki välispäringuid teha, siis on see, et puhtalt nende õigusabi palvete järgi ootamine tapab selle menetluse ära. Sul hakkab aeguma see otsast.”* (I3, 2017)
PPA, spetsialist	*“alati on võimalik eelnev suhtlus, mis ei toimu õigusabipalve raames, vaid eelneva suhtluse käigus antakse teada, milliseid andmeid, mis hulgal on vaja, millele siis koostatakse näiteks kolme kuu pärast, siis õigusabipalve, mis jõuab lõpuks sellesse riikigi. Et see riik juba eelnevalt salvestab need andmed või hoiab neid andmeid, ei lase nendel andmetel ära kustuda.”* (I9, 2017)

Õigusabipalvete probleemi juures käsitlesid politseinikest intervjueeritavad ka **kiirkoostöö võrgu** nõrku kohti. Nimelt toodi välja, et kuigi on loodud kiirkoostöövõrk ja vajaduse korral fikseerib teine riik soovitud hetkeolukorra (käesolev töö, lk 24), mida saab kasutada ka õigusabipalvetega andmete säilitamise probleemi puhul. Probleem tekib sellega, et kogutud info edastatakse soovijale õigusabipalve raames, mis nagu eelpool mainitud, võib võtta kaua aega. Samas digitaalkeskkonna vahendusel ei pruugi koostööd vaja olla vaid kahe riigi vahel, vaid on ka olukordi, kui saadakse lõpuks soovitud informatsiooni õigusabipalve kaudu, kuid siis selgub, et on vaja sama protseduur veel mitmes teises riigis läbi viia, kuid selleks ajaks võivad tõendid juba kadunud või aegunud olla. Selline asjaolu vähendab võrgustiku kasulikkust. Üks intervjueeritav tõi välja ka võimaluse küsida teisest riigist soovitud teave koheselt infona ja õigusabipalvega saab selle hiljem kätte tõendi

väärtusena. Sellisel juhul oleks võimalik kiiremini saadud teabe põhjalt edasi tegutseda ja vältida info seismist. Pidades silmas asjaolu, et ainult üks intervjueeritav oskas välja tuua antud võimaluse, võib järeldada, et **erinevate koostöö instrumentide kasutusvõimalused ei ole laialdaselt levinud ka neid kasutavate ametnike seas.**

Tabel 6. Tsitaadid ekspertintervjuudest kategooria „Õiguslikud probleemid“ alamkoodi kiirkoostöövõrk kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, juht	*“Tõendiks muutub see, mis sulle õigusabitaotluse vastusena saadetakse. See info, mis sa enne saanud oled, seda on sul õigus kasutada ainult oma edasise menetluse planeerimiseks, millegi analüüsimiseks, väga nii-öelda taustainfona. Seda ei saa esitada kohtus tõendina, mitte enne, kui see ametlik vastus tuleb.”* (I6, 2017)

JIT temaatikat käsitledes erinesid intervjueeritavate arvamused. Ühest küljest küberkuritegevuse vastastest üksustest toodi välja, et kuna jälitus on tundlik teema, siis sellest eriti ei räägita ning kuna seal on raske ühtset praktikat luua, siis igaüks tegutsebki oma loovuse põhjal. Seda mõjutab ka riikide erinev menetluskord (käesolev töö, lk 20). Samuti toodi välja, et kuigi on pakutud JIT osalemist, on nendest keeldutud, kuna Eesti vastab õigusabipalvetele niivõrd kiiresti, siis ei ole JIT kuulumisel olulist ajavõitu (käesolev töö lk 18-19), seda eriti, kui info on eelnevalt meili peale saadetud. Sellisel juhul on tihti peale vastus juba valmis, kui ükskord ametlikku kanalit pidi õigusabipalve kohale jõuab. Samuti ei olnud rahapesu puhul ühtegi JIT isiklikku kokkupuudet olnud, kuid toodi näitena, et Eesti on edukalt kuulunud ka suuremate kaasuste lahendamistel JIT nagu näites *Ghost Click*’i kaasus. Kahel intervjueeritaval oli endal kogemus JIT’sse kuulumisega ja isikliku kogemuse põhjalt ei osanud nad midagi negatiivset välja tuua. Nende hinnangul võiks JIT’sid rohkem luua.

Samas intervjueeritavad, kes JIT’sse olid kuulunud, tõid välja selle positiivsete omadustena riikidevahelise infovahetuse kiirenemise, ning ühiste reeglite paika panemise nii, et kõik osapooled teadsid, mida teised riigid said teha ja mida mitte (käesolev töö, lk 18-19). Samuti toodi olulise omadusena välja uute otsekontaktide loomise, kuna JIT käigus loodud head suhted teiste riikide ametnikega, jäid kestma ka peale JIT lõppu.

Eeltoodut arvestades võib järeldada, et JIT loomise kasulikkus sõltub suuresti, millist liiki kuritegu menetletakse. Kui näiteks narkokuritegevuse uurimisel on JIT positiivsed omadused selgelt esile tulnud, siis küberkuritegude uurimisel ei ole see kasutegur piisavalt suur, et õigustada JIT loomist ning seda on võimalik isikliku kontakti ja õigusabipalvete koostööga asendada. Autori hinnangul on

see ainult kasulik, kui menetlejatel on võimalik piiriülese kuritegevusega võideldes erinevaid alternatiive kasutada. Samas peab arvestama, et kuigi Eesti vastab kiiresti õigusabipalvetele, ei pruugi teha seda riik, kellelt on vaja informatsiooni saada ja kui tegemist on rohkem kui ainult ühe toiminguga siis sõltuvalt kaasusest peaks ikkagi kaaluma JIT loomist.

Tabel 7. Tsitaadid ekspertintervjuudest kategooria „Õiguslikud probleemid" koodi JIT kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
Riigiprokuratuur, juht	*"Eesti on Euroopa Liidu liikmesriikidest üks esirinnas olevaid riike, kes erinevates JIT või siis riikidevahelistes uurimisrühmades osalenud. Ma arvan, et oleme Euroopa Liidus nende koguarvult kas top kolmes või top viie sees."* (I4, 2017)
PPA, spetsialist	*"/.../ põhimõtteliselt kui varem saatsid näiteks mingisuguse õigusabipalve kuskile, siis siin mingisugune paar kuud, ma arvan, läks aega enne kui lihtsalt mingisugune vastus tagasi tuli, siis selle puhul oli see, et kuna istumisel olid kohal kõigi riikide prokurörid kõigi riikide jälitusametnikud, siis selles mõttes oli hästi-hästi lihtne, kui õigusabipalve saatis põhimõtteliselt nädal nädal-paar ja siis selles mõttes sai, vajadusel neid igasuguseid toiminguid teha."* (I8, 2017)

Isiku põhiõiguste mittetagamist kui koostöö probleemi, toodi välja vähem kui pooltes intervjuudes. Intervjueeritavad olid ühisel seisukohal, et põhiõigused on Eestis piisavalt kaitstud ka jälitustoimingute läbiviimisel, kuna kohus on see objektiivne organ, kes hindab jälitustoimingu vajadust, *ultima ratio* tingimuse täitmist ja läbiviimise pikkust nii, et ei riivataks liigselt põhiõigusi. Samasugusel seisukohal on ka avalikkus (käesolev töö, lk 27-28) nõustudes, et riigil peab olema võimalus julgeoleku tagamiseks ilma loata isikuandmete töötlemisega, mis iseloomustab jälitustoiminguid, kui vajalikku kurjust (käesolev töö, lk 12).

Intervjueeritavate seisukoht, et isiku põhiõiguste kaitse on piisavalt tagatud, ei ühti töö dokumendianalüüsi tulemustega. Dokumendianalüüsis on analüüsitud erinevaid EIK, EK ja Eesti kohtute otsuseid (käesolev töö, lk 33-36), millest nähtub, et EL teeb muudatusi põhiõiguste kaitse paremaks tagamiseks, millest võib järeldada, et praegu ei ole need veel piisavalt kaitstud.

Tabel 8. Tsitaadid ekspertintervjuudest kategooria „Õiguslikud probleemid" koodi inimõiguste riive kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, juht	*"Kohus on võimeline hindama iga erineva loa puhul, iga erineva menetluse puhul, kas see on õigustatud või mitte."* (I2, 2017)
PPA, spetsialist	*"Tänapäeval on inimeste enda elu niivõrd digitaalne ja me hoiame erinevatel e-kontodel niivõrd palju informatsiooni enda kohta, et kas me saame öelda, et kas see riive on proportsionaalne kui ma tahan saada näiteks ainult seda ühte digitaalset tõendite mingi 100kB andmeid aga selle 100kB andmete hankimiseks pean ma koguma 1MB andmeid – piltlikult öeldes. Siis võib see riive olla suurem aga mina jällegi olen sellisel seisukohal, et selle riive maandab meil ära eeluurimiskohtunik kui ta ütleb, et see toiming ei ole õigustatud."* (I1, 2017)

Analüüsides intervjueeritavate väljatoodud õiguslikke probleemkohti digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel on selge, et enim probleeme tekitab riikide erinev õiguskord ja sellega seonduv. See aga näitab, et sõltumata EL'i institutsionaalsest ülesehitusest (käesolev töö, lk 13) ei ole selle sisene koostöö kriminaalasjade raames nii sujuv, kui on oodatud. See kinnitab töö teooria osas väljatoodud koostöö probleemkohti EL'i regulatsioonide erineval sisustamisel (käesolev töö, lk 20).

Teisele uurimisküsimusele, milliseid takistusi esineb praktikas digitaalkeskkonnas jälitustoimingute läbiviimisel, vastas teine kategooria, mis käsitles **praktilisi nõrku kohti.** Kõik intervjueeritavad leidsid, et on väga oluline tõsta nii praeguste kui ka tulevaste menetlejate **pädevust.** Probleemina leiti, et kiire tehnoloogia arenguga ei pruugi menetlejad olla teadlikud kõikidest võimalustest, kust tõendeid leida. See kehtib eriti küberkuritegude puhul, kuid digitaaltõendeid on võimalik leida iga kuritegu uurides. Sama seisukoha tõi autor välja ka töö teooria osas, mille kohaselt on infotehnoloogia ja kuritegevus järjest rohkem omavahelises seoses ja see paneb tõsiselt proovile politseinike võimekuse (käesolev töö, lk 11; 22). Nenditi, et otseselt piiriülese- ja küberkuritegevusega mitte kokku puutuv uurija ilmselt IP aadressi oskab küsida, kuid kardeti, et sellega asi ka piirdub. Selleks, et osata infot otsida, peab mõistma asja toimimise põhimõtet. Samuti toodi välja, et kui ka menetleja saab digitaalkeskkonnast info, siis peab ta oskama seda töödelda, analüüsida ja lõppkokkuvõttes suutma selle inimkeelde panna nii, et ka inimesed, kes seda valdkonda ei valda, aru saaks tõendi päritolust ja seetõttu ka selle usaldusväärsusest. Sama kinnitas ka dokumendianalüüsis analüüsitud M. Pirita kaasus, kus Ringkonnakohus tühistas Maakohtu otsuse just seetõttu, et Maakohus oli tõendeid valesti tõlgendanud, kuna ei saanud nendest piisavalt hästi aru. (käesolev töö, lk 36)

Menetlejate digitaalteadmiste puudulikkuse põhjusena tõid kõik intervjueeritavad välja sellealase väljaõppe nõrkuse. Politseinike õppekavas on digitaaltõendi käsitlemine alates 2013. aastast, (käesolev töö, lk 22) kuid oluline oleks õpetada lisaks digitaaltõendi tundmisele ka küberruumi eripära. Kuigi menetlejatele pakutakse TTÜ'ga koostöös digitaaltõenditele keskenduvaid koolitusi (käesolev töö, lk 6), ei oska menetlejad neid tahta kuna puuduvad üldteadmised, millist infot on võimalik digitaalkeskkonnast saada. Kui ei teata küberruumi võimalustest siis ei osata ka koolitusi soovida seal leiduva info saamiseks. Puudusi toodi enim välja küll küberruumi tundmise osas, kuid leiti, et puudu jääb ka jälitustoimingute olemuse selgeks tegemisest.

Tabel 9. Tsitaadid ekspertintervjuudest kategooria „Praktilised nõrgad kohad" koodi pädevus kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	Tsitaat
PPA, juht	*"mingisugune arusaam sellest, mis see küberruum on, mida seal leida võib, mida seal kindlasti ei ole. Millises olukorras kindlasti pead iseenda mõistust kriitiliselt hindama ja nõu küsima. Et kui ta selle äratundmise koolist saab siis on väga hästi."* (I6, 2017)
Riigiprokuratuur, juht	*"No selles mõttes, et elu ise teeb korrektuurid ju, et kui enamik tõendeid, mis üldse võimalik saada, on mingil digitaliseeritud kujul, siis see loob sellise väljapääsmatu olukorra, kus me ise seame - reeglid paika, et tekibki vajadus."* (I4, 2017)

Peaaegu kõik intervjueeritavad käsitlesid **digitaalkeskkonna võimekust**. Intervjueeritavad olid seisukohal, et tänapäeval saab väga palju informatsiooni inimeste kohta just digitaalkeskkonnast ja kuna internet ei tunne riigi - piire siis ei saa menetleda ilma rahvusvahelise koostööta. Sama rõhutavad ka erinevad Eesti arengu- ja tegevuskavad, mis toovad esile rahvusvahelise koostöö edendamise võitluses kuritegevusega (käesolev töö, lk 15). Digitaalkeskkonna eripära puhul toodi välja asjaolu, et inimesed ei taju kui palju jälgi neist tänapäeval digitaalkeskkonda maha jääb. See annab hea võimaluse menetlejale info leidmiseks, tuleb lihtsalt teada, kust otsida (käesolev töö lk 22).

Samuti annab digitaalkeskkond võimaluse jälitustoimingute läbiviimiseks menetleja riigis kohapeal, mis vähendab õigusabipalvete süsteemi koormust (käesolev töö, lk 24). Samas toodi digitaalkeskkonna puhul välja piiride puudumise, mille tõttu esineb sageli, et enamus inimesi, ei kurjategijaid ega kannatanuid, ei pruugi menetlevas riigis ollagi, vaid on tegemist variisikutega. Digitaalkeskkond loob anonüümsuse tunde ja annab asjatundlikematele hea võimaluse oma identiteeti varjata. Samad digitaalkeskkonna probleemid tulid välja nii töö teooria osas kui ka kohtuotsuste analüüsis (käesolev töö, lk 23; 36). Kui kannatanu ega kahtlustatav ei asu menetleja riigis, ei pruugi see ka riigi jaoks prioriteet olla.

Mõned intervjueeritavad tõid välja digitaalkeskkonna kiire arengu, mille tõttu ei pruugi õiguskaitse organisatsioonid omada vajalikke tehnilisi vahendeid. Kuritegevusega võitlevatele ametkondadele modernsete tehniliste vahendite võimaldamise vajaduse tõi autor välja ka töö teooria osas (käesolev töö, lk 7). Intervjueeritavad ei osanud küll tuua ühtegi näidet, mille puhul see oleks menetlust takistavaks teguriks osutunud, kuna tavaliselt on saadud uued vajalikud vahendid kiiresti soetatud. Teise digitaalkeskkonna arengust maha jääva elemendina toodi välja õigusnormid. Ühe intervjueeritava hinnangul ei jõua regulatsioonid digitaalkeskkonna arengule järele. Tema hinnangul on praegune õiguskord digitaalkeskkonna võimekusele jalgu jäänud ning juhtumeid lahendatakse *case by case*, kuna digitaalkeskkonna võimaluste, nt „asukoha puudumise", tõttu ühtset praktikat ei ole. Samasuguse Euroopa Nõukogu seisukoha tõi autor välja töö teooria osas (käesolev töö, lk 20).

Selle leevendamiseks tõi Euroopa Komisjon oma hiljutises raportis välja teenusepakkujatega tõhusama koostöö loomise vajaduse (käesolev töö, lk 24).

Paar intervjueeritavat tõid välja tehniliste võimaluste all ka serverilaenutused ja infohaldajad, mis muudavad rahvusvahelise koostöö hädavajalikuks (käesolev töö, lk 15; 23). Samuti toodi välja ka pilveteenuste puhul „asukoha puudumise“ element, mille puhul ei pruugi isegi teenuse pakkuja teada, kus info hetkel on.

Tabel 10. Tsitaadid ekspertintervjuudest kategooria „Praktilised nõrgad kohad“ koodi digitaalkeskkonna võimekuse kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, Juht	*“Ja jällegi tulles tagasi selle minu valdkonna küberi peale, siis seda üldjuhul on võimalik läbi viia siit Eestis, et ma ei peagi lootma, et teises riigis on mingi ametnik, kes peab viitsima minuga koostööd teha või mulle kuidagi abiks olla, et üldjuhul saab siit teha otse.”* (I2, 2017)

Peaaegu kõik menetlejad tõid välja **otse kontaktide** kasutamise tähtsuse. Kuigi käesoleva töö teooria osas tuvastas autor, et piiriüleste jälitustoimingute objektiivsemaks läbiviimiseks on oluline kindel õiguslik raamistik, (käesolev töö, lk 13) on rahvusvahelise koostöö kiirendamiseks ja sujuvamaks muutmiseks vaja kasutada ka isiklikke kontakte. Rahvusvahelise koostöö puhul kontaktide kasutamisel lisaks infovahetuse kiirendamisele tuuakse välja ka kvaliteedi paranemist. Mitmed intervjueeritavad väitsid, et kontakte kasutades saab täpsema ja põhjalikuma vastuse kui ainult ametlikke kanaleid kasutades. Samuti toodi välja, et kui on olemas ühe suurema riigiga, näiteks Inglismaaga, head kontaktid siis saab vajadusel nende kaudu ka Indiaga edukamalt koostööd teha.

Lisaks aitab otse kontaktide kasutamine rahvusvahelise koostöö puhul ka siis, kui on vaja koostööd teha kaasustega, millel võib ette tulla riikide erinevat kahju ulatuse käsitlemist. (käesolev töö, lk 39) Kui teine riik ei leia, et tegemist on olulise kaasusega, siis võivad õigusabipalved väga kaua aega võtta. Sellisel juhul saaks isiklikud kontaktid õigusabipalvet nn eelisjärjekorda panna.

Intervjueeritavad tõid välja, et selleks, et oleks kontakte läbi kelle koostööd tõhustada on vaja neid kõigepealt luua. Kõige parematekstööalaste kontaktide loomiseks peetakse mitte rahvusvahelisi koostöö koolitusi, vaid kokkusaamisi, mis koolituse päeva lõpus toimuvad. Veel soovitati üksuste vahel otse sidemete loomist ühiste külastuste raames. Näiteks ühe riigi küberüksuse ametnikud tulevad tutvuma teise riigi küberüksuse tööga või vastupidi. Selline vabamas õhkkonnas suhete loomine on intervjueeritavate hinnangul efektiivsem kui loengu stiilis koolitused.

Tabel 11. Tsitaadid ekspertintervjuudest kategooria „Praktilised nõrgad kohad“ koodi tutvused kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, juht	*“Midagi teha ei ole, kuigi kriminaalmenetluse seadustik seda ette ei näe siis kiired ja head, meile fokusseeritud vastused tulevad ikkagi sellise isikliku lobitööga.”*(I2, 2017)
PPA, spetsialist	*“Nuta või naera, aga sul peavad olema isiklikud kontaktid.”* (I5, 2017)
PPA, spetsialist	*“Absoluutselt, me kasutame kõiki kontakte sellises variatsioonis, mis kiirema tulemuse annab.” (I1, 2017)*

Üheks kasulikumaks meetmeks piiriüleste jälitustoimingute läbiviimisel ja üldiselt rahvusvahelise koostöö puhul tõid mõned intervjueeritavad välja **sideohvitserid**. Sellisel juhul oleks riigil oma esindaja, kelle poole saaks nad ise pöörduda, kui soovivad teise riigi õigusnormide või menetluskorra kohta infot, samas saab ka teine riik tema käest asukoha riigi kohta infot. Oluline on, et õigusabipalvete esitamisel oleks juba esimene kord see nii koostatud, et teisel riigil ei oleks õigusabipalve täitmisest keeldumiseks alust. Siinkohal on kasu sideohvitserist, kes saab anda kiiremini infot, et saaks esimese korraga õigusabipalve niiviisi esitatud, et see sobiks teisele riigile. Samuti toodi välja, et kui ühes suuremas riigis on sideohvitser, siis tema kaudu saab ka tegelikult lähikaudsete riikide menetluskorra ja õigusnormide kohta infot jagada. Lisaks on võimalik informatsiooni saada sideohvitseri kaudu ka käimasolevate menetluste kohta. Näiteks kui Eestis uuritakse kuritegelikku grupeeringut, kes tegeleb narkootiliste ainete transpordiga Hollandist Eestisse, siis sideohvitseri kaudu oleks võimalik saada infot selle kohta, kas ka Holland on teadlik toimuvast ja kas nad on omalt poolt menetlust alustanud. Sealt saab edasi kaaluda juba JIT loomist. Samas oskas üks intervjueeritavatest välja tuua asjaolu, et sideohvitser on kõige kallim koostöömeede ning selle asemel tuleks kindlasti enne teisi meetmeid kaaluda, kasvõi ajutiselt kedagi lähetusse saata.

Tabel 12. Tsitaadid ekspertintervjuudest kategooria „Praktilised nõrgad kohad“ koodi sideohvitser kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, juht	*“Tema saab teada, kui tahetakse õigusabitaotlust ja midagi mahukamat siis pöördutakse tema poole ja tema siis meie poole. Saame ennetada, neid tekkida võivaid probleeme.”* (I7, 2017)
MTA, spetsialist	*“Aga sideohvitser on absoluutselt kõige kallim meede. kui mingi riigiga on näha mingi trend, kasvab kuidagi mingi konkreetne probleem, mingi konkreetne case. Siis võib sinna kas või paariks kuuks inimese lähetada selles ei ole küsimust, see maksab riigile kordades vähem, kui keegi terve perega kuhugi elama saata, et ta seal siis nii-öelda kontakti hoiaksid. See sideohvitser on absoluutselt kõige kallim meede üleüldse, et on väga palju muid asju, mida tasub alati enne kaaluda, kui hakata kuskile sideohvitseri saatma.”* (I6, 2017)

Enamus intervjueeritavatest leidis, et rahvusvahelise koostöö puhul võib takistuseks saada ka riikide **motiveeritus**. Käesoleva töö teooria osas tõi autor välja liberaalsete institutsionalistide seisukoha, mille kohaselt saab riikidevaheline koostöö toimida ainult siis, kui kõik osapooled saavad sellest kasu (käesolev töö lk 13). Paraku ei esine iga kaasuse puhul selline olukord – nt on tegemist transiitriigiga, millest ainult läbi sõidetakse või siis on server laenutatud, milles info omaja on hoopis keegi kolmas. Taoliseid probleeme on autor ka eelpool välja toonud (käesolev töö, lk 23). Kuna ressursid on piiratud pea igal pool siis pannakse rõhku ikka sellele, mis enda riigile kasu toob. Samuti on see seotud erinevate kahju ulatuse käsitlemistega, mida analüüsiti koodi all erinevate riikide õiguskord (käesolev töö, lk 39).

Tabel 13. Tsitaadid ekspertintervjuudest kategooria „Praktilised nõrgad kohad“ koodi sideohvitser kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	Tsitaat
PPA, juht	*“Nii, et kogu selle rahvusvahelise koostöö puhul /…/ on põhiline võti see, et mõlemad osapooled, mõlemad riigid - neid võib olla rohkem kui kaks, soovivad selles asjas nii-öelda lahendust leida. Seadus annab hästi palju võimalusi, seadus ei ole nii-öelda politsei tööd piirav, pigem on küsimus selles, kas on aega ja ressurssi, kas teisel poolel on ka näiteks mingisugune oma huvi selles asjas. Kui nende jaoks on ka oluline teema siis see alati kiirendab ja lihtsustab protsessi.”* (I6, 2017)

Kolmandale uurimisküsimusele, **kuidas lahendada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevaid probleemkohti,** vastas kolmas kategooria, mis käsitleb **parendus ettepanekuid,** püüdis autor välja selgitada, millised on intervjueeritavate hinnangul digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise parendamiseks vajalikud tegevused. Peaaegu kõik intervjueeritavad tõid välja nii õiguslikke kui praktilisi parandusettepanekuid.

Praktilistest ettepanekutest kõige olulisema lahendusena rahvusvahelise koostöö probleemidele toodi välja otse kontaktide kasutamine. Otse kontaktidega suheldes saab kiirendada vajadusel nii õigusabipalvete täitmist, kui näidata teisele riigile, miks see vajalik on ja, et ka neil on sellest võimalik kasu saada ehk tõsta nende motivatsiooni koostööks (käesolev töö, lk 46). Lisaks muudab tuttavatega koostöö tegemine oluliselt ka töö kvaliteeti. Nimelt leiti, et kui õigusabipalve taotlusele vastaja on isik, kellega on varem edukalt koostööd tehtud või tuttav, siis saab lisaks kiiremale ka tunduvalt põhjalikuma vastuse. Lisaks sellele saab otsekontaktide kaudu teada, kuidas saada paremini koostööd teha. Näiteks kui esitada õigusabipalve teises riigis jälitustoimingu läbiviimiseks, on hea, kui see tuttavale ametnikule, kes sellega hiljem tegelema hakkab, ka e-mailile saata. Kui õigusabipalve ükskord ametlikke kanaleid pidi kohale jõuab, on täitja jõudnud sellega

juba tutvuda ja ettevalmistusi teha. Samamoodi ka vastupidi – täitja saab jooksvalt infot edastada taotluse esitajale, et edasine tegevus otsustada.

Lisaks toodi välja ka asjaolu, et tuttavad teavad või saavad üle täpsustada, kuidas oleks kõige targem infot küsida, et võimalikult palju infot ühe korraga saaks. Näiteks võib tuua jälle telefoni pealtkuulamise. Kui taotleja on esitanud taotluse, et numbrit pealt kuulata, aga pealtkuulates tuleb välja, et isik kasutab veel ka mõnda teist numbrit, siis ilma selle kohase nõudeta ei ole võimalik täitjal seda teist numbrit pealt kuulata. Kui aga taotleja on esitanud taotluse, et kuulataks pealt seda numbrit ja selle isikuga veel seonduvaid numbreid, siis ei oleks kiirem ja tõhusam mitte ainult antud kaasuse puhul rahvusvaheline koostöö, vaid jääks ära õigusabipalve süsteemi asjatu koormamine. Selline paar sammu ette mõtlemine muudaks omakorda juba õigusabipalvete süsteemi kiiremaks.

Teise praktilise soovitusena tõid enamus intervjueeritavaid välja väljaõppe kaasajastamise (käesolev töö, lk 44). Intervjueeritavate hinnangul on oluline, et juba koolis õpetataks digitaaltõendite ja küberkuritegevuse kohta (käesolev töö, lk 23). Oluliseks peeti just tulevastele ametnikele selgeks tegemist, kust kohast üldse on võimalik digitaaltõendeid otsida ja mis infot nende kaudu saada. Samuti on vaja see info ka hetkel töötavatele tavamenetlejateni jõuaks, näiteks koolituste kaudu.

Üks intervjueeritavatest tõi välja ka Europoli kasutamise võimaluse, mille menetluse juhtimise omadused tõi autor välja ka töö teooria osas (käesolev töö, lk 17). Tema hinnangul saaks Europoli kaudu leevendada nii õiguslikke kui praktilisi rahvusvahelise koostöö probleeme.

Tabel 14. Tsitaadid ekspertintervjuudest kategooria „Parendus ettepanekud“ koodi praktilised parendusettepanekud kohta (autori koostatud uuringu intervjuude analüüsi põhjal)

Ekspert	**Tsitaat**
PPA, juht	*“teha seda lobitööd pisut sinna alla, selle ajal ja pärast seda ka “aitäh” öelda, kui see tehtud, tulevikku vaadates, et siis on võimalik saada ka väga suurtest riikidest, mis muidu ägisevad õigusabipalvete all häid vastuseid.”* (I2, 2017)
PPA, juht	*“Kindlasti on abiks ja see osakaal, kus tõendid on ja kus inimesed üldse oma aega veedavad, ju kogu aeg kus nad on sinna poole kaldumas.”* (I6, 2017)
PPA, spetsialist	*“Europoli rolli ma näeksin, peaks tõusma tulevikus kindlasti*.” (I9, 2017)

Peale praktiliste ettepanekute tõid peaaegu kõik intervjueeritavad välja ka **õiguslikke parendusettepanekuid.** Kuigi töö teooria osas toodi välja, et EL’i institutsionaalne ülesehitus peaks edendama rahvusvahelist koostööd (käesolev töö, lk 13), leidsid mitmed intervjueeritavad, et bürokraatia peaks lihtsustuma. Täpsemalt toodi välja Euroopa tasandil õigusabipalvete süsteemi paindlikumaks muutmise lihtsustades ja ühtlustades siseriiklikke õigusi. Enim toodi selle

ettepaneku juures välja andmete säilitamise erinevusi, mida autor käsitles dokumendianalüüsis (käesolev töö, lk 36).

Samuti peaks Euroopa uurimismääruse ülevõtmine siseriiklikusse õigusesse ühtlustama õigusabipalvete täitmise aegu. Kuna Eesti keskmine õigusabipalvele vastamise aeg kattub uurimismääruse tähtaegadega, siis selles osas ei muutuks Eesti õigusesse ülevõtmisel midagi. Küll aga peaks oluliselt paranema just teistelt riikidelt saadavate vastuste kiirus. See ei tähenda muidugi aga kvaliteedi paranemist.

Tabel 15. Tsitaadid ekspertintervjuudest kategooria „Parendus ettepanekud“ koodi õiguslikud parendusettepanekud kohta (autori koostatud)

Ekspert	**Tsitaat**
Pangaliit, juht	*“Bürokraatia peab lihtsustama, aga see ongi see, et Eestis on väga raske seda muuta, me saame seda riigisiseselt seda teha võimalikult kiireks, ma usun et riigi seest ongi see isegi üpris kiire. Aga teisi riike mõjutada väga keeruline, aga selle vastu just aitabki see, et kui siin oleks see tugev üksus kes, keskelt tegeleb nende asjadega ja tal tõesti on see töökogemus”* (I3, 2017)
PPA, spetsialist	*“Ettepanek olekski seda paindlikumaks muuta kogu seda õigusabipalvete süsteemi. Kindlasti ühtlustada ja lihtsustada siseriiklike õigusi selles valdkonnas.”* (I1, 2017)

Kokkuvõtvalt saab öelda, et intervjueeritavad nõustusid enim seisukohaga, mille kohaselt on vaja luua otsekontakte erinevate riikide ametnikega nende praktika ja võimalustega tutvumiseks ja seeläbi arendada üldist infovahetust. Samuti peeti oluliseks tulevaste ametnike ning ka juba töötavate menetlejate IT alase teadlikkuse tõstmist.

2.3. Järeldused ja ettepanekud piiriüleste jälitustoimingute parendamiseks digitaalkeskkonnas

Magistritöö teoreetilises osas analüüsiti digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise teoreetilisi ja õiguslikke aluseid, rahvusvahelise koostöö funktsioone ning põhiinstrumente. Empiirilises osas viidi läbi dokumendianalüüs ning ekspertintervjuude võrdlev analüüs digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemide väljaselgitamiseks. Dokumendianalüüsi ja intervjuu käigus leiti vastused kõikidele uurimisküsimustele.

Esimesele uurimisküsimusele, milliseid õiguslikke probleeme esineb piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas, leiti vastus teooria osas ja dokumendianalüüsi

käigus. Teooria osast selgus, et suurimad probleemid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise regulatsioonis on EL-i õiguse ebapiisav ülevõtmine, riigisisese õiguse kohaldamata jätmine vastavalt uutele reeglitele, riigisisese õiguse vastuolu või õiguslikult reguleerimata olukord (käesolev töö lk 20). Dokumendianalüüsis selgus, et Eesti sõnumite saladuse kaitseala erineb EL'i omast (käesolev töö, lk 34), mis iseloomustab riigisisese õiguse vastuolu probleemi. Sama probleemi tõid välja ka kõik intervjueeritavad, kes kinnitasid töö teooria ja dokumendianalüüsi tulemusi, et rahvusvahelise koostöö probleeme võib tekitada nii siseriiklik erinev õiguskord kui ka EL'i raamotsuste erinev tõlgendamine (käesolev töö, lk 39). Kuigi kõik intervjueeritavad tunnistasid eelkirjeldatud probleemi, tõi enamik intervjueeritavatest välja, et selle lahendamine on iga liikmesriigi enda ülesanne ja seda ei ole võimalik mõjutada.

Samuti selgus nii teooria osast (käesolev töö, lk 33), dokumendianalüüsist (käesolev töö, lk 25) , kui ka ekspertintervjuudest (käesolev töö, lk 38), et kehtiv kriminaalmenetluse seadustik ei arvesta digitaaltõendite eripäradega. Kogutud tõendite usaldusväärsuse hilisemaks hindamiseks on vaja jälitustoimingute dokumenteerimist selles osas, mis puudutab digitaalandmete kogumise protsessi ning andmete autentsuse ja terviklikkuse tagamise meetmete kirjeldamist (käesolev töö, lk 25). Praegune KrMS seda ette ei näe. Lisaks on Eesti õigusnormides piiritlemata kaugläbiotsimise ja võrgu pealtkuulamise erinevus (käesolev töö, lk 25; 33).

Seetõttu teeb autor ettepaneku:

1) KrMS §126[10] lg 2 tekstist jätta välja fraas "vajaduse korral" (Tehver, 2016)

Intervjueeritavate hinnangul tekitab probleeme riikide erinevas kahju ulatuse käsitlemisel (käesolev töö, lk 39), mille tõttu ei pruugi õigusabipalve saanud riik mõista kaasuse tõsidust ja seetõttu taotluse täitmine pikale venida. Sellega seoses tunnistas enamik intervjueeritavatest otsekontaktide kasutamise vajalikkust, kuna otse suheldes saab õigusabipalve täitmist kiirendada. Kõigest kaks intervjueeritavat nägi rahvusvahelise koostöö edendamisel Europoli (käesolev töö, lk 17; 49) kasutamise vajalikkust, see tähendab autori hinnangul, et ametnikud ei tule selle peale, et rahvusvahelise koostöö organisatsioonide poole pöörduda. Sellest võib järeldada, et kuna Eesti ei saa mõjutada teiste riikide õigusnorme ega menetluskorda, siis on vajalik rahvusvahelist koostööd kiirendada läbi otse kontaktide ja koostöö organisatsioonide.

Eeltoodust tulenevalt teeb magistritöö autor ettepaneku PPA'le

2) Viia läbi erinevate riikide ametnike ühiseid koolitusi, koostööharjutusi ja vahetusprogramme, ning külastusi erinevate riikide samade üksuste vahel.

3) Viia läbi õppepäev menetlejatele Europoli ja teiste koostööorganisatsioonide võimaluste tutvustamiseks.

Teise õigusliku probleemina võib välja tuua õigusabipalvete mittesobivuse digitaalsete tõendite kogumiseks (käesolev töö, lk 20). Sama probleemi tõid välja ka kõik intervjueeritavad, kes nentisid, et õigusabipalved võtavad kaua aega, mis pidurdab või raskendab menetluse läbiviimist (käesolev töö, lk 40). Mitu intervjueeritavat tõi välja ka rahvusvahelise koostöö toimimise sõltuvuse riikide vahelistest suhetest (käesolev töö, lk 40). Samas toodi välja, et õigusabipalvetele on võimalik saada kiiremini vastuseid kui on vastajaga head suhted.

Samuti selgus teooria osast (käesolev töö, lk 20), dokumendianalüüsist (käesolev töö, lk 35) ja intervjuude analüüsist (käesolev töö, lk 38), et õigusabipalvete süsteemi toimimist raskendab ka EL'i raamotsuste erinev tõlgendamine või liikmesriikide õigussüsteemi inkorporeerimise edasi lükkamine. Seda on teinud ka Eesti Vabariik, näiteks ei ole Eesti Euroopa uurimismäärust (käesolev töö, lk 19-20), mille eesmärgiks on rahvusvahelise koostöö tõhustamine ja mis määraks õigusabipalve tunnustamise tähtajad, KrMS'i inkorporeerinud. Sellest võib järeldada, et rahvusvaheline koostöö toimiks tõhusamalt kui EL'i raamotsuseid ja direktiive sisustataks siseriiklikult ühtlasemalt ja õigeaegselt.

Seetõttu teeb autor ettepaneku:

4) Eestis viia KrMS'i Euroopa uurimismäärus, mis seaks õigusabipalvetele vastamise tähtajad.

Õigusabipalvete probleemi juures käsitlesid politseinikest intervjueeritavad ka kiirkoostöö võrgu nõrku kohti. Nimelt toodi välja, et kuigi on loodud kiirkoostöövõrk ja vajaduse korral fikseerib teine riik soovitud digitaalse hetkeolukorra (käesolev töö lk 24), kuid probleem tekib sellega, et infot edastatakse soovijale õigusabipalve raames, mis nagu eelpool mainitud võib võtta kaua aega. Samas digitaalkeskkonna vahendusel ei pruugi koostööd vaja olla ainult kahe riigi vahel, vaid sõltuvalt informatsioonist võib vaja olla ka edasisi päringuid teha. Antud probleemi lahenduseks oskas ainult üks intervjueeritavatest välja pakkuda võimaluse paluda õigusabipalvega soovitud teave infona eelnevalt kätte saada, et vajadusel ajatundlike menetlustoimingutega jätkata ja kui õigusabipalve vastus saabub, siis saab selle teabe tõendina vormistada. Sellest võib järeldada, et menetlejad ei ole teadlikud kiirkoostöö võrgu kasutusvõimalustest (käesolev töö, lk 42).

Eeltoodust lähtudes teeb magistritöö autor ettepaneku PPA'le:

5) Viia läbi koolitused kriminaalpolitseile kiirkoostöö võrgustiku kohta

Koostöö instrumendi **JIT** osas erinesid intervjueeritavate arvamused. Küberüksustes töötavad ametnikud leidsid, et kuigi on pakutud JIT osalemist, on nendest keeldutud, kuna Eesti vastab õigusabipalvetele niivõrd kiiresti, siis ei ole JIT kuulumisel olulist ajavõitu (käesolev töö lk 42), seda eriti otsekontakte kasutades. Sellisel juhul on tihti - peale vastus juba valmis, kui ükskord ametlikku kanalit pidi õigusabipalve kohale jõuab. Samas ametnikud, kes olid JIT'sse kuulunud tõid välja selle infovahetuse kiiruse, menetluse ühtluse ning kontaktide saamise, mida saab ka tulevikus kasutada (käesolev töö, lk 19; 42).

Eeltoodut arvestades võib järeldada, et kuigi JIT loomisel on palju kasulikke omadusi, on siiski isikliku kontakti ja õigusabipalvete kaudu võimalik seda asendada. Autori hinnangul on see ainult kasulik, kui menetlejatel on võimalik piiriülese kuritegevusega võideldes erinevaid alternatiive kasutada. Samas peab arvestama, et kuigi Eesti vastab kiiresti õigusabipalvetele, ei pruugi teha seda riik, kellelt on vaja informatsiooni saada ja kui tegemist on rohkem kui ainult ühe toiminguga, siis peaks sõltuvalt kaasusest kaaluma ikkagi JIT loomist.

Seetõttu teeb autor ettepaneku PPA'le ja MTA'le:

6) Siseveebis artikli vahendusel tutvustada JIT'de parimaid praktikaid kriminaalpolitseile ja MTA uurijatele.

Inimõiguste riive osas erinesid oluliselt dokumendi- ja intervjuude analüüsi tulemused. Dokumendianalüüsi käigus kohtuotsuste analüüsist selgus, et EL suurendab inimõiguste kaitset tühistades vajadusel ka direktiive ja võttes vastu uusi inimõigusi enam kaitsvaid määruseid (käesolev töö lk 34-36). Samuti on EL'i sõnumite saladuse kaitseala Eesti omast laiem (käesolev töö, lk 34). Intervjueeritavad olid aga ühisel seisukohal, et inimõigused on Eestis piisavalt kaitstud ka jälitustoimingute läbiviimisel. See seisukoht ei ole aga kooskõlas dokumendianalüüsi tulemustega (käesolev töö, lk 43). Autori hinnangul on selline vastuolu põhjendatud intervjueeritavate ametikohtade iseloomust tulenevalt (vt tabel 2.) ning on dokumendianalüüsile ja töö teoreetilisele osale tuginedes seisukohal, et jälitustoimingute läbiviimise puhul on tegemist vajaliku kurjusega (käesolev töö, lk 12) ja peamine on tasakaal julgeoleku tagamise ja inimõiguste kaitse vahel (käesolev töö, lk 13).

Teisele uurimisküsimusele, milliseid takistusi esineb praktikas digitaalkeskkonnas jälitustoimingute läbiviimisel, leiti vastus dokumentide ja intervjuude analüüsimise käigus. Kõik intervjueeritavad tõid välja, et kiire tehnoloogia arenguga ei pruugi menetlejad olla teadlikud kõikidest võimalustest, kust tõendeid leida (käesolev töö, lk 44), mis ühtis teooria osas väljatooduga (käesolev töö, lk 22). Samuti toodi välja digitaalkeskkonna kiire areng, millega peab kursis olema (käesolev töö, lk 44).

Menetlejate digitaalteadmiste puudulikkuse põhjuseks tõid kõik intervjueeritavad välja väljaõppe sellealase nõrkuse (käesolev töö, lk 44). Puudusi toodi enim välja küberruumi tundmise osas, kuid leiti, et puudu jääb ka jälitustoimingute olemuse mõistmisest. Kuigi digitaaltõendi käsitlemise õpe on politsei õppekavas, on oluline, et menetlejad teaks lisaks sellele, kuidas sündmuskohalt ohutult arvutit kaasa võtta ilma tõendeid kontamineerimata, kuidas küberruumis infot otsida ja millised võimalused selleks on. Samale järeldusele jõudis magistritöö autor ka töö teooria osas, kus selgus, et kuigi digitaalkeskkonna võimalusi tulevastele ametnikele õpetatakse, ei tehta seda piisavas mahus (käesolev töö, lk 22)

Sellest tulenevalt teeb autor Sisekaitseakadeemiale ettepaneku:

7) Suurendada õppemahtu, mille raames õpetatakse IT võimekust ja digitaalkeskkonnas tõendite kogumist;

Intervjueeritavad juhtisid tähelepanu ka **digitaalkeskkonna võimekusele,** mille juures toodi välja, et tänapäeval saab väga palju informatsiooni inimeste kohta just digitaalkeskkonnast (käesolev töö, lk 45) ja kuna internet ei tunne riigi - piire, siis ei saa ilma rahvusvahelise koostööta (käesolev töö, lk 13; 22). Digitaalkeskkond annab võimaluse jälitustoimingute läbiviimiseks menetleja riigis kohapeal tehes koostööd ISP'ga (käesolev töö, lk 24), mis vähendab õigusabipalvete süsteemi koormust. Digitaalkeskkonna pakutavad võimalused jälitustoimingute läbiviimiseks ühtivad infrastruktuurilise jälitusteooriaga, mille puhul on jälitustoimingud näiliselt võrgustatud ja toetuvad digitaaltehonoloogiale (käesolev töö, lk 11). Samuti tõid eksperdid välja, et digitaalkeskkonna kiire arenguga ei pruugi õiguskaitseorganitel olla vastavaid tehnilisi lahendusi (käesolev töö, lk 36-37; 45). Sellest võib järeldada, et ka eriala eksperdid tunnetavad, et digitaalkeskkonna arengutest mitte oluliselt maha jääda on vaja end pidevalt kursis hoida ja ka tehnilisi vahendeid kaasajastada.

Eeltoodut arvestades teeb autor PPA'le ettepaneku:

8) Viia läbi koolitusi või õppepäevi kriminaalmenetlejate seas digitaalkeskkonna võimaluste ning arengute kohta, k.a ISP'ga koostöö arendamiseks.

9) Tagada menetlejatele kaasaegsed tehnilised vahendid digitaalkeskkonnas jälitustoimingute läbiviimiseks.

Väga oluliseks peeti intervjueeritavate seas ka **ametnike otsekontaktide** kasutamist, ilma milleta oleks paljude hinnangul väga raske piiriüleseid jälitustoiminguid läbi viia (käesolev töö, lk 46). Rahvusvahelise koostöö puhul otsekontaktide kasutamisel lisaks infovahetuse kiirenemisele tuuakse välja ka kvaliteedi paranemist. Mitmed intervjueeritavad väitsid, et otsekontakte kasutades saab täpsema ja põhjalikuma vastuse kui ainult ametlikke kanaleid kasutades. Tegemist on sellise koostöö vahendiga, mis oluliselt lihtsustab, kiirendab ja tõstab koostöö kvaliteeti.

Umbes pooled intervjueeritavatest tõid välja ühe kasulikuma meetmena piiriüleste jälitustoimingute läbiviimisel ja üldiselt rahvusvahelise koostöö puhul **sideohvitserid** (käesolev töö, lk 46). Kõige suurema boonusena sideohvitseride olemasolu puhul nähti, et selle näol oleks riigil oma esindaja, kelle poole saaks nad ise pöörduda kui soovivad teise riigi kohta infot, samas saab ka teine riik tema käest asukoha riigi kohta infot. Samas toodi välja, et sideohvitser on kõige kallim koostöö meede. Intervjuusid läbi viies jäi käesoleva töö autorile mulje, et sideohvitseri mõistet ei sisustata ühtemoodi. Arvestades, et sideohvitser on kallis meede teeb autor ettepaneku PPA'le ja MTA'le :

10) Sideohvitseride asemel suurendada ekspertide lähetustesse saatmise võimalusi.

Kuigi riikide **motiveerituse** puudulikkust rahvusvahelise koostöö osas oskasid välja tuua ainult pooled intervjueeritavatest, siis kinnitas seda ka töö teoorias väljatoodu liberaalsete institutsionalistide seisukoht, mille kohaselt saab riikidevaheline koostöö toimida ainult, siis kui kõik osapooled saavad sellest kasu (käesolev töö lk 13). Kuna ressursid on piiratud igal pool, siis pannakse rõhku sellele, mis enda riigile kasu toob. Motivatsiooni tõstmiseks oskasid intervjueeritavad välja tuua ainult otse kontaktide kaudu teise poole koostööle innustamist. Autori hinnangul on tegemist siiski olulise probleemiga ja seda ka intervjueeritavate arvates, kuna motiveeritus ühtib ka eelpool väljatoodud riikide erineva kahju ulatuse käsitlemise probleemiga. Seetõttu on ka ettepanekud samad.

Kolmandale uurimisküsimusele, kuidas lahendada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevaid probleemkohti, leiti vastused ekspertintervjuude käigus. Selgus, et paljusid probleeme saab, kui just mitte lahendada siis leevendada otse kontakte

kasutades. Kõik intervjueeritavad tõid välja ka väljaõppe kaasajastamise vajaduse (käesolev töö, lk 48). Autor nõustub intervjueeritavate sellise seisukohaga ning peab vajalikuks digitaalkeskkonna õppe sisseviimise politsei õppekavasse, samuti on oluline koolitada antud valdkonnas juba töötavaid menetlejaid. Intervjueeritavate ettepanekud ühtivad antud osas juba varem töös väljatoodud ettepanekutega.

Lisaks praktilistele ettepanekutele pidasid enamus intervjueeritavatest probleemide lahendamiseks vajalikuks ka õiguslikke muudatusi. Enim tõid intervjueeritavad välja Euroopa tasandil õigusabipalvete süsteemi paindlikumaks muutmise lihtsustades ja ühtlustades siseriiklikke õigusi, mis ühtib teoorias väljatoodud seisukohaga, mille kohaselt töötab EL sellessuunas, et jälitustoimingute läbiviimiseks oleks kriminaalkoostöö ühtlane ja sujuv (käesolev töö, lk 20). Samuti toodi välja ühtsete direktiivide vajaduse, seda eriti andmete säilitamise osas, kuna EK otsus direktiiv tühistada (käesolev töö, lk 34-35) on rahvusvahelist koostööd raskendanud. Dokumendianalüüsis välja toodud 2018. aasta kevadel kehtima hakkav isikuandmete kaitse üldmäärus peaks seda võimaldama.

Eeltoodust nähtub, et suur osa digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel esinevaid probleeme on seotud rahvusvaheliste suhete ja EL'i põhiselt lahendatavad liikmesriikide ühiselt seatud eesmärkide kaudu. See kinnitab teoorias käsitletud liberaalsete institutsionalistide seisukohta, mille kohaselt rahvusvahelised institutsioonid ja organisatsioonid võivad suurendada ja abistada rahvusvahelist koostööd (käesolev töö, lk 13). Digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise parendamiseks tegi autor uuringu põhjal 11 ettepanekut, mis on kokkuvõtlikult toodud tabelis 16.

Tabel 16. Digitaalkeskkonnas piiriüleste jälitustoimingute praktika järeldused ja ettepanekud (käesoleva töö autori koostatud magistritöö põhjal)

DIGITAALKESKKONNAS PIIRÜLESTE JÄLITUSTOIMINGUTE LÄBIVIIMISE PRAKTIKA JÄRELDUSED JA ETTEPANEKUD

Probleemid		Järeldused	Ettepanekud
Õiguslikud probleemid	Erinevate riikide õiguskord	Eesti ei saa mõjutada teiste riikide õigusnorme ega menetluskorda, seetõttu on vajalik rahvusvahelist koostööd läbi ametnike otsekontaktide ja koostöö organisatsioonide kiirendada. Digitaaltõendite usaldusväärsuse hilisemaks hindamiseks on vaja jälitustoimingute dokumenteerimist.	1) Toetada erinevate riikide ametnike ühiseid koolitusi, koostööharjutusi ja vahetusprogramme, ning külastusi erinevate riikide samade üksuste vahel erinevate riikide samade üksuste vahel. 2) Viia läbi õppepäev menetlejatele Europoli ja teiste koostööorganisatsioonide võimaluste tutvustamiseks (nt Europoli kaudu on võimalik vajadusel kiirendada õigusabipalve täitmist). 3) KrMS §126[10] lg 2 tekstist jätta välja fraas "vajaduse korral".
	Õigusabipalved	Õigusabipalvete süsteem aeglane, ning ei sobi digitaaltõendite kogumiseks.	4) Eestis viia KrMS'i Euroopa uurimismäärus, mis seaks õigusabipalvetele vastamise tähtajad, ning ühtlustaks EL piires tõendite kogumise taktikat.
	24/7	Menetlejate teadlikkus 24/7 ja selle võimalustest on nõrk.	4) Viia läbi tutvustused kriminaalpolitseile kiirkoostöö võrgustiku kohta.
	JIT	Õigusabipalvete süsteemi aeganõudvuse tõttu suurendada JIT'de loomist.	5) Siseveebis artikli vahendusel tutvustada JIT'de parimaid praktikaid kriminaalpolitseile ja MTA uurijatele.
Praktilised probleemid	Menetlejate digitaalteadlikkuse puudulikkus	Menetlejad ei ole teadlikud kõikidest võimalustest, kust digitaalkeskkonnas tõendeid leida ja seda väljaõppe puudulikkuse tõttu.	6) Suurendada õppemahtu SKA's, mille raames õpetatakse IT võimekust ja digitaalkeskkonnas tõendite kogumist.
	Digitaalkeskkonna võimekus	Selleks, et digitaalkeskkonna arengutest mitte oluliselt maha jääda on vaja end pidevalt kursis hoida ja ka tehnilisi vahendeid kaasaegsena hoida.	8) Viia läbi koolitusi või õppepäevi kriminaalmenetlejate seas digitaalkeskkonna võimaluste ning arengute kohta, k.a ISP'ga koostöö arendamiseks. 9) Tagada menetlejatele kaasaegsed tehnilised vahendid digitaalkeskkonnas jälitustoimingute läbiviimiseks.
	Ametnike otsekontaktid	Otsekontaktide kasutamisel lisaks infovahetuse kiirenemisele paraneb ka koostöö kvaliteet.	• Kasutada ka ettepanekut nr 1.
	Sideohvitser	Kasulik, kuid väga kallis meede.	11) Sideohvitseride asemel suurendada lähetustesse saatmise võimalusi.
	Motiveeritus	Koostöö on riikide motiveerituse tõttu raskendatud kui õigusabipalve saanud riik koostööst ise kasu ei saa.	• Kasutada ettepanekuid nr 1 ja 2.
EL tasandil		Riikide endapoolne EL'i regulatsioonide erinev siseriiklik sisustamine ja kohaldamata jätmine raskendavad oluliselt rahvusvahelist koostööd	• EL'i regulatsioonide ühtlustamist ja juhendite või standardite väljatöötamist piiriüleste jälitustoimingute läbiviimise lihtsustamiseks digitaalkeskkonnas.

KOKKUVÕTE

Käesolev magistritöö otsis vastust **uurimisprobleemile**, milliseid tõrkeid ja takistusi esineb piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas? Magistritöö **eesmärgiks** oli välja selgitada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohad ja esitada uurimispõhiselt rakendusettepanekuid nende lahendamiseks. Eesmärgi saavutamiseks püstitas autor kolm uurimisküsimust, millele vastuste leidmine andis võimaluse esitada ettepanekud digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohtade lahendamiseks.

Uurimisprobleem sai poolstruktureeritud ekspertintervjuude ja dokumendianalüüsi tulemusel põhjendatud lahenduse ning magistritöö eesmärk digitaalkeskkonnas piiriüleste jälitustoimingute rakendusprobleemide lahendamiseks esitatud ettepanekute kaudu täidetud. Magistritöö väärtus seisneb digitaalkeskkonnas läbiviidavate piiriüleste jälitustoimingute probleeme käsitlevate hinnangute analüüsimises, nende võrdlemises valdkonna teoreetiliste käsitlustega, kohtute praktikaga ning uuringust tulenevate järelduste põhjal vastavate ettepanekute tegemises.

Magistritöö eesmärgi saavutamiseks ja uurimisprobleemile vastuse leidmiseks püstitati kolm uurimisülesannet. **Esimeseks uurimisülesandeks** oli analüüsida teoreetilisi ja õiguslikke aluseid piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas, selgitamaks välja levinumad probleemid. Uurimistöös jõuti järeldusele, et suurimad probleemid digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise regulatsioonis on EL-i õiguse ebapiisav ülevõtmine, riigisisese õiguse kohaldamata jätmine vastavalt uutele reeglitele, riigisisese õiguse vastuolu või õiguslikult reguleerimata olukord. Kaasa arvatud Eesti sõnumi saladuse kaitseala kitsus võrreldes EL'i omaga. Samuti õigusabipalvete süsteemi mittesobivus digitaalsete tõendite kogumiseks ja digitaalkeskkonna „asukoha puudumise" võimalus. Dokumendianalüüsi käigus kohtuotsuste analüüsist selgus, et EL suurendab inimõiguste kaitset tühistades vajadusel ka varasemaid direktiive inimõiguste tagamiseks ja võttes vastu uusi määrusi. Eeltoodut võttis autor arvesse teise uurimisülesande täitmisel digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohtade väljaselgitamiseks.

Teiseks uurimisülesandeks oli välja selgitada dokumendianalüüsi ja ekspertintervjuudega, milliseid tõrkeid ja takistusi esineb piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas. Selgus, et eksperthinnangud ühtisid enamjaolt magistritöö teooria osas ning dokumendianalüüsis väljatooduga - et enim probleeme tekitab riikide erinev õiguskord. Samuti kinnitasid

intervjueeritavad töö teoorias välja toodut, et praegune õigusabipalvete süsteem ei sobi digitaaltõendite kogumiseks, kuna on liiga aeglane ajatundlike digitaaltõendite kogumiseks. Seejuures tuli ekspertintervjuude analüüsist välja, et teadmised kiirkoostöövõrgu kasutamise võimalikkusest olid piiratud või puudusid täielikult. Puudusi leiti ka menetlejate IT alases teadlikkuses.

Väljaselgitatud probleemidest tulenevalt ei taga olemasolevad rahvusvahelise koostöö instrumendid optimaalseid tulemusi digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel, seejuures on selliste probleemide põhjustajaks olulises osas õigusabitaotluste süsteem, mis on üldiselt aeglane ning digitaalsete tõendite saamiseks ebaefektiivne, kuna ei arvesta digitaaltõendi ajakriitilisusega. Kõik intervjueeritavad toetasid rahvusvahelise koostöö probleemide lahendamist ja edasiarendamist.

Enamik intervjueeritavaid tõid välja ka vajaduse täiendada või muuta EL-i ja/või Eesti piiriüleste jälitustoimingute läbiviimist käsitlevaid regulatsioone. Lisaks leiti, et vajalik on tõsta menetlejate teadlikkust digitaalvõimekusest ja seda nii politsei õppekava kaasajastades kui ka juba töötavate menetlejate koolitamisega. Samuti peetakse väga oluliseks otse kontaktide olemasolu, mis koostöös esinevate probleemide esinemisel aitavad nende mõju menetlusele vähendada.

Kolmandaks uurimisülesandeks oli välja töötada ettepanekud ja soovitused digitaalkeskkonnas piiriüleste jälitustoimingute tõhustamiseks. Sellise eesmärgi täitmiseks töötas magistritöö autor ekspertintervjuude, dokumendianalüüsi ning teooria kõrvutamise põhjal välja ettepanekud digitaalkeskkonnas piiriüleste jälitustoimingute rakendusprobleemide lahendamiseks, mis on kokkuvõtlikult toodud tabelis 16. Autor peab digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemide lahendamisel oluliseks EL'i regulatsioonide ühtlustamist ja juhendite või standardite väljatöötamist piiriüleste jälitustoimingute läbiviimise lihtsustamiseks digitaalkeskkonnas. Tuginedes intervjueeritavate seisukohtadele teeb autor ettepaneku suurendada oluliselt politseinike digitaalkeskkonna võimekuse väljaõpet ja pöörata tähelepanu ka juba hetkel töötavate ametnike sellealasele koolitamisele, juhendamisele ning toetada otse kontaktide loomist teise riigi ametnikega koostöö edendamiseks.

Eeltoodust tulenevalt sai magistritööle püstitatud eesmärk täidetud. Töö autori hinnangul aitavad uuringu tulemused ja sellele tuginedes tehtud ettepanekud kaasa rahvusvahelise koostöö edenemisele digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel. Magistritöös lähtuti probleemide väljaselgitamisel õiguslikest ja praktilistest probleemidest digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel, kuid edaspidi võiks keskenduda digitaalkeskkonnas

läbiviidavate jälitustoimingute tehnilisele ja metoodilisele poolele. Antud juhul nõuaks töö riigisaladuse käitlemise luba, kuid antud valdkonnas oleks vaja uuring läbi viia, kuna mitmed intervjueeritavad tõid välja, et jälitustoimingute läbiviimise tehnilises ja metoodilises osas esineb mitmeid probleeme.

SUMMARY

This MA dissertation is seeking an answer to problems about the delays and obstacles in carrying out cross-border surveillance activities in the digital environment. The aim is to establish the problematic issues in surveillance activities in the digital environment and to suggest research-based proposals for solving them. In order to achieve the aim, the author set three research questions, the answers to which enabled to make such suggestions.

The research issue was given a carefully reasoned solution through semi-structured expert interviews and document analysis; the aim of solving problems in cross-border surveillance activities in the digital environment was fulfilled via the presented suggestions. The hoped merits of the current MA as a research paper lie in analysing evaluations dealing with problems of cross-border surveillance in the digital environment, in comparing them with theoretical treatments within the relevant field, the practice of the courts and in making suggestions relying on the reached conclusions.

Three tasks were set to attain the aim of the dissertation and to find an answer for the investigated problem. The first task was to analyse the theoretical and legal foundations of cross-border surveillance activities, establishing the more widely-occurring problems. The dissertation concluded that the biggest problems in the regulation of cross-border surveillance in the digital environment include the insufficient adaptation of EU law to national laws, not applying national law according to new regulations, conflicts within national law or a legally unregulated situation. Also, the secrecy of messages in Estonia is not so strictly protected as in the EU. Also the unsuitability of the system of legal aid requests for gathering digital evidence and the possibility of "loss of location" of the digital environment. Analysing court judgements in the course of document analysis, it transpired that the EU increases human rights protection, when necessary annulling directives and passing new regulations. The author took into consideration the above when fulfilling the second research task, establishing the problems in cross-border surveillance activities in the digital environment.

The second research task was to establish, via document analysis and expert interviews, what kind of delays and obstacles occur in cross-border surveillance activities in the digital environment. It turned out that expert assessments largely coincided in the theoretical part of the MA thesis and in what was established by document analysis. Document analysis and interview analysis established that most problems are caused by different national legislations. The interviewees confirmed what

was said in the theoretical part of the dissertation, i.e. the current system of legal aid requests is not suitable for gathering digital evidence, as it is too slow. The bodies conducting proceedings had sometimes poor cyber knowledge. Similarly, the interviewees were of the opinion that the system of legal assistance requests was too bureaucratic and time-consuming. Moreover, the expert analyses showed that any knowledge on how to use 24/7 network was limited or altogether lacking.

On the basis of established problems, the existing instruments of transnational cooperation do not guarantee optimal results in cross-border surveillance activities in digital environment, whereas the problems are largely caused by the EU countries. All interviewees supported more transnational cooperation in solving these problems.

Most underlined the necessity to supplement or change the EU and/or Estonian regulations concerning cross-border surveillance activities. They also found that it was crucial to raise the awareness about the digital power of bodies conducting proceedings, both by updating police curricula as well as by training the already operating bodies. Direct contacts were also deemed crucial, as they would help to lessen the impact of weak points in cooperation on proceedings.

The third research task was to list proposals and recommendations in order to make cross-border surveillance activities more efficient. For that aim, the author worked out proposals on the basis of expert interviews, document analysis and theory for solving problems in cross-border surveillance activities in digital environment. These are presented in Table 16. The author considers it crucial to homogenise EU regulations and to work out directives and standards in order to simplify the cross-border surveillance activities in the digital environment. Relying on the views of the interviewees, the author suggests a considerable improvement in the knowledge of the police in the field of digital environment, and to pay attention to more training and supervising of the employees already working in the field. She also encourages making contacts with employees in other countries and thus furthering all cooperation.

On the basis of the above, the aim of the MA dissertation was met. In the author's view, the results of the research and subsequent proposals could help increase transnational cooperation in carrying out cross-border surveillance activities. The dissertation focused on establishing the problems, but in future various technical and methodical aspects of surveillance activities in the digital environment should be tackled. In that case, the paper would require permission to access state secrets. However, research is truly needed because quite a number of interviewees underlined that the technical and methodical part in surveillance activities still contains various problems.

VIIDATUD ALLIKATE LOETELU

Andrei Pavlištšuki kriminaalasi KarS § 164 järgi (2012), 3-1-1-31-12.

Andres Sarapuu ja Jüri Oidekivi kriminaalasi KarS § 184 lg 2 p 1, 2 ning Ervin Kurmi kriminaalasi KarS § 184, lg 1 järgi (2011), 3-1-1-31-11.

Argomaniz, J., 2014. European Union responses to terrorist use of Internet. *Cooperation and Conflict.* 50(2), pp. 250–268. [Võrgumaterjal] Leitud: http://journals.sagepub.com/doi/abs/10.1177/0010836714545690 [Kasutatud 21.12.2016].

Avutikuritegudevastane konventsioon (2004).

Barnard-Wills, D. & Wells, H., 2012. Surveillance, technology and the everyday. *Criminology & Criminal Justice*, Vol 12(3), pp. 227-237. Leitud: Sage Journals Online [10.05.2017].

Bazeley, P. & Jackson, K., 2013. *Qualitative data analysis with NVivo.* 2 ed. London: Sage.

Bhatt, H., 2006. RIPA 2000: a human rights examination. *International Journal of Human Rights,* Vol 10(3), pp. 285-314.

Bindar, V., 2010. Aspects regarding judicial cooperation in criminal matters in the light of the Lisbon Treaty. *Annals of the "Constantin Brancusi" University of Targu Jiu, Juridical Sciences Series,* Issue 4, pp. 201–210. Leitud: HeinOnline [21.12.2016].

Bocaniala, T. & Bocaniala, A., 2012. Aspects of European Cooperation in the Fight against Cross-border Crime. *Contemporary Readings in Law and Social Justice,* 4(2), pp. 509–516. Leitud: EBSCOHost [21.07.2015].

Bowden, C., 2013. *The US Surveillance Programmes and Their Impact on EU Citizens' Fundamental Rights.* Brussels: European Parliament.

Brands, J. & Schwanen, T., 2014. Experiencing and governing safety in the night-time economy: nurturing the state of being carefree. *Emotion, Space and Society,* Vol 11, pp 67–78.

Brunton, F. & Nissenbaum, H., 2013. Political and ethical perspectives on data obfuscation. Rmt: M. Hildebrandt & K. De Vries, toim-d. *Privacy, due process and the computational turn*. New York: Routledge, pp. 164–188.

Brenner, S.W., 2007. Cybercrime: Re-thinking crime control strategies. Rmt: Y. Jewkes toim., *Crime Online*. Portland, OR: Willan, pp.12–28.

Brown, I. & Korff, D., 2009. Terrorism and the proportionality of Internet surveillance. *European Journal of Criminology*. 6(2). pp. 119–134. Leitud: Sage Journals Online [21.12.2016]

Clarke, R. (1988). Information technology and dataveillance. *Communications of the ACM*, Vol 31(5), pp 498–512.

Copland vs. Ühendkuningriik (2007) EIKo 62617/00.

Council of the European Union, 2011. *Joint Investigation Teams Manual.* Brussels: Council Secretariat.

Council on Foreign Relations, 2013. *The Global Regime for Transnational Crime.* [Võrgumaterjal] Leitav: http://www.cfr.org/transnational-crime/global-regime-transnational-crime/p28656 [Kasutatud 19.12.2016].

Creswell, J. W., 2003. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches.* 2 ed. Thousand Oaks, London, New Delhi: Sage.

Davies, S., 2014. *Väärikus inimõiguste kontekstis* [Võrgumaterjal] Leitav: https://www.youtube.com/watch?v=PiTkSaJpwsw. [Kasutatud 20.09.2016]

Deleuze, G.,1992. Postscript on the Societies of Control. *The MIT Press: October.* Vol 59, pp 3-7.

Department of Justice, 2007. *Computer Crime & Intellectual Property Section*. [Võrgumaterjal] Leitav: http://www.oas.org/juridico/english/cyb20_network_en.pdf [Kasutatud 30.06.2015].

Digital Rights Irelang ja Seitlinger jt. EKo (2014) C-293/12 ja C-594/12.

Eesti Vabariigi põhiseadus (2015).

Eesti Vabariigi valitsuse ja Ameerika Ühendriikide valitsuse vahelise lepingu vastastikusest õigusabist kriminaalasjades muutmise kokkuleppe ratifitseerimise seadus (2006).

Elektroonilise side seadus (2004).

Ering, S. O., 2011. Trans-border Crime and Its Socio-economic Impact on Developing Economies. *J Sociology Soc Anth*. 2(2). pp. 73-80 Leitud: KRE Publishers [20.11.2016].

Estonian Cyber Security News Aggregator, 2016. *Court decision on alleged SMIT account blocker.* [Võrgumaterjal] Leitav: https://cybersec.ee/tag/mart-pirita/ [Kasutatud 03.04.2017].

Euroopa Komisjon, 2010. *Komisjoni teatis Euroopa Parlamenile ja nõukogule*: *ELi sisejulgeoleku strateegia toimimine: viis sammu turvalisema Euroopa suunas.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52010DC0673&from=EN [Kasutatud 01.04.2016].

Euroopa Komisjon, 2014. *Komisjoni teatis Euroopa Parlamendile, Nõukogule Avatud ja turvalise Euroopa muutmine tõelisuseks.* [Võrgumaterjal]
Leitav: http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/an_open_and_secure_europe_-_making_it_happen_et.pdf
[Kasutatud 28.10.2016].

Euroopa Komisjon, 2016. *Council conclusions on improving criminal justice in cyberspace.* [Võrgumaterjal] Leitav: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/ [Kasutatud 04.05.2017].

Euroopa Inimõiguste ja põhivabaduste kaitse konventsioon (1996).

Euroopa Liidu Nõukogu, 2010. *Project on Cybercrime: Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* [Võrgumaterjal] Leitav: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3df [Kasutatud 28.04.2017]

Euroopa Liidu Nõukogu, 2014. *T-CY assessment report: The mutual legal assistance provisions of the Budapest Convention on Cybercrime.* [Võrgumaterjal] Leitav: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c [Kasutatud 04.05.2017]

Euroopa Liidu Nõukogu, 2015. *Eelnõu: nõukogu järeldused Euroopa Liidu sisejulgeoleku uuendatud strateegia (2015-2020) kohta.* [Võrgumaterjal] Leitav: http://data.consilium .euroa.eu/doc/document/ST-9798-2015-INIT/et/pdf [Kasutatud 04.12.2016].

Euroopa Liidu Nõukogu, 2016. *Vastastikuste hindamiste seitsmenda vooru hindamisaruanne: Küberkuritegevuse ennetamise ja sellega võitlemise Euroopa poliitika praktiline rakendamine ja toimimine.* [Võrgumaterjal] Leitav: http://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/et/pdf [Kasutatud 27.04.2017]

Euroopa Liidu Teataja, 1992. *Treaty of Maastricht on European Union.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3Axy0026 [Kasutatud 04.11.2016].

Euroopa Liidu Teataja, 1997. *Treaty of Amsterdam amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts*. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:11997D/TXT [Kasutatud 12.12.2016].

Euroopa Liidu Teataja, 2000. *Euroopa Liidu liikmesriikide vaheline kriminaalasjades vastastikuse õigusabi konventsioon*. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32000F0712(02) [Kasutatud 12.12.2016].

Euroopa Liidu Teataja, 2001. *Treaty of Nice amending the Treaty on European Union, the Treaties establishing the European Communities and certain related acts.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:12001C/TXT [Kasutatud 12.12.2016].

Euroopa Liidu Teataja, 2002a. *Nõukogu otsus, 28. veebruar 2002, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1451906790166&uri=CELEX:32002D0187 [Kasutatud 12.12.2016].

Euroopa Liidu Teataja, 2002b. Nõukogu raamotsus, 13. juuni 2002, ühiste uurimisrühmade kohta. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/ALL/?uri=CELEX%3A32002F0465 [Kasutatud 12.12.2016].

Euroopa Liidu Teataja, 2005a. *Komisjoni teatis Nõukogule ja Euroopa Parlamendile - teatis kriminaalasjades tehtud kohtuotsuste vastastikuse tunnustamise ja liikmesriikidevahelise usalduse tugevdamise programmi kohta.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A52005DC0195 [Kasutatud 01.11.2016].

Euroopa Liidu Teataja, 2005b. *Haagi programm: vabaduse, turvalisuse ja õiguse tugevdamine Euroopa Liidus*. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52005XG0303(01) [Kasutatud 01.11.2016].

Euroopa Liidu Teataja, 2006. *Euroopa Liidu liikmesriikide õiguskaitseasutuste vahelise teabe ja jälitusteabe vahetamise lihtsustamise kohta 2006/960/JHA* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32006F0960 [Kasutatud 01.11.2016].

Euroopa Liidu Teataja, 2007. *Küberkuritegevuse vastase võitluse üldise poliitika kujundamine.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/summary/ET/URISERV:l14560 [Kasutatud 01.02.2017].

Euroopa Liidu Teataja, 2008a. *Nõukogu otsus 2009/426/JSK, 16.12.2008, millega tugevdatakse Eurojusti ja muudetakse otsust 2002/187/JSK, millega moodustatakse Eurojust, et tugevdada võitlust raskete kuritegude vastu.* [Võrgumaterjal] Leitav: https://publications.europa.eu/et/publication-detail/-/publication/d865eac2-06cc-4a67-a613-ae2cbae56fbd/language-et [Kasutatud 01.11.2016].

Euroopa Liidu Teataja, 2008b. *Euroopa tõendikogumismäärust esemete, dokumentide ja andmete kogumiseks kriminaalmenetluses kasutamise eesmärgil* (2008). [Võrgumaterjal] Leitav: http://publications.europa.eu/resource/cellar/20069902-d0dc-4820-9a5f-28037724bfa0.0008.02/DOC_1 [Kasutatud 01.11.2016].

Euroopa Liidu Teataja, 2009a. *Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut 2007/C 306/01.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/ALL/?uri=OJ:C:2007:306:TOC [Kasutatud 04.11.2015].

Euroopa Liidu Teataja, 2009b. *Nõukogu otsus 2009/371/JSK, 6. aprill 2009, millega asutatakse Euroopa Politseiamet (Europol).* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32009D0371#ntr2-L_2009121ET.01003701-E0002 [Kasutatud 02.10.2016].

Euroopa Liidu Teataja, 2010a. *Stockholmi programm - avatud ja turvaline Euroopa kodanike teenistuses ja nende kaitsel*. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=celex:52010XG0504(01) [Kasutatud 04.11.2015].

Euroopa Liidu Teataja, 2010b. *Euroopa Liidu põhiõiguste harta.* [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:et:PDF [Kasutatud 11.05.2017].

Euroopa Liidu Teataja, 2014. *Euroopa Parlamendi ja nõukogu direktiiv 2014/41/EL, 3. aprill 2014, mis käsitleb Euroopa uurimismäärust kriminaalasjades.* [Võrgumaterjal] Leitav: http:// eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:32014L0041 [Kasutatud 02.10.2016].

Euroopa Liidu Teataja, 2015. Komisjoni teatis Euroopa Parlamendile, Nõukogule, Euroopa Majandus- ja Sotsiaalkomiteele ning Regioonide Komiteele: Euroopa julgeoleku tegevuskava. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/HTML/?uri=CELEX:52015DC0185&from=EN [Kasutatud 04.05.2017].

Euroopa Liidu Teataja, 2016. *EUROOPA PARLAMENDI JA NÕUKOGU MÄÄRUS (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus)*. [Võrgumaterjal] Leitav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32016R0679 [Kasutatud 28.03.2017].

Euroopa Liit, 2015. *ELi Ametid.* [Võrgumaterjal] Leitav: http://europa.eu/about-eu/agencies/index_et.htm [Kasutatud 09.09.2016].

Euroopa Parlament, 1999. *Tampere European Council 15 and 16 october 1999 Presidency Conclusions.* [Võrgumaterjal] Leitav: http://www.europarl.europa.eu/summits/tam_en.htm [Kasutatud 13.01.2017].

Euroopa Parlament, 2014. *Euroopa Parlamendi 27. veebruari 2014. aasta resolutsioon soovitustega komisjonile Euroopa vahistamismääruse läbivaatamise kohta.* [Võrgumaterjal] Leitav: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0174+0+DOC+XML+V0//ET [Kasutatud 13.01.2017].

Euroopa Parlament, 2015. *Euroopa Parlamendi resolutsioon Euroopa Parlamendi prioriteetide kohta komisjoni 2016. aasta tööprogrammiks.* [Võrgumaterjal] Leitav: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+MOTION+B8-201506 63+0+DOC+XML+V0//ET&language=et [Kasutatud 13.01.2017].

Flick, U., 2009. *An Introduction to Qualitative Research*, 4. London: SAGE Publications.

Flick, U., 2011. *Introducing Research Methodology: A Beginner's Guide to Doing a Research Project.* Los Angeles, London, New Delhi, Singapore, Washington DC: Sage.

Foucault, M., 2002. Power: essential works of Foucault 1954–1984, Vol. 3 Rmt: J.D. Faubion, toim. London: Penguin Books.

FRA, 2015. *Annual Report 2014.* [Võrgumaterjal] Leitav: http://fra.europa.eu/en/publication/2015/fundamental-rights-challenges-and-achievements-2014 [Kasutatud 13.01.2017].

French, M. & Smith, G.JD., 2016. Surveillance and Embodiment. *Body & Society.* Vol 22(2). pp. 3-27. Leitud: Sage Journals Online [09.05.2017]

French, M., & Browne, S., 2014. Profiles and profiling technology: Stereotypes, surveillance and governmentality. Rmt: D. Brock, A. Glasbeek, C. Murdocca, toim-d. *Representation and Regulation: Thinking Differently About Crime.* Toronto: Univeristy of Toronto Press. pp. 251-284.

Galic, M., Timan, T., Koops, B.-J., 2017. Bentham, Deleuze and Beyond: An Overview of Surveillance Theories from the Panopticon to Participation. *Philosophy & Technology*, Vol 30(1), pp. 9-37.

Gandy, O., 1989. The surveillance society: Information technology and bureaucratic social control. *Journal of Communication 39(3),* pp. 61-76.

Ginter, J., Plekksepp, A., Soo, A., Kairjak, M., Kangur, A., Mets, T., 2013. *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses.* [Võrgumaterjal] Leitav: http://www.kriminaalpoliitika.ee/et/analuus-isikute-pohioiguste-tagamisest-ja-eeluurimise-kiirusest-kriminaalmenetluses [Kasutatud 04.05.2017].

Goos, K., Friedewald, M., Webster, C. W. R. & Leleux, C., 2015. The co-evolution of surveillance technologies and surveillance practices. Rmt: D. Wright & R. Kreissl, toim-d. *Surveillance in Europe.* London, New York: Routledge, pp. 51–100.

Haggerty, K., 2006. Tear down the walls: on demolishing the panopticon. Rmt: D. Lyon, toim-d. *Theorising surveillance: The panopticon and beyond.* Portland: Willan Publishing, pp. 23–45.

Haggerty, K. D. & Ericson, R. V., 2000. The surveillant assemblage. *British Journal of Sociology*, Vol 51(4), pp. 605–22.

Hallinan, D., 2015. Effects on surveillance on freedom of assembly, association and expression. Rmt: D. Wright & R. Kreissl, toim-d., *Surveillance in Europe*. London, New York: Routledge, pp. 268–271.

Heldna, E., 2016. Julgeolekuasutuste kogutud informatsiooni kasutamine kriminaalmenetluses ja jagamine uurimisasutustega. *Juridica X*, pp 718-726.

Hoye, J. M. & Monaghan, J., 2015. Surveillance, freedom and the republic. *European Journal of Political Theory*, pp. 1-21. Leitud: Sage Journals Online [29.01.2017].

Hurt, U., 2013. *Politsei- ja Piirivalveameti ning TTÜ koostööleppe rakendamises osaleb ka Logistikainstituut*. [Võrgumaterjal] Leitav: https://www.ttu.ee/ttu-uudised/uudised/instituudid/logistikainstituut-3/politsei-ja-piirivalveameti-ning-ttu-koostooleppe-rakendamises-osaleb-ka-logistikainstituut/ [Kasutatud 26.10.2016].

Inimõiguste Instituut, 2012. *Inimõigused* [Võrgumaterjal] Leitav: https://www.eesti.ee/est/kodakondsus/inimoiguste_kaitse/inimoigused_1 [Kasutatud 26.10.2016].

Inimõiguste Instituut, 2014. *Privaatsusõigus inimõigusena ja igapäevatehnoloogiad* [Võrgumaterjal] Leitav: http://www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-II-osa-Uuringu-kokkuvote1.pdf. [Kasutatud 26.09.2016].

Ivor Onksioni kriminaalasi KarS § 137 lg 1 ja § 156 lg 1 järgi, Priit Toobali kriminaalasi KarS § 137 lg 1 – § 22 lg 2, § 156 lg 1 – § 22 lg 2, § 344 lg 1 järgi ja Lauri Laasi kriminaalasi KarS § 137 lg 1 – § 22 lg 2, § 156 lg 1 – § 22 lg 2 järgi (2015), 3-1-1-93-15.

Jackson, R. & Sorensen, G., 2015. *Introduction to International Relations: theories and approaches.*VI. Oxford: Oxford University Press.

Jupille, J., & Caporaso, J., 1999. Institutionalism and the European Union: Beyond International Relations and Comparative Politics. *Annual Review of Political Science, Vol. 2*, pp. 429-444.

Justiitsministeerium, 2010. *Kriminaalpoliitika arengusuunad aastani 2018*. [Võrgumaterjal] Leitav: http://www.just.ee/sites/www.just.ee/files/elfinder/article_files/seletuskiri_kriminaalpoliitika_arengusuunad_aastani_2018.pdf [Kasutatud 31.01.2017].

Justiitsministeerium, 2016. *Rahvusvaheline õiguskoostöö*. [Võrgumaterjal] Leitav: http://www.just.ee/et/eesmargid-tegevused/rahvusvaheline-oiguskoostoo [Kasutatud 30.06.2015].

Karistusseadustik (2016).

Keevallik, A., 2014. *CyberCrime Konverents 2014*. [Võrgumaterjal] Leitav: https://www.conference-expert.eu/et/cybercrime-konverents-2014 [Kasutatud 27.04.2017].

Keohane, R.O. &Martin, L.L., 1995. The Promise of Institutionalist Theory. *International Security, 20,* pp. 39–51. The MIT Press: London.

Kergandberg, E., 2000. Jälitustegevus kui riigisaladus ja jälitustegevuse tulemina saadud tõendi spetsiifika. *Juridica,* IX, pp. 602–611.

Kergandberg, E., Järvet, T., Ploom, T. & Jaqqo, O., 2004. *Kriminaalmenetlus 2*. Tallinn: Sisekaitseakadeemia.

Kergandberg, E. & Sillaots, M., 2006. *Kriminaalmenetlus*.Tallinn: Juura.

Kergendberg, E., 2005. Natuke privaatsusest ja mõnevõrra enam selle jälitustegevlikust riivest isikuandmeid töötleva Eest avaliku võimu poolt. *Juridica*, VIII, pp. 544–552.

Kergandberg, E. & Sillaots, M., 2006. *Kriminaalmenetlus.* Tallinn: Juura

Koch, L. C., Niesz, T. & McCarthy, H., 2014. Understanding and Reporting Qualitative Research: An Analytical Review and Recommendations for Submitting Authors. *Rehabilitation Counseling Bulletin*, 57(3), pp. 131-143. Leitud: Sage Journals Online. [15.01.2017].

Krevald, J., 2013. *Tõendite lubatavus kriminaalmenetluses.* Magistritöö, Tartu: Tartu Ülikool.

Kriminaalmenetluse seadustik (2016).

Kruusamäe, M. & Timo, R., 2013. *Jälitustegevuse kohtulik eelkontroll Eestis*, Tartu: Riigikohus.

Laaneoks, E., 2010. *Sissejuhatus võrgutehnoloogiasse.* Tartu: Tartu Ülikool.

Laherand, M.-L., 2008. *Kvalitatiivne* uurimisviis. Tallinn: OÜ Infotrükk.

Laos, S., 2008a. *Õiguskantsleri 2007. aasta tegevuse ülevaade.* [Võrgumaterjal] Leitav: https://www.riigiteataja.ee/aktilisa/0000/1303/2210/13032213.pdf# [Kasutatud 19.05.2015].

Laos, S., 2008b. *Riigi sisejulgeolekut tagava jälitustegevuse eesmärgid ja kontroll*. Akadeemia 11, pp. 2403–2446.

Leppänen, A.; Kiravuo, K.; Kajantie, S., 2016. Policing the cyber-physical space. *The Police Journal: Theory, Practice na Principles.* 89(4). Leitud: Sage Journals Online [31.01.2017].

Liiv, E., 2014. Kas eraisikul on õigus unustusele Internetis? *Juridica IX,* pp. 643-651.

Linask, R., 2014. *Jälitustoimingute regulatsioon ettenähtavuse aspektist,* Magistritöö, Tallinn: Tartu Ülikool.

Lipartito, K., 2010. *The economy of surveillance.* [Võrgumaterjal] Leitav: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1582218 [Kasutatud 19.01.2017].

London, M., 2011. *Politsei- ja õigusalase koostöö areng Euroopa Liidus, teabe ja tõendite vahetus Euroopa Liidu liikmesriikide vahel*. Magistritöö, Tallinn: Tartu Ülikool.

Lott, A., 2015. *Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis.* [Võrgumaterjal]Leitav:http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf [Kasutatud 04.01.2017].

Lõhmus, U., 2008. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. *Juridica VII,* pp. 462–472.

Lõhmus, U., 2010. Põhiõiguste kaitse kolmnurgas riik – Euroopa Nõukogu – Euroopa Liit. *Juridica V*, pp 354-370 .

Lõhmus, U., 2014. *Põhiõigused kriminaalmenetluses.* Teine väljaanne toim. Tallinn: Juura.

Lõhmus, U., 2016a. Kontroll jälitustegevuse üle (kriitiline analüüs). *Kohtute aastaraamat 2015,* pp 59-72.

Lõhmus, U., 2016b. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. *Juridica III,* 175-183.

Lyon, D., 2001. *Surveillance Society: Monitoring Everyday Life*. Philadelphia: Open University Press

Lyon, D., 2007. Surveillance studies: an overview. Cambridge: Polity.

Madisson, K., 2015. *Jälitustegevus ja salajane pealtkuulamine kui jälitustoiming*. Magistritöö, Tallinn: Tartu Ülikool.

Mahoney, C., 1997. Overview of Qualitative Methods and Analytic Techniques. Y. Frechtling & L. Sharp Westat, eds. *User-friendly Handbook for Mixed Method Evaluations.* s.l.: DIANE Publishing, p. Part II/3.

Majandus- ja Kommunikatsiooniministeerium, 2014. *Küberjulgeoleku strateegia 2014-2017*. [Võrgumaterjal] Leitav: https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf [Kasutatud 27.04.2017].

Malone vs. Ühendkuningriik (1984) EIKo 8691/79.

Mart Pirita kriminaalasi KarS § 207 lg 1 järgi, (2016) 1-15-509/50.

Marx, G.T., 1988. *Undecover: Police Surveillance in America.* Berkeley, CA: University of California.

Mikli, S., 2015. Kui kauge Euroopa Liidu õigus saab järsku igapäevatöö osaks: probleeme Euroopa Liidu õiguse ülevõtmisel ja rakendamisel õiguskindluse põhimõtte kontekstis. *Juridica,* II, lk 103–112.

Minarik, T; Osula, A.-M., 2016. Tor does not stink: Use and abuse of the Tor anonymity network from the perspective of law. *Computer Law & Security Review.* Vol 32/1, pp 111-127.

Nhan, J.& Huey, L., 2011. Policing through nodes, clusters and bandwitch. Rmt: S. Leman-Langlois. toim., *Technocrime: Technology, Crime and Social Cotnrol.* NY: Routledge pp. 66-87.

Nilsson, H. G., 2006. *From classical judicial cooperation to mutual recognition. Revue internationale de droit pénal*, 77, pp. 53–58. Publisher: ERES.

Osula, A.-M., 2015. Mutual Legal Assistance & Other Mechanisms for Accessing Extraterritorially Located Data. *Masaryk University Journal of Law and Technology,* Vol 9, pp 43-64.

Osula, A.-M., 2017. *Remote search and seizure of extraterritorial data.* Doktoritöö, Tartu: Tartu Ülikool.

Owsley, B.L., 2016. Teaching Criminal Procedure – Especially the Fourth Amendment on Electronic Surveillance – to Everyone but Law Students. *Saint Louis University Lae Journal*, 60(3), pp. 507-514. Leitud: EBSCOhost. [31.03.2017].

Parkin, J., 2012. EU Home Affairs Agencies and the Construction EU Internal Security. [Võrgumaterjal] Leitud: https://www.ceps.eu/publications/eu-home-affairs-agencies-and-construction-eu-internal-security [Kasutatud 03.12.2016].

Parm, U., 2014. *Pilvandmetöötlus*. Andmekaitse Inspektsioon [Võrgumaterjal] Leitav: http://www.aki.ee/et/pilvandmetootlus [Kasutatud 29.04.2017].

Passas, N., 2002. *Cross-border crime and the interface between legal and illegal actors*. Rmt: P.C. van Duyne, K. von Lampe &N. Passas, eds. *Upperworld and Underworld in Cross-Border Crime.* Nijemegen: Wolf Legal Publishers, pp. 11–42.

Perling, L., 2014. Eessõna. *Juridica VIII*, pp. 573–574.

Politsei- ja Piirivalveamet, 2011. *Infotehnoloogiakutitegude menetlemise käsiraamat. s.l.* Phare mestiprojekt.

Ploom, T., 2010. *Strasbourgi konventsioonist Lissaboni lepinguni: Rahvusvaheline koostöö kriminaalasjades.* Tallinn: Juura.

Ploom, T., 2016. Jälitustoimingute infosüsteem ja järelevalve jälitustoimingute seaduslikkuse üle. *Kohtute aastaraamat 2015*, pp 109-114.

Porter, M., 1996. Tackling Cross Border Crime. Rmt: B. Webb, toim. *Crime Detection and prevention services*. London: Crown. pp. 1–39

Pruulmann-Vengerfeldt, P., 2014. *Väärikus inimõiguste kontekstis.* [Võrgumaterjal] Leitav: https://www.youtube.com/watch?v=EIQt19VP3M4 [Kasutatud 20.09.2016].

Raba, K., 2002. Õigusalane koostöö kriminaalasjades. Arengust Euroopa Liidus. *Juridica* II, pp. 126–131.

Reiner, R., 2000. *The Politics of the Police. Oxford*: Oxford University Press.

Riigikogu, 2008. *Lissaboni lepingu, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut, ratifitseerimise seaduse 193 SE seletuskiri.* [Võrgumaterjal] Leitav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=dea3f64e-4a15-5197-e589-7986 bcb7dee4& [Kasutatud 02.11.2015].

Rijken, C., 2006. Joint Investigation Teams: principles, practice, and problems. *Utrecht Law Review*, 2, pp. 99–118.

Rondel, M., 2016. Informatsioonilise enesemääramise õigus ja jälitustegevus: isiku õigus teada saada tema suhtes tehtud jälitustoimingutest. *Juridica X*, pp 709-717.

Ross, J.E., 2007. The place of covert surveillance in democratic societies: a comparative study of the United States and Germany. *Annual Review of Law and Society*, Vol 4, pp. 493-579.

Ruve Veski, Jaanus Lauri, Tõnu Schasmini ja Roland Feodorovi kriminaalasi KarS § 212 lg 1 järgi, (2015) 3-1-1-51-14.

Saar, J.; Marina, A.; Resetnikova, A.; Ginter, J.; Sootak, J.; Parmas, A., 2013. *Eesti õiguskaitseasutuste koostöö Euroopa Liidu liikmesriikidega piiriülese kuritegevuse tõkestamisel (olukord enne ja pärast liitumist Euroopa Liiduga)* [Võrgumaterjal] Leitav: https://www.riigikantselei.ee/valitsus/valitsus/et/riigikantselei/euroopa/arhiiv/uuringud/2002-2003-tellitud-uurimused/2_uurimus.pdf [Kasutatud 18.10.2016].

Schofield, P., 2009. *Bentham: a guide for the perplexed.* London: Continuum.

Schengen Facility vahendite kasutamise kord, (2011).

Schwartz, P. M., 2002. *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance.* California: Berkley Law.

Schwerha, J.J., 2010. *Project on Cybercrime: Law Enforcement Challenges in Transborder Acquisition of Electronic Evidence from "Cloud Computing Providers"*. Council of Europe. [Võrgumaterjal] Leitav: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa3dc [Kasutatud 28.04.2017].

Simons, H., 2009. *Case Study Research in Practice.* London, Thousand Oaks, New Delhi, Singapore: Sage.

Sisekaitseakadeemia, 2013. *Politseiteenistuse eriala õppekava. Kinnitatud nõukogu 22.04.2014 otsusea nr 1.1-6/9*

Siseministeerium, 2013. *Valitsemisala arengukava 2014-2017.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/public/2013_03_01_VAAK_2014-2017_Hetkeolukorra_analuus_POV_9_siseturvalisus_Siseministeerium.pdf [Kasutatud 18.10.2016].

Siseministeerium, 2015. *Siseturvalisuse arengukava 2015-2020.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/sites/default/files/dokumendid/Arengukavad/siseturvalisuse_arengukava_2015-2020_kodulehele.pdf [Kasutatud 20.10.2016].

Spoenle, J., 2010. *Cloud Computing and cybercrime investigations: Territoriality vs. the power of disposal?* Euroopa Liidu Nõukogu. [Võrgumaterjal] Leitav: https://rm.coe.int/16802fa3df [Kasutatud 11.05.2017].

Stranburg, K. J., 2007. Surveillance of emergement associations: Freedom of association in a network society. Rmt: A. Acquisti, A. de Capitani di Vimercati,; S. Gritzalis & C. Lambrinoudakis, toim-d. D*igital privacy: Theory, technologies, and practices.* BocaRaton: Auerbach Publications, pp. 435–459.

Zuboff, S., 2015. Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology* Vol 30, pp 75–89.

Tamme, M.-L., 2016. *Euroopa Liidus justiits- ja siseasjade koostöö rakendusprobleemid.* Magistritöö. Tallinn: Sisekaitseakadeemia.

Teddlie, C. & Yu, F., 2007. Mixed Methods Sampling. A Typology With Examples. *Journal of Mixed Methods Research,* 1(1), pp. 77–100. Leitud: Sage Journals Online. [10.11.2016].

Tehver, J., 2016. *Digitaalsete tõendite kasutamise võimaldamine.* [Võrgumaterjal] Leitav: http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf [Kasutatud 04.05.2017].

Tele2 Sverige AB ja Secretary of State for the Home Department jt. EKo, (2016) C-203/15 ja C-698/15.

The Tor Project, 2016. *Tor Browser.* [Võrgumaterjal]
Leitav: https://www.torproject.org/projects/torbrowser.html.en
[Kasutatud 11.01.2017].

Tikk-Ringas, E., 2012. Küberjulgeoleku õiguslik raamistik. *Juridica,* IV, pp. 274-283.

Turu-uuringute AS, 2016. *Avaliku arvamuse uuring inimõigustest Eestis.* [Võrgumaterjal]
Leitav:http://www.humanrightsestonia.ee/wp/wp-content/uploads/2016/12/AvalikArv_Tulemused.pdf
[Kasutatud 17.12.2016].

Tüür, K., 2001. *Piiriülene koostöö: Eesti - Vene näide*. Bakalaureusetöö. Tartu: Tartu Ülikool.

United Nations, 2011. *Countering the use of the Internet for Terrorist purposes - Legal and Technical Aspects*. New York: CTITF Publication Series.

UNODC, 2011. *Estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes.* Vienna: UNODC.

UNODC, 2013. *Comprehensive Study on Cybercrime.* Vienna: UNODC.

Vabariigi Valitsus, 2011. Vabariigi Valitsuse tegevuskava 2011-2015. [Võrgumaterjal] Leitav: https://www.riigiteataja.ee/aktilisa/3300/4201/3002/VV_25042013_194k_lisa.pdf [Kasutatud 30.03.2017].

Velasco, C.; Hörnle, J.; Osula, A.-M., 2016. Global Views on Internet Jurisdiction and Trans-Border Access. Rmt: S. Gutwirth; R. Leenes; P. De Hert, toim-d. *Data Protection on the Move.* Law, Governance and Technology Series, 24. Netherland: Springer, pp 465-476.

Vernimmen-Van Tiggelen, G. & Surano, L., 2008. *Analysis of the future of mutual recognition*. Brüssel: Université Libre de Bruxelles.

Välisministeerium, 2014. Välisministeeriumi arengukava 2015-2018. [Võrgumaterjal] Leitav: http://www.vm.ee/sites/default/files/content-editors/VM_arengukava_2015-2018.pdf [Kasutatud 03.12.2016].

Wieser ja Bicos Beteiligungen GmGH vs. Austria (2007) EIKo 74336/01.

Wills, A. & Vermeulen, M., 2011. *Parliamentary Oversight of Security and Intelligence Agencies in The European Union.* Brussels: European Parliament.

Wood, D.M., 2006. Beyond the panopticon? Foucault and surveillance studies. Rmt: J. Crampton & S. Elden, toim-d. *Space, knowledge and power: Foucault and geography.* Aldershot: Ashgate, pp. 245–263.

Wright, D. & Kreissl, R., 2015. European responses to the Snowden revelations. Rmt: D. Wright & R. Kreissl, toim-d. *Surveillance in Europe.* London, New York: Routledge, pp. 6–50.

Õiguskantsler, 2015. *Õiguskantsleri aastaülevaade 2014/2015.* [Võrgumaterjal] Leitav: http://oiguskantsler.ee/ylevaade2015/julgeolekuasutused# [Kasutatud 20.05.2016].

Yin, R. K., 2009. *Case Study Research: Design and Methods.* 4 ed. Thousand Oaks, New Dehli, London, Singapore: Sage.

TABELITE JA JOONISTE LOETELU

LISAD

Lisa 1. Ekspertintervjuud küsimustik

Lugupeetud kolleeg!

Pöördun Teie poole seoses käsiloleva magistritööga „Piiriüleste jälitustoimingute läbiviimine digitaalkeskkonnas“. Magistritöös uurin, millised on rahvusvahelise koostöö probleemkohad digitaalkeskkonnas jälitustoimingute läbiviimisel ja kuidas on neid võimalik lahendada. Töö eesmärgiks on välja selgitada digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimise probleemkohad ja esitada uurimispõhiselt rakendusettepanekuid nende lahendamises.

Mõisted:

Millised on digitaalkeskkonnas läbiviidavad jälitustoimingud? Digitaalkeskkonnas on võimalik jälitustoiminguid läbi viia näiteks sidevahendi kaudu edastatavat teavet pealtkuulates või vaadates (telefonivestlused, veebikaamera kaudu jälgimine), internetis liikumist jälgides (IP aadressi kaudu), GPS'i positsioneerimine, *TOR – browser'i* kasutaja tuvastades.

Mis on piiriülene kuritegevus? Käesolevas magistritöös käsitleb autor piiriülest kuritegevust kui illegaalset käitumist, mille tegu, vahend või tagajärg ulatub teise riigi jurisdiktsiooni ning mille tõkestamiseks või avastamiseks on vaja riikidevahelist koostööd.

Töö uurimisprobleem on järgmine: milliseid tõrkeid ja takistusi esineb piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas?

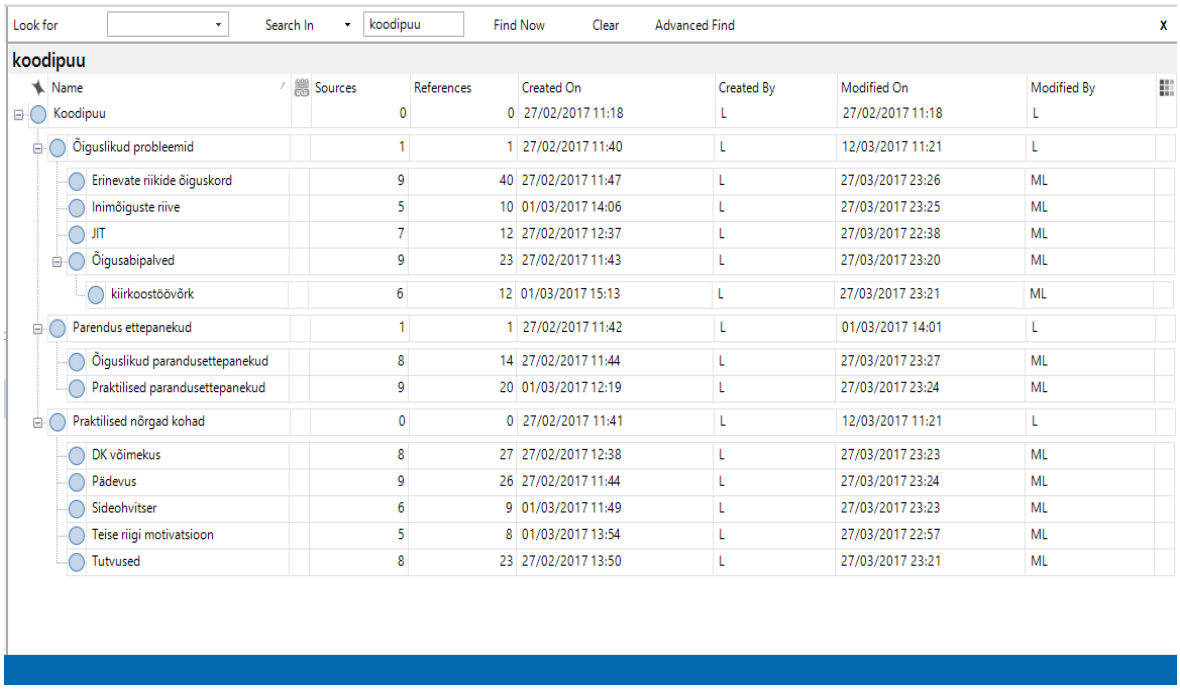
Selleks et leida vastused püstitatud uurimisprobleemile, esitan intervjuu käigus 4 küsimust:

1. *Eksperdi kokkupuude digitaalkeskkonnas läbiviidud piiriüleste jälitustoimingutega.* Kui sageli on tulnud Teil koostööd teha teiste riikidega jälitustoimingute läbiviimisel digitaalkeskkonnas? Selgitage palun, milliste kuritegude puhul ja milliseid jälitustoiminguid olete läbiviinud ja kui kaua on need aega võtnud, kas moodustati JIT?
2. *Eksperdi kogemus probleemide esinemisega:* Milliseid probleeme on esinenud digitaalkeskkonnas piiriüleste jälitustoimingute läbiviimisel digitaalkeskkonnas? Selgitage palun, kuidas on need probleemid menetlust mõjutanud ja kuidas on need lahenenud.
3. *Eksperdi hinnang, õigusabipalvete toimimisele:* Kuidas on Teie kogemuse põhjal mõjutanud rahvusvahelised õigusabipalved menetluse läbiviimist? Mida olete teinud juhul kui

õigusabipalve täitmisest on keeldutud? Milliseid õigusabipalvetele alternatiivseid rahvusvahelise koostöö meetodeid olete kasutanud seoses digitaalkeskkonnas jälitustoimingute läbiviimisega?

4. *Eksperdi soovitus olukorra parendamiseks:* Kuidas Teie hinnangul parendada piiriüleste jälitustoimingute läbiviimist digitaalkeskkonnas?

Lisa 2. NVivo11 koodipuu



Name	Sources	References	Created On	Created By	Modified On	Modified By
Koodipuu	0	0	27/02/2017 11:18	L	27/02/2017 11:18	L
Õiguslikud probleemid	1	1	27/02/2017 11:40	L	12/03/2017 11:21	L
Erinevate riikide õiguskord	9	40	27/02/2017 11:47	L	27/03/2017 23:26	ML
Inimõiguste riive	5	10	01/03/2017 14:06	L	27/03/2017 23:25	ML
JIT	7	12	27/02/2017 12:37	L	27/03/2017 22:38	ML
Õigusabipalved	9	23	27/02/2017 11:43	L	27/03/2017 23:20	ML
kiirkoostöövõrk	6	12	01/03/2017 15:13	L	27/03/2017 23:21	ML
Parendus ettepanekud	1	1	27/02/2017 11:42	L	01/03/2017 14:01	L
Õiguslikud parandusettepanekud	8	14	27/02/2017 11:44	L	27/03/2017 23:27	ML
Praktilised parandusettepanekud	9	20	01/03/2017 12:19	L	27/03/2017 23:24	ML
Praktilised nõrgad kohad	0	0	27/02/2017 11:41	L	12/03/2017 11:21	L
DK võimekus	8	27	27/02/2017 12:38	L	27/03/2017 23:23	ML
Pädevus	9	26	27/02/2017 11:44	L	27/03/2017 23:24	ML
Sideohvitser	6	9	01/03/2017 11:49	L	27/03/2017 23:23	ML
Teise riigi motivatsioon	5	8	01/03/2017 13:54	L	27/03/2017 22:57	ML
Tutvused	8	23	27/02/2017 13:50	L	27/03/2017 23:21	ML