Sisekaitseakadeemia
Politsei- ja piirivalvekolledž

Maarja-Liis Põder

MENETLUSES OSALEJATE POOLT ESITATUD DIGITAALSETE TÕENDITE VORMISTAMINE PÕHJA PREFEKTUURIS

Lõputöö

Juhendaja:
Eneli Laurits, MA
Kaasjuhendaja:
Ardo Ranne, BA

Tallinn 2023

ANNOTATSIOON

Kolledž/instituut: Politsei- ja piirivalvekolledž	Kaitsmise kuu ja aasta: juuni 2023
Töö pealkiri eesti keeles: Menetluses osalejate poolt esitatud digitaalsete tõendite vormistamine Põhja prefektuuris	
Töö pealkiri võõrkeeles: *Formalisation of Digital Evidence Submitted by Persons Participating in the Proceedings in North Prefecture*	
Lõputöö on kirjutatud eesti keeles ning sisaldab ingliskeelset kokkuvõtet. Töö maht on 48 lehekülge. Lõputöös on kasutatud 53 erinevat allikat, millest 27 on eestikeelsed ja 26 on ingliskeelsed. Lõputöös on püstitatud uurimisprobleem: kuidas menetluses osalejate poolt esitatud digitaalseid tõendeid korrektselt ja usaldusväärselt tõendiks vormistada? Uurimisprobleemi täpsustavad kolm uurimisküsimust. Lõputöö eesmärk on välja selgitada menetluses osalejate poolt esitatud digitaalsete tõendite vormistamise põhimõtted ja kitsaskohad ning teha ettepanekuid olukorra parandamiseks. Uurimismeetodina kasutatakse kvalitatiivset empiirilist uuringut, mille käigus viiakse läbi dokumendianalüüs. Lõputöö koosneb kahest peatükist. Töö teoreetilises osas antakse ülevaade digitaalsete tõendite olemusest ning digitaalsete tõendite vormistamise teoreetilistest lähtekohtadest. Samuti tuuakse välja digitaalsete tõenditega seonduvad õiguslikud probleemid. Töö empiirilises osas analüüsitakse Põhja prefektuuri menetluses olnud KarS § 157^3 kriminaalasjade toimikuid, et selgitada välja digitaalsete tõendite vormistamisel esinevad probleemid. Teooria ja empiirilise uuringu tulemuste alusel tehakse järeldusi ja ettepanekuid menetluspraktika ühtlustamiseks. Töö tulemuste põhjal tehti kokku kolm ettepanekut.	
Lisad:	
Võtmesõnad: digitaalne tõend, digitaalkriminalistika, vaatlusprotokoll, menetlusosalised, menetluses osalejad, jälgitavuse ahel	
Võõrkeelsed võtmesõnad: *digital evidence, digital forensics, report of an inspection, parties to proceedings, persons participating in the proceedings, chain of custody*	
Säilitamise koht: SKA raamatukogu	
Töö autor: Maarja-Liis Põder	
Olen koostanud lõputöö iseseisvalt. Kõik lõputöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma lõputöö avaldamisega elektroonilises keskkonnas.	
Allkiri:	Kommentaar (soovi korral)
Vastab lõputöö nõuetele	
Juhendaja:	Allkiri:
Kaasjuhendaja:	Allkiri:
Kaitsmisele lubatud	
Kolledži direktor/instituudi juhataja:	Allkiri:

SISUKORD

SISSEJUHATUS

Lõputöös uuritakse menetluses osalejate poolt esitatud digitaalsete tõendite vormistamise protsessi ja sellega seonduvaid probleeme. Aastal 2022 lahendas Riigikohtu kriminaalkolleegium kassatsiooni korras vaidluse, mille käigus käsitleti ligipääsu digitaalsetele andmekandjatele. Riigikohtu kriminaalkolleegiumi otsusega tunnistati lubamatuks selle kriminaalmenetluse käigus koostatud digitaalsete andmekandjate vaatlusprotokollid (Kriminaalasi K. K. süüdistuses KarS § 184 lg 2^1 ja M. R-i süüdistuses KarS § 184 lg 2 p-de 1 ja 2 järgi, 2022) Antud kohtulahend on üks näide sellest, kuidas digitaalsete tõenditega seonduv tekitab segaseid olukordi ka kogenud praktiku seas.

Teema on **aktuaalne**, sest digitaalsete tõendite kogumine ja usaldusväärsus on tekitanud aastaid küsimusi ning ebaselge on seegi, kas traditsiooniline õigusharidus on piisav, et mõista digitaalsete tõenditega seotud detaile (Laurits, 2015, lk 135). Teema olulist rõhutab muuhulgas asjaolu, et kriminaalmenetlus tugineb üha enam digitaalsetele tõenditele (Euroopa Komisjon, 2019, p. 1). „Siseturvalisuse arengukava 2020–2030“ kohaselt vajab digi- ja infoajastu keskkond uudset lähenemist, sest praegused lahendused on piiratud või puudulikud. Arengukava üks eesmärk on luua õiguskaitseasutustele paremad eeldused ja arendada menetlusahela võimekust ning selleks on tarvis arendada digitaalkriminalistika teenust. (Siseministeerium, 2021, lk 31–32, 39) Samuti rõhutab Euroopa Liidu raske ja organiseeritud kuritegevuse põhjustatud ohtude hinnang, et järgmise viie aasta jooksul toimub veelgi intensiivsem digitaliseerumine, mis mõjutab nii kuritegevust kui ka kuritegude uurimist (Europol, 2021, p. 92).

Lisaks on teema problemaatikale viidanud kriminaalmenetlusõiguse revisjoni töörühma liige, kelle analüüsist nähtub, et praegusel juhul kohaldatakse digitaalsete tõendite kogumisel, käitlemisel, uurimisel ja esitamisel selliseid norme, mis on tegelikult kriminaalmenetluse seadustikus mõeldud teiste tõendiliikide reguleerimiseks (Tehver, 2016, lk 2). Tegemist on üsna laiaulatusliku probleemiga, sest statistika kohaselt on 85% kriminaalmenetlustest sellised, kus kasutatakse digitaalseid tõendeid (Euroopa Komisjon, 2019, p. 1). Kuivõrd ei ole digitaalsete tõendite jaoks vaja tingimata luua eriregulatsiooni, siis oleks sellegipoolest oluline teha seaduses täiendusi ja muudatusi, et praktikas esinevaid vastuolusid ja lünkasid kõrvaldada (Prokuratuur, 2017, lk 4).

Lõputöö on **uudne**, sest varasemalt pole menetluses osalejate poolt esitatud digitaalsete tõendite vormistamisega seotud uuringut läbi viidud. Sarnasel teemal on kirjutatud üks lõputöö ja kaks magistritööd. Alas (2013) käsitles oma lõputöös digitaalsete tõendite kogumist internetis toimepandud autoriõiguste menetlemisel. Raudsepp (2018) analüüsis magistritöös, kas kehtiv seadus võimaldab kriminaalmenetluses digitaalseid tõendeid kasutada ning kas selle puhul esineb olulisi puudusi. Luuk (2017) uuris oma magistritöö käigus, kuivõrd vajalik oleks digitaalsete tõendite kogumise ja kasutamise osas kehtestada eriregulatsioon. Käesolevas lõputöös keskendutakse aga menetluses osalejate poolt esitatud digitaalsete tõendite korrektse vormistamise põhimõtetele ning sellega seonduvatele probleemidele.

Siseriiklikul tasandil viis uurimisinstituut RAND Europe Siseministeeriumi tellimusel läbi uuringu, mille eesmärk oli analüüsida tulevikutehnoloogiaid ja nende mõju küberkuritegevusele. Ehkki uuringu põhifookus oli seotud tehnoloogia ja küberkuritegevusega, tõid uuringu koostajad eraldi välja, et järgmise kümnendi jooksul mõjutavad küberkuritegude lahendamist ka kriminaalõiguse ja kriminaalmenetlusega seotud probleemid. Uuringust tulenevalt tehti Eestile ettepanek arendada ja muuta õiguslikku süsteemi, et tagada võimekus tegeleda küberkuritegevusest tulenevate probleemide lahendamisega. (Bellasio, *et al*., 2020, p. 8–9) Rahvusvahelises vaates saab välja tuua Buzarovska Lazetiku ja Koshevaliska (2013) läbi viidud uuringu, mille üks eesmärk oli anda ülevaade digitaalsete tõendite käitlemisest Makedoonias. Uuringu tulemuste põhjal tehti ettepanek täiendada riigi kriminaalmenetluse seadustikku ning määratleda digitaalse tõendi mõiste ja digitaalsete tõendite kogumise, käitlemise ja säilitamise kord.

Tänapäeval on enamikel kuritegudel digitaalne dimensioon (Casey, 2011, p. 16). Uued tehnoloogilised lahendused soodustavad inimeste sotsiaal- ja majanduselu ümberasumist internetti, mistõttu tuleks digitaalseid tõendeid otsida ja kasutada peaaegu iga kuriteo puhul (Tartu Ülikool, 2013, lk 132). Ehkki digitaalsed tõendid erinevad oma olemuselt esemelistest tõenditest, siis kehtiv õigus nende tarbeks eraldi menetluskorda ei kehtesta – mõistagi tekitab see praktikas segaseid olukordi (Justiitsministeerium, 2015, lk 9). Eelnevast lähtuvalt on oluline leida vastus **uurimisprobleemile**, kuidas menetluses osalejate poolt esitatud digitaalseid tõendeid korrektselt ja usaldusväärselt vormistada?

Uurimisprobleemi täpsustavad kolm **uurimisküsimust**:

1. Mis on digitaalne tõend?
2. Kuidas menetluses osalejad digitaalseid tõendeid esitavad?
3. Millised puudused esinevad digitaalsete tõendite vormistamisel?

Lõputöö **eesmärk** on välja selgitada menetluses osalejate poolt esitatud digitaalsete tõendite vormistamise põhimõtted ja kitsaskohad ning teha ettepanekuid olukorra parandamiseks.

Lõputöö eesmärgi saavutamiseks on püstitatud järgnevad **uurimisülesanded**:

1. Analüüsida digitaalse tõendi olemuse ja vormistamise teoreetilisi lähtekohti ning õiguslikke probleeme.
2. Analüüsida Põhja prefektuuri menetluses olnud KarS § 157^3 kriminaalasjade toimikuid, selgitamaks välja digitaalsete tõendite vormistamisel esinevad probleemid.
3. Teha teooria ja uuringu tulemuste alusel järeldusi ja ettepanekuid menetluspraktika ühtlustamiseks.

Lõputöö eesmärgi täitmiseks viiakse läbi kvalitatiivne empiiriline uuring (Hirsjärvi, *et al*., 2004, lk 151). Andmekogumismeetodina kasutatakse dokumendianalüüsi (Laherand, 2008, lk 258). Dokumendianalüüsi positiivse küljena saab välja tuua selle tõhususe ja täpsuse – võrreldes mõne teise andmekogumismeetodiga on see vähem aeganõudev ning hõlmab endas andmete kogumise asemel andmete valimist (Bowen, 2009, p. 31).

Uuringu valimiks on ettekavatsetud valim, mille puhul võetakse uuritavad objektid valimisse eesmärgist lähtuvalt kindlate kriteeriumite alusel (Õunapuu, 2012). Valimiks on Põhja prefektuuri erinevate allüksuste menetluses olnud karistusseadustiku (KarS) § 157^3 kriminaalasjade toimikud, mis said 2021. aastal kohtus lahendi. Toimikutes analüüsitakse menetluses osalejate poolt esitatud digitaalseid tõendeid. Menetluses osalejad on käesoleva töö kontekstis tunnistaja ja menetlusosalised. Kriminaalmenetluse seadustiku (KrMS) § 16 lg 2 kohaselt on menetlusosalised kahtlustatav, süüdistatav ning nende kaitsjad, kannatanu, tsiviilkostja ja kolmas isik (Kriminaalmenetluse seadustik, 2003). Kriminaaltoimikute analüüs annab kõige asjakohasemase ülevaate sellest, mil moel digitaalseid tõendeid vormistatakse ning millised probleemid sellega seoses esinevad. Andmeanalüüsimeetodina rakendatakse kvalitatiivset sisuanalüüsi (Kalmus, *et*

al., 2015), mille raames analüüsitakse kriminaaltoimikutes olevaid tõendeid ning moodustatakse kategooriad ja koodid.

Töö koosneb kahest peatükist. Esimeses peatükis antakse teoreetiline ülevaade digitaalsete tõendite olemusest, definitsioonidest ning selle valdkonna rahvusvahelistest uuringutest. Samuti tuuakse välja digitaalsete tõendite vormistamise nõuded ja võimalikud õiguslikud probleemid. Töö teises peatükis kirjeldatakse empiirilise uuringu metoodikat, analüüsitakse kriminaaltoimikutes olevaid tõendeid, et selgitada välja, millised probleemid esinevad digitaalsete tõendite vormistamisel, ning tehakse uuringu tulemuste põhjal järeldusi ja ettepanekuid.

1. TEOREETILISED LÄHTEKOHAD

Lõputöö esimeses peatükis antakse teoreetilistele allikatele tuginedes ülevaade digitaalsete tõendite olemusest, omadustest ja eripärast. Samuti tuuakse teoreetiliste lähtekohtade raames välja see, kuidas mõista digitaalseid tõendeid Eesti kriminaalmenetluse seadustiku ja Riigikohtu praktika kontekstis, kuidas võiks digitaalseid tõendeid vormistada ning millised on sealjuures võimalikud probleemid. Ehkki Eesti õiguses ei ole eraldi välja toodud digitaalse tõendi legaaldefinitsiooni või käsitletud digitaalset tõendit eraldi tõendiliigina, siis kasutatakse seda mõistet laialdaselt nii praktikute seas kui ka rahvusvahelises teaduskirjanduses. Töö omaette eesmärk ei ole põhjalikult analüüsida terminoloogiaga seonduvat ning sellest tulenevalt kasutatakse käesolevas töös üheselt mõistet digitaalne tõend.

1.1. Digitaalse tõendi olemus ja definitsioon

Käesolevas alapeatükis antakse ülevaade digitaalsete tõendite olemusest. Sellega seonduvalt tuuakse välja digitaalkriminalistika mõiste, digitaalse tõendi definitsioon ning selle võimalikud allikad ja omadused, mis on olulised, et mõista digitaalsete tõendite vormistamisega seonduvat.

Tänapäeval on digitaalsed seadmed praktiliselt kõikjal (Hsieh, 2023, p. 8), mistõttu on digitaalsetest tõenditest saanud mahukas ja oluline osa erinevates menetlustes. Enamik kuritegusid on ühel või teisel viisil arvutisüsteemidega seotud – arvutiandmed ja-süsteemid võivad olla nii kuriteo objektiks kui ka kuriteo toimepanemise vahendiks. Samas on kuritegusid, mille toimepanemine pole iseenesest kuidagi arvutisüsteemidega seotud, kuid mille puhul asuvad olulised tõendid just arvutis. (Laurits & Kasper, 2016, p. 197) Teisisõnu on digitaalne maailm üheaegselt kuritegevuse toimumise koht, kuritegude toimepanemise vahend ning kuritegude sihtmärk (Savona & Mignone, 2004, pp. 6–10).

Arvestades asjaolu, et ühiskond sõltub suuresti infotehnoloogiast, on loogiline, et digitaalkriminalistika tähtsus on viimaste aastate jooksul üha kasvanud (Valjarevic & Venter, 2015, p. 339). Digitaalkriminalistika mõistet ei ole üheselt määratletud, samuti pole jõutud üksmeelele selles osas, kuidas digitaalkriminalistikat liigitada. Seetõttu on mõistlik digitaalkriminalistika olemuse kirjeldamisel lähtuda selle peamistest eesmärkidest ja ülesannetest.

Digitaalkriminalistika eesmärk on hankida digitaalseid tõendeid ning neid analüüsida, et saada vastused järgmistele küsimustele: miks, millal, kus, mida, kes (Lopez, *et al*., 2016 p. 2). Digitaalkriminalistika põhiülesanded on seotud erinevatest allikatest saadud digitaalsete tõendite kogumise, säilitamise, tuvastamise, uurimise, analüüsimise, tõlgendamise ja dokumenteerimisega, samuti nende esitamisega kohtus (Olber, 2021, p. 160). Selleks, et digitaalsed tõendid oleksid usaldusväärsed ja neid saaks kasutada, on oluline rakendada teaduslikku lähenemist – seetõttu võib öelda, et digitaalkriminalistika eesmärk on teaduslike meetodite abil tagada digitaalsete tõendite lubatavus süüteomenetluses (Lall, *et al*., 2021, p. 141). Sobilike digitaalkriminalistika meetodite ja tehnikate valik ning teaduslik lähenemine on usaldusväärsuse tagamisel kahtlemata vajalik.

Digitaalne tõend on igasugune digitaalsel kujul loodud, töödeldud, salvestatud või edastatud teave, mida saab kasutada kohtus tõendamiseseme asjaolude selgitamisel. Samuti on digitaalseks tõendiks koopia, mis on tehtud originaalsest digitaalsest teabest. (Buzarovska Lazetik & Koshevaliska, 2013, p. 66) Digitaalne teave omakorda on mistahes andmed, olenemata vormist ja omadustest, mis sisalduvad ja mida töödeldakse info- ja telekommunikatsiooniseadmetes, -süsteemides ja -võrkudes (Ühinenud Rahvaste Organisatsiooni Peaassamblee, 2022, p. 22). Seega on digitaalne tõend ja digitaalne teave küllaltki sarnase sisuga mõisted. Teabest saab tõend, kui seda on võimalik konkreetses kriminaalasjas tõendamise eesmärgil kasutada.

Võimalikud digitaalsete tõendite allikad on andmekandjad ja digitaalsed seadmed, nagu näiteks mobiiltelefonid, tahvelarvutid, digitaalkellad, GPS seadmed, mängukonsoolid, iPod/MP3 mängijad, mälukaardid, biomeetrilised skännerid, automaatvastajad, digitaalkaamerad, kiipkaardid, modemid, ruuterid, serverid, DVD ja CD kettad, flopikettad, printerid, skännerid, mobiiltelefonid, koopiamasinad, krediitkaartide skimmerid, arvuti riistvara komponendid jpm. Seega võib digitaalseid tõendeid leida sisuliselt igalt poolt. (Hsieh, 2023, pp. 9–10) Olulised digitaalsed tõendid võivad olla erinevad dokumendid, e-kirjad, külastuslogid, internetiportaalide postitused, viirusetõrje logid, internetis tehtud toimingute logid, telefoni logid jne (Buzarovska Lazetik & Koshevaliska, 2013, pp. 67–69).

Nii nagu iga füüsilises maailmas toimepandud kuritegu jätab erinevaid jälgi ja tõendeid (sõrme- ja jalatsijäljed, DNA, tunnistajad), jääb ka digitaalses maailmas toimepandud

kuriteost (digitaalseid) jälgi, mille abil kurjategijat otsida ning mida tõendina kasutada (Tara & Mishra, 2021, p. 97). Erinevalt teistest tõendi vormidest saab digitaalseid tõendeid luua hetkega, üksnes mõne klahvivajutusega või ilma inimese vahetu sisendita. Digitaalsetest tõenditest saab informatsiooni, mis ei pruugi olla muul viisil kättesaadav – näiteks metaandmetes olev teave. (Buzarovska Lazetik & Koshevaliska, 2013, p. 64)

Metaandmed on andmed, mis kirjeldavad andmeid ning mis kajastavad kogu faili töötlemise ja kasutamisega seonduvat teavet, mis on omakorda vajalik selleks, et tuvastada ja tõendada teabe mahtu, autentsust ja terviklikkust (Krotoski, 2011, p. 52). Metaandmed näitavad faili nime, faili asukohta (nt kataloogistruktuuris), failivormingut või failitüüpi, faili suurust, kuupäevi (nt loomise kuupäev, viimatise muutmise kuupäev, viimane metaandmete muudatus) jne (Hannon, 2014, p. 318). Seega digitaalsete tõendite eripära ja väärtus seisnebki tihti metaandmetes, millest saab informatsiooni, mida mujalt ei pruugi saada.

Digitaalsetel tõenditel on erinevaid omadusi, mille tõttu võib nende käitlemine ja haldamine olla tunduvalt keerulisem kui esemeliste tõendite puhul (Prayudi & SN, 2015, p. 2). Esiteks, digitaalsed tõendid on **latentsed** ehk peidetud, nagu sõrmejäljed või DNA (Hshieh, 2023, p. 8). Latentsus seisneb selles, et digitaalsed tõendid on inimese meeltele tajumatud ning neid ei ole võimalik tuvastada näiteks andmekandja välisel uurimisel (Lall, *et al*., 2021, p. 142). Selleks, et taolist tõendit leida, on tarvis eriteadmisi ja eritehnikat.

Teiseks, digitaalsed tõendid on **haprad** – neid on väga lihtne muuta, kahjustada, hävitada või uute andmetega saastada (Hshieh, 2023, p. 8). Näiteks seadmes olevad andmed võivad muutuda või kahjustuda ainuüksi toite väljalülitamisel (Lopez, *et al*., 2016, p. 11). Digitaalsete tõendite haprus väljendub eelkõige juhul, kui tõendite kogumiseks kasutatakse valesid võtteid või kui seadme omanik üritab seadmes olevaid andmeid pahatahtlikul eesmärgil muuta või hävitada. Kolmandaks, digitaalsed tõendid on **volatiilsed** ehk püsimatud – isegi juhul, kui andmed näiliselt salvestatakse turvaliselt kõvakettale, siis võivad need hävineda (Lall, *et al*., 2021, p. 142).

Neljandaks iseloomustab digitaalsed tõendeid **asukoha määramatus**, sest need suudavad kiiresti ja lihtsalt ületada erinevate jurisdiktsioonide piire (Hshieh, 2023, p. 8). Kuna digitaalsete tõendite liikumine ei ole piiratud geograafiliste piiridega, siis muudab see

nendeni jõudmise mõnevõrra keerulisemaks. Vajalike andmete saamisel võib esineda viivitusi ning see omakorda võib viia tõendite hävimiseni (Lall, *et al*., 2021, p. 142), sest andmeid säilitatakse ainult teatud aja jooksul. Eeltoodust nähtub omakorda digitaalsete tõendite **ajakriitilisus** (Hshieh, 2023, p. 8).

Lisaks iseloomustab digitaalseid tõendeid **suur andmemaht** – üha enam suureneb andmekandjate hulk, mis on uurimisasutuste poolt ära võetud, ning sellega seoses suureneb ka digitaalsete tõendite analüüsimiseks kuluv aeg. Samuti kasvab nende andmete maht, mida on tarvis menetluste raames säilitada. (Lall, *et al*., 2021, p. 142) Mõistagi on vaja tagada piisav salvestusruum ning turvaline keskkond andmetele.

Digitaalsete tõendite käitlemist saab pidada küllaltki **keerukaks** – arvutisüsteemid muutuvad kogu aeg komplitseeritumaks ning pilveteenuste ja muude rakenduste iseloomust lähtuvalt on tarvis pidevalt uusi teadmisi, et tõendeid koguda. Muuhulgas on digitaalsete tõendite käitlemine üsna **aeganõudev** protsess, mis tuleneb osaliselt üha kasvavast andmemahust, kuid ka nn uurimistõrje (ingl k *anti forensics*) võtete kasutamisest, mis muudab andmete analüüsimise keeruliseks ja segaseks. (Lall, *et al*., 2021, p. 142)

Alapeatüki kokkuvõtteks võib järeldada, et digitaalsed tõendid on tänapäeva menetlustes olulisel kohal ning neid võib leida peaaegu kõikjalt olenemata kuriteo iseloomust. Digitaalsed tõendid on oma olemuselt latentsed, haprad ja volatiilsed ning neid iseloomustab ajakriitilisus, suur andmemaht, suur ajakulu, keerukus ning võime ületada erinevate jurisdiktsioonide piire. Seega on digitaalsed tõendid võrreldes esemeliste tõenditega nii mõneski osas keerulisemad, kuid nende olemuse mõistmine on oluline, et tagada vajalikud teadmised nende käitlemiseks. Sealjuures on oluline, et digitaalkriminalistikas kasutataks teaduslikku lähenemist.

1.2. Digitaalsete tõendite õiguslik käsitlus ja selle puudused

Käesolevas alapeatükis tuuakse välja võimalikud probleemid, mis seoses digitaalsete tõenditega esinevad. Sellest tulenevalt analüüsitakse, kuidas mõista digitaalseid tõendeid Eesti õigusruumis, ning antakse ülevaade foto, filmi või muu teabetalletuse, asitõendi ning dokumendi kui tõendivormide olemusest, et mõista digitaalsete tõendite

vormistamisega seonduvaid kitsaskohti. Lisaks antakse ülevaade piiriülesest andmevahetusest ning sellega seonduvatest probleemidest.

Arvutitehnoloogia areng on olnud kiire ning sellega seoses on riikidel tekkinud vajadus seaduste muutmiseks, et tagada võimekus küberkuritegevuse vastu võitlemiseks ja kriminaalõigusega seotud küsimustega toime tulemiseks (Buzarovska Lazetik & Koshevaliska, 2013, p. 63). Üha rohkem tuleb kriminaalmenetluse raames arvestada interneti, tehnoloogiate ning digitaalselt salvestatud või edastatud andmete eripäraga (Osula, 2017, lk 559). Selleks, et õiguslikku regulatsiooni arendada, on mõistagi vaja erinevad kitsaskohad välja selgitada.

Võib väita, et arvutitehnoloogia ja küberkuritegevuse valdkonnaga seotud rahvusvahelis-õiguslik regulatsioon ebapiisav, sest ainus asjakohane taoline dokument on Euroopa Nõukogu poolt vastu võetud arvutikuritegevusvastane konventsioon (Kergandberg, 2013, lk 255). Arvutikuritegevusvastane konventsioon (ingl k *Convention on Cybercrime*) võeti vastu 2001. aastal. Eesti ratifitseeris konventsiooni 2003. aastal. Arvutikuritegevusvastase konventsiooni artikkel 14 kohaselt peaks liikmesriik (sh Eesti) võtma vastu seadusandlikke ja muid meetmeid, et kehtestada eeluurimise ja menetluse kord konventsioonis nimetatud kuritegude suhtes ning anda menetlemiseks vajalikud volitused; muuhulgas peaks kehtestama digitaalsete tõendite kogumise korra (Riigikogu, 2001). Sellegipoolest ei ole Eesti kriminaalmenetluse seadustikus digitaalsete tõendite kogumise korda või muud sellega seonduvat kehtestatud.

Oluline on välja tuua, et kriminaalmenetluse seadustikus ei ole välja toodud digitaalse tõendi definitsiooni. Muuhulgas ei ole seadusandja esitanud ka tõendi enda legaaldefinitsiooni, vaid on piirdunud lubatavate tõendivormide loeteluga (Kergandberg & Pikamäe, 2012, lk 217). Seega tekib küsimus, kas ja kuidas digitaalseid tõendeid tõendamiseseme asjaolude tuvastamisel kasutada saab. KrMS § 63 lg 1 kohaselt saab tõendiks olla kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või muu dokument või foto või film või muu teabetalletus (Kriminaalmenetluse seadustik, 2003). Seega on seaduses välja toodud konkreetsed tõendivormid, mida on võimalik kriminaalmenetluses tõendamisel kasutada.

Lisaks on KrMS § 63 lg-s 2 sätestatud, et kriminaalmenetluse asjaolude tõendamiseks võib kasutada ka eelpool loetlemata tõendeid, välja arvatud juhul, kui tegemist on kuriteo või põhiõiguse rikkumise teel saadud tõendiga (Kriminaalmenetluse seadustik, 2003). Küll aga tuleneb Riigikohtu kriminaalkolleegiumi otsusest nr 3-1-1-142-05, et KrMS § 63 lg-s 1 loetlemata tõenditele on võimalik tugineda üksnes menetlusliku sisuga asjaolude (nt menetlustähtaja järgimise) tõendamiseks (Kriminaalasi L. H. süüdistuses KarS § 118 p-de 1, 2 ja 3 järgi). Seega tasub silmas pidada, et olenemata KrMS § 63 lg-s 2 välja toodust tuleb kriminaalmenetluses tõendamiseseme asjaolude tuvastamisel piirduda üksnes KrMS § 63 lg-s 1 loetletud tõendivormidega.

Ehkki eeltoodust nähtub, et Eesti kriminaalmenetluse seadustik digitaalsete tõendite tarbeks erisätteid välja ei too, siis ei ole sellegipoolest välistatud digitaalsete tõendite kasutamine tõendamiseseme asjaolude tuvastamisel, sest KrMS § 63 lg-s 1 loetletud tõendiliigid on küllaltki üldised ning hõlmavad seetõttu enamikku digitaalsetest tõenditest. Segadust tekitab siiski küsimus, kuidas kvalifitseerida erinevaid digitaalseid tõendeid eelpool nimetatud tõendi liikide alla, sest ei ole üheselt arusaadav, millisel juhul liigituvad digitaalsed andmed ja andmekandjad asitõendiks, dokumendiks või teabetalletuseks. Segadus tõendi liikide kohaldamisel tekitab omakorda olukorra, kus pole selge, milliseid nõudeid on vaja järgida tõendi vormistamisel. (Tehver, 2016, lk 2, 5) Ühest küljest võib võrdlemisi vähene konkreetsus ja legaadefinitsioonide puudumine anda tõendamisel rohkem võimalusi ja vabadust, kuid teisalt võib tekitada segadust ja ebamäärasust.

Üldiselt võib digitaalseid tõendeid ka Eesti õigusruumis mõista kui digitaalsel kujul olevaid andmeid (digitaalset teavet), mida saab liigitada KrMS § 63 lg-s 1 loetletud tõendivormide alla ning mida saab kasutada KrMS §-s 62 sätestatud tõendamiseseme asjaolude selgitamiseks. Tõendite korrektse vormistamise tagamiseks on siiski oluline mõista, millise tõendivormi alla konkreetset digitaalset tõendit liigitada. Siinkohal on oluline välja tuua erinevate tõendivormide (foto, film või teabetalletus, asitõend ja dokument) olemus.

KrMS § 63 lg 1 kohaselt saab foto, film või muu teabetalletus olla iseseisvaks tõendiliigiks. Riigikohtu praktika kohaselt on see siiski võimalik vaid teatud juhul. Tegemist peab olema uurimistoimingu käigus tehtud ning toimingu käiku ja tulemusi kajastava salvestisega (teabetalletusega), mis vormistatakse protokolli lisana ning mille

seos kriminaalasjaga nähtub protokolli tekstist. Selline salvestis on iseseisev tõend juhul, kui ilmneb vastuolu protokollis ja salvestises kajastatu vahel – siis käsitab kohus nii protokolli kui ka sellele lisatud salvestist iseseisvate tõenditena. (Olle Koki (Kokk) kriminaalasi süüdistuses KarS § 141 lg 1 järgi, 2009) Ehk siis – kui kannatanu ülekuulamine viiakse läbi videoülekuulamise vormis, siis on tõendiks kannatanu ülekuulamise protokoll, mille juurde on vormistud lisana videosalvestis ülekuulamisest. Kui esineb vastuolu protokollis kajastatu ja salvestises kajastatu vahel, siis on kohus õigustatud käsitama nii protokolli kui salvestist iseseisvate tõenditena.

Riigikohus on muuhulgas välja toonud, et võib esineda olukordi, kus menetlejad võtavad tõendite kogumisel isikutelt ära varem saadud salvestisi või kus isikud annavad menetlejatele selliseid salvestisi üle omal initsiatiivil. Kõik sellised salvestised peaksid sõltuvalt nende sisust olema käsitatavad kas asitõenditena või dokumentidena ning ka vormistatud vastavalt. Mistahes muudel salvestistel ei ole kriminaalmenetluses mingit tõenduslikku tähendust. (Olle Koki (Kokk) kriminaalasi süüdistuses KarS § 141 lg 1 järgi, 2009) See tähendab, et näiteks kannatanu poolt üle antud fotosid või salvestisi tuleks (sõltuvalt sisust) vormistada kas asitõendi või dokumendi vormistamise nõuetest lähtuvalt.

Asitõend on KrMS § 124 lg 1 kohaselt kuriteo objektiks olnud asi, kuriteo toimepanemise vahend, kuriteojäljest valmistatud jäljend või tõmmis või sündmusega seotud muu asendamatu objekt, mida saab kasutada tõendamiseseme asjaolude selgitamisel (Kriminaalmenetluse seadustik, 2003). Kusjuures on oluline märkida, et menetluslikus mõttes saab kuriteoga oletatavasti seotud esemest asitõend alles siis, kui seda on üksikasjalikult kirjeldatud asitõendi vaatlusprotokollis või asitõendi leidmist/saamist kajastavas uurimistoimingu protokollis (Kergandberg & Pikamäe, 2012, lk 218). KrMS § 124 lg 2 sätestab samuti, et juhul, kui asitõendina kasutatavat objekti pole uurimistoimingu protokollis tõendamiseks vajaliku üksikasjalikkusega kirjeldatud, siis tuleb selle tunnuste talletamiseks teha vaatlus (Kriminaalmenetluse seadustik, 2003).

Kurm (2016, lk 8–9) on välja toonud, et väljaspool menetlustoiminguid tekkinud foto, filmi või teabetalletuse käsitamine asitõendina võib olla problemaatiline, sest sisuliselt tähendab see vaatlemist või vajaliku üksikasjalikkusega kirjeldamist, mille käigus tuleb fotot, filmi või teabetalletust paberil ümber jutustada. Lisaks on Kurm välja toonud, et selliselt vaatlemine on üsna töömahukas ning samas võib kahandada tõendi väärtust, sest

ümberjutus on vaatleja tõlgendus. Kurmi ettepaneku kohaselt võiks teabetalletuste puhul lähtuda sellest, et need on iseseisvad tõendid ning ei vaja eraldi vormistust, sealjuures on aga oluline, et oleks näidatud teabetalletuse päritolu ehk millal ja kuidas see on saadud.

Eelpool mainitut arvesse võttes nõustub autor sellega, et digitaalseid tõendeid ei peaks eraldi ümber jutustama, kui visuaalselt ja/või audiaalselt on võimalik neid tajuda. Autori hinnangul peaks digitaalsete tõendite puhul olema põhirõhk sellel, kuidas tõend kriminaalasja juurde jõudis, mida sellega tehti ning millised on näiteks tõendile väärtust ja usaldusväärsust lisavad metaandmed. Ehkki tõendi sisu ümberjutustamine ei pruugi olla mõistlik, siis vähemalt tõendi jälgitavuse ja metaandmete kajastamiseks oleks asjakohane kasutada protokolli või muud dokumenti. Seega on küll oluline, et digitaalsete tõendite vormistamine oleks võimalikult optimaalne, kuid tõendi esitamisel kohtus tuleb tagada, et tõendi sisu, jälgitavus ja muud olulised andmed oleksid esitatud võimalikult arusaadavalt ja usaldusväärselt.

Dokumendi kohta sätestab KrMS § 123, et tõendamisel võib kasutada dokumenti, mis sisaldab teavet tõendamiseseme asjaolude kohta (Kriminaalmenetluse seadustik, 2003). Dokumendi kvaliteet on ka originaaldokumendi koopial ja ärakirjal, mis sisaldavad teavet tõendamiseseme asjaolude kohta. Dokument on kõikvõimalik materiaalne ese, millele on erinevaid märgisüsteeme kasutades kantud mõtestatud teavet ning mis sisaldab teavet tõendamiseseme asjaolude kohta, kuid mis ei ole käsitatav uurimistoimingu, kohtuistungi või jälitustoimingu protokollina. (Kergandberg & Pikamäe, 2012, lk 332–333) See tähendab, et oluline on eristada dokumenti uurimistoimingu protokollidest – näiteks kannatanu ülekuulamise protokoll ei ole dokument KrMS § 63 lg 1 tähenduses.

Dokumendi vormistamist tõendina ei ole seaduses täpsemalt reguleeritud ning sellised dokumendid, millel asitõendi tunnuseid ei ole, köidetakse eeluurimispraktika kohaselt lihtsalt kriminaaltoimikusse (Kergandberg & Pikamäe, 2012, lk 334). Seadus ei kohusta dokumente vaatlema, refereerima või muul viisil sekundaarselt jäädvustama (Kurm, 2016, lk 7). Kusjuures digitaalsete tõendite seisukohast on oluline, et Eesti kohtupraktikas aktsepteeritakse näiteks e-kirjade väljatrükke dokumendina (Kergandberg & Pikamäe, 2012, lk 333).

Seega ei ole dokumentide puhul eraldi vormistamist vaja, mis lihtsustab nende kasutamist tõendina. Küll aga peab sealjuures arvestama võimalike usaldusväärsuse küsimustega,

mis võivad tekkida seoses pelgalt paberkandjale välja trükitud e-kirjaga, kust ei nähtu, kes, millal, kust ja kellele kirja saatis. Riigikohtu kriminaalkolleegium on oma otsuses nr 3-1-1-104-05 välja toonud, et nende küsimuste puhul tuleks pöörduda selliseid andmeid kajastavate andmekandjate poole – e-kirjadel on olemas päis, mille järgi on võimalik kirja identifitseerida, samuti tuleks kirja liikumist kontrollida arvuti IP-aadresside abil (Kriminaalasi T. T. süüdistuses KarS § 266 lg 1, § 257 ja § 323 järgi). Seega võib kohus küll aktsepteerida e-kirjade väljatrükke dokumendina, kuid tõendi esitaja peab suutma näidata tõendi usaldusväärsust, mistõttu on mõistlik juba algselt välja tuua usaldusväärsuse tagamiseks vajalikud andmed.

Digitaalsete tõendite puhul on muuhulgas oluline ka koopiate tegemine. Kopeerimisprotsessist ja selle olulisusest antakse täpsem ülevaade kolmandas alapeatükis, kuid etteruttavalt võib välja tuua, et õiguslikult on tõendusväärtusliku koopia loomine reguleerimata. Tehver (2016, lk 2) on välja toonud, et kopeerimisprotsessi käsitletakse enamasti vaatlusena ning vormistatakse vaatlusprotokolliga, kuid tegelikult ei vasta kopeerimise toimingu sisu ega eesmärk vaatlusele kui seaduses sätestatud toimingule. Seega ei ole probleem ainult selles, kuidas digitaalseid tõendeid olemasolevate tõendivormide alla paigutada, vaid ka selles, kuidas mõista praeguse kehtiva seaduse raames muid toiminguid (nt koopiate tegemine), mis digitaalsete tõenditega seonduvad.

Paljudes kriminaalmenetlustes on digitaalsed tõendid määrava tähtsusega, eriti juhul, kui kuriteo iseloomust lähtuvalt on põhiline tõendamiseks vajalik informatsioon digitaalsel kujul. Keeruline olukord võib tekkida siis, kui kurjategija peetakse kinni ühes jurisdiktsioonis, kuid uurimiseks vajalikud digitaalsed tõendid, nagu näiteks teenuse kasutaja andmed, metaandmed, andmeliikluse väljavõtted jms, asuvad teised riigis (Blažič & Klobučar, 2020, p. 88). Just lähtuvalt digitaalsete tõendite asukoha määramatusest ja nende võimest riigipiire ületada (vt lõputöö lk 10) tekib vajadus piiriüleseks andmevahetuseks.

Piiriülese andmevahetuse hulk aina kasvab ning üha suurem osa kriminaalmenetlustest tugineb digitaalsetele tõenditele, mida tuleb hankida teises jurisdiktsioonis asuvatelt veebiteenuse pakkujatelt. Perioodil 2013–2018 kasvas peamistele veebiteenuste pakkujatele tehtud päringute arv koguni 84%. (Euroopa Komisjon, 2019, p. 1) Seega on

teises jurisdiktsioonis asuvad digitaalsete tõendite osatähtsus tõusvas trendis ning sellega seonduvad võimalikud probleemid üha aktuaalsemad.

Euroopa Liidu siseselt kasutatakse Euroopa uurimismäärust (ingl k *European Investigation Order*), mis võeti 2014. aastal vastu Euroopa Nõukogu ja Euroopa Parlamendi poolt ja millega on võimalik taotleda juurdepääsu piiriülestele digitaalsetele tõenditele. Kolmandatest riikidest (nt Ameerika Ühendriikidest) andmete saamiseks tuleb täita vastastikuse õigusabi taotlus või võtta ühendust otse teenusepakkujaga. Vastastikuse õigusabi taotlus on küllaltki aeganõudev meetod, sest keskmiselt kulub taotluse täitmiseks 10 kuud. (Euroopa Komisjon, 2019, p. 1) Arvestades asjaolu, et digitaalsed tõendid on oma olemuselt ajakriitilised ning neid on lihtne muuta (Hsieh, 2023, p. 8), siis on kuluv aeg üsna pikk. Üleüldiselt on ebaselge, kas traditsiooniline koostöövorm (vastastikuse õigusabi taotlus) on digitaalsete tõendite temaatikas jätkusuutlik meetod (De Busser, 2018, p. 161).

Lisaks vastastikuse õigusabi taotlusele on olemas lihtsustatud koostöövorm, mis seisneb selles, et Euroopa Liidu liikmesriigi ametiasutus võtab otse ühendust kolmanda riigi teenusepakkujaga. Ehkki selline koostöö võib olla küll kiirem, siis piirdub see ainult teatud sorti andmetega. Teenusepakkuja väljastab ainult mitte-sisuandmeid (ingl k *non-content data*), milleks on teenuse kasutaja andmed või andmeliikluse väljavõtted, kuid vahetu koostöö raames ei ole võimalik taotleda sisuandmeid (ingl k *content data*), nagu e-kirjade, tekstisõnumite, fotode jms sisu. (Euroopa Komisjon, 2019, p. 1)

Kusjuures selline vahetu koostöö on vabatahtlik – teenusepakkujad on tavaliselt eraettevõtted, kes ei ole kohustatud päringutele vastama, mistõttu sõltuvad uurimisasutused teenusepakkuja koostöövalmidusest (Cole & Quintel, 2018, p. 1). Siinkohal on oluline märkida, et kõigist teenusepakkujatele esitatud taotlustest täidetakse reaalselt vähem kui pooled (Euroopa Komisjon, 2019, p. 1). Seega on praegused digitaalsete tõenditega seonduvad rahvusvahelise koostöö võimalused kohati piiratud ja puudulikud.

Eelnevast võib järeldada, et digitaalsete tõenditega seonduv on tõepoolest problemaatiline ning vajab ülevaatamist. Teistest jurisdiktsioonidest (eriti kolmandatest riikidest) vajalike digitaalsete tõendite taotlemine võib osutuda keeruliseks ning statistikat arvesse võttes on see üsna aktuaalne probleem. Eestis pole seaduse tasandil vastu võetud seadusandlikke

ja muid meetmeid, mida arvutikuritegevusvastase konventsiooni kohaselt kehtestama peaks. Digitaalsete tõendite kasutamine on küll kohtupraktikast nähtuvalt võimalik, kuid selles esineb probleeme, sest teistele tõendiliikidele seatud vormistuslikud nõuded ei pruugi digitaalsete tõendite eripära arvestades kuigi sobilikud olla.

1.3. Digitaalsete tõendite vormistamise põhimõtted

Järgnev tekst on tööst eemaldatud AvTS § 35 lg 1 p 5^1 alusel (vt täies mahus tööd).

TÖÖST ON EEMALDATUD JUURDEPÄÄSUPIIRANGUGA TEAVE

Rektori otsus: 24.04.2023 nr 6.1-19/1297-1

TÖÖST ON EEMALDATUD JUURDEPÄÄSUPIIRANGUGA TEAVE

Rektori otsus: 24.04.2023 nr 6.1-19/1297-1

TÖÖST ON EEMALDATUD JUURDEPÄÄSUPIIRANGUGA TEAVE

Rektori otsus: 24.04.2023 nr 6.1-19/1297-1

TÖÖST ON EEMALDATUD JUURDEPÄÄSUPIIRANGUGA TEAVE

Rektori otsus: 24.04.2023 nr 6.1-19/1297-1

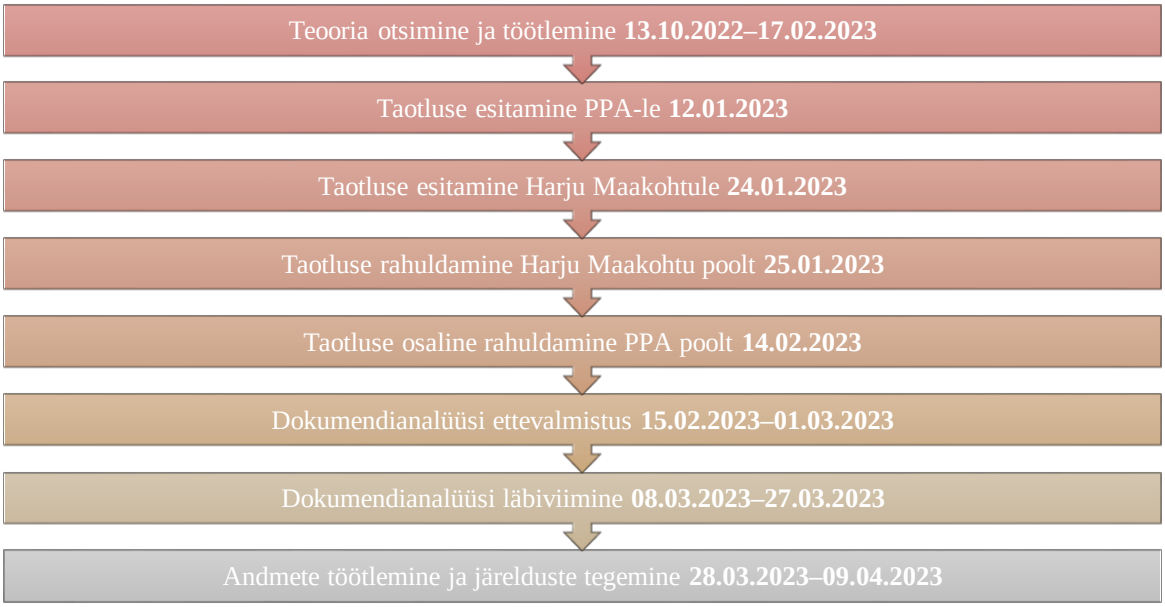
TÖÖST ON EEMALDATUD JUURDEPÄÄSUPIIRANGUGA TEAVE

Rektori otsus: 24.04.2023 nr 6.1-19/1297-1

2. EMPIIRILINE OSA

Käesoleva lõputöö raames viiakse läbi uuring, mille eesmärk on välja selgitada digitaalsete tõendite vormistamise praktika Põhja prefektuuris, et analüüsida sellega seonduvaid põhimõtteid ja probleeme. Esimeses alapeatükis kirjeldatakse uuringu meetodit, protsessi ja valikut, sh tuuakse välja lõputöö etapid kuupäevaliselt (vt joonis 1). Teises alapeatükis tuuakse välja uuringu tulemused ning kolmandas alapeatüki tehakse tulemustest lähtuvalt järeldusi ja ettepanekuid võimalike kitsaskohtade parandamiseks.

2.1. Uuringu meetodid, protsess ja valik



Joonis 1. Lõputöö etapid (2023, autori koostatud)

Uuringu läbiviimiseks taotleti luba Politsei- ja Piirivalveameti (PPA) uurimistööde komisjonilt. Muuhulgas taotleti uuringu raames kriminaaltoimikuid nii PPA-lt kui ka Harju Maakohtult. Töö esialgne eesmärk oli analüüsida nii kohtulahendi saanud kriminaalasjade toimikuid kui ka lõpetatud kriminaalasjade toimikuid, et saada laiem ülevaade menetluspraktikast ning võimalikest kitsaskohtadest. PPA kooskõlastas küll uurimistöö teema, kuid ei pidanud isikuandmete kaitse nõuete tagamisest tulenevalt võimalikuks toimikute väljastamist. Harju Maakohus kinnitas loa toimikute väljastamiseks, seega analüüsitakse käesolevas töös ainult kohtulahendi saanud toimikuid.

Lõputöös kasutatakse **uurimismeetodina** kvalitatiivset empiirilist uuringut. Kvalitatiivse uurimistöö mõistet on keerukas defineerida, kuivõrd pole võimalik välja töötada üldiselt aktsepteeritud määratlust (Õunapuu, 2014, lk 52). Kvalitatiivne uuring võimaldab probleemi põhjalikku ja üksikasjalikku uurimist (Patton, 2002, p. 14). Kvalitatiivse uuringu eesmärk on saada detaile hõlmavat empiirilist andmestikku, mis oleks terviklik (Laherand, 2008, lk 21). Selleks, et selgitada välja, millised on digitaalsete tõendite vormistamise põhimõtted ja puudused ning kuidas selliseid tõendeid Eesti menetluspraktikas vormistatakse, on tarvis kriminaaltoimikutes olevat teavet detailselt ja terviklikult analüüsida. Seetõttu täidab kvalitatiivne empiiriline uuring käesoleva töö eesmärki kõige edukamalt.

Andmekogumismeetodina kasutatakse töös dokumendianalüüsi, mille positiivsus seisneb selle tõhususes ja täpsuses. Võrreldes teiste andmekogumismeetoditega nõuab dokumendianalüüs vähem aega ning selle sisuks on andmete valimine, mitte andmete kogumine. Negatiivsena võib välja tuua dokumentide ebapiisava detailsuse – dokumente koostatakse muul eesmärgil kui uurimistööks ning seetõttu ei pruugi need uurimisküsimustele vastamiseks piisavalt detaile sisaldada. (Bowen, 2009, p. 31) Siiski on dokumendianalüüs käesoleva uuringu läbiviimiseks kõige sobilikum – see on ainus meetod, millega on võimalik menetluspraktikat ja sellega seonduvaid probleeme reaalselt uurida. Kriminaaltoimikutes olevaid dokumente analüüsides on võimalik uurida, mil moel on praktikas tagatud digitaalsete tõendite usaldusväärsus, jälgitavus, kontrollitavus jms.

Uuringu **valimiks** on ettekavatsetud valim, mille puhul koostatakse uuritavate objektide valim eesmärgist lähtuvalt kindlate kriteeriumite alusel (Õunapuu, 2012). Ettekavatsetud valim puhul on süvendatult fookuses kindlatel alustel valitud uuritavad objektid, mis on konkreetse nähtuse uurimiseks kõige sobilikumad ning mis võimaldavad nähtuse kohta kõige asjakohasemat ja põhjalikumat teavet saada (Patton, 2002, p. 230). Käesoleva uuringu valimiks on Põhja prefektuuri allüksuste menetlustes olnud kriminaaltoimikuid karistusseadustiku § 157^3 kriminaalasjades, mis said 2021. aastal kohtulahendi – kokku 13 kriminaalasja. Kriminaaltoimikutes olevate tõendite analüüsimine annab kõige asjakohasema ülevaate sellest, kuidas digitaalseid tõendeid vormistatakse.

Valimi puhul oli eesmärk taotleda vähemalt ühe aasta jooksul kohtuotsuse saanud toimikud, et saada menetluspraktikast laiem ülevaade. Selleks, et valimis ei oleks

käesoleva töö mahtu arvestades liiga suur hulk toimikuid, valiti üks kindel kuriteokoosseis. Valimi kitsendamiseks sobis KarS § 157^3 ehk ahistava jälitamise koosseis, mille sisuks on teise isikuga korduva või järjepideva kontakti otsimine, tema jälgimine või muul viisil isiku tahte vastaselt tema eraellu sekkumine, kui selle eesmärk või tagajärg on tema hirmutamine, alandamine või muul viisil oluliselt häirimine (Karistusseadustik, 2001). KarS § 157^3 kriminaalasjad olid uuringuks sobilikud, sest nende menetluste raames esineb sageli olukordi, kus mõni menetluses osaleja esitab ise menetlejale digitaalseid tõendeid. Siiski on selliste tõendite olemus ka teiste koosseisude puhul sisuliselt sama, mis võimaldab uuringu tulemusi üldistada laiemalt kui ainult KarS § 157^3 koosseisu menetluste raames.

Andmeanalüüsimeetodina rakendatakse kvalitatiivset sisuanalüüsi, mida kasutatakse tekstide sisu või kontekstilise tähenduse uurimiseks (Laherand, 2008, lk 290). Kvalitatiivse sisuanalüüsi positiivse küljena saab välja tuua, et see on tundlik ja täpne ning tähelepanu on võimalik pöörata ka harva esinevatele nähtustele tekstis. Samas on kvalitatiivse sisuanalüüsi käigus keeruline läbi töötada suuri valimeid, mistõttu iseloomustab seda kohati vähene üldistatavus. (Kalmus, *et al*., 2015) Tavapärast sisuanalüüsi kasutatakse enamasti siis, kui konkreetse nähtuse kohta ei ole piisavalt teooriaid või uurimisandmeid (Hsieh & Shannon, 2005, lk 1279 ref Laherand, 2008, lk 290), mistõttu on seda igati sobilik kasutada menetluses osalejate poolt esitatud digitaalsete tõendite vormistamise protsessi ja sellekohase menetluspraktika uurimiseks.

2.2. Uuringu tulemused

Käesolevas alapeatükis antakse ülevaade dokumendianalüüsi tulemustest. Sealjuures on välja toodud kõik kategooriad ja koodid, mis uurimisküsimuste ja 13 kohtutoimiku analüüsi põhjal moodustusid. Samuti antakse ülevaade sellest, milline kategooria millisele uurimisküsimusele vastab, ning tuuakse välja üldised uuringu tulemused.

Uuringu raames koostati neli kategooriat, mille eesmärk oli vastata töö sissejuhatuses püstitatud kolmele uurimisküsimusele (vt tabel 1). Esimesele uurimisküsimusele vastuse saamiseks loodi kategooria „Digitaalne tõend“, mille raames koostatud koodid näitlikustavad seda, milliseid erinevaid digitaalseid tõendeid toimikutes esines. Teisele uurimisküsimusele vastab teine kategooria ehk „Digitaalse tõendi edastamise viis menetluses osaleja poolt“, mille raames tuuakse välja erinevad viisid, kuidas menetluses

osalejad digitaalseid tõendeid menetlejale edastavad. Edastamise viis on oluline, sest sellest võib sõltuda tõendi vormistamine ja usaldusväärsus. Kolmandale uurimisküsimusele vastuse saamiseks loodi kaks kategooriat – „Digitaalse tõendi vormistus toimikus“ ning „Puudused (vaatlusprotokolli) vormistamisel“. Eelmainitu väljaselgitamine on oluline selleks, et saada ülevaade menetluspraktikast ning selgitada selle põhjal välja võimalikud kitsaskohad.

Tabel 1. Kategooriate ja uurimisküsimuste vastavus (2023, autori koostatud)

UURIMISKÜSIMUS	KATEGOORIA
Mis on digitaalne tõend?	Kategooria 1. Digitaalne tõend
Kuidas menetluses osalejad digitaalseid tõendeid esitavad?	Kategooria 2. Digitaalse tõendi edastamise viis menetluses osaleja poolt
Millised puudused esinevad digitaalsete tõendite vormistamisel?	Kategooria 3. Digitaalse tõendi vormistus toimikus
Millised puudused esinevad digitaalsete tõendite vormistamisel?	Kategooria 4. Puudused (vaatlusprotokolli) vormistamisel

Tabel 2. Kategooria 1. Digitaalne tõend (2023, autori koostatud)

KATEGOORIA 1	KOOD		ESINEMINE TOIMIKUTES
DIGITAALNE TÕEND	1	Suhtlusrakenduse sõnum	10
	2	SMS sõnum	6
	3	E-kiri	8
	4	Kõnelogi	4
	5	Pangaülekande väljavõte	1
	6	Postitus internetileheküljel	4
	7	Videosalvestis	3
	8	Helisalvestis	5
	9	Foto	6
	10	Muu dokument	2

Kategooria 1 näitlikustab seda, millised võivad olla erinevad digitaalsed tõendid (vt tabel 2). Esimesele uurimisküsimusele vastuse saamiseks analüüsiti 13 erinevat KarS § 157[3] koosseisu toimikut ning selle käigus selgitati välja kõik erinevad digitaalsed tõendid, mis menetluses osalejad menetlejale esitanud on. Analüüsi tulemusena on võimalik välja tuua 10 erinevat koodi, mis tähistavad toimikutes olnud digitaalseid tõendeid.

Kõige rohkem oli selliseid toimikuid (10), kus oli digitaalseks tõendiks suhtlusrakenduse sõnumivahetus (**kood 1**). Peamiselt oli tegemist selliste rakendustega, nagu WhatsApp, Viber, Facebook Messenger, Snapchat, Instagram. Eraldi on välja toodud SMS sõnumid ehk siis tekstisõnumid (**kood 2**), mille saatmiseks/vahetamiseks ei ole vaja eraldi rakendust. SMS sõnumid olid digitaalseks tõendiks kuue toimiku puhul. Lisaks olid enam kui pooltes toimikutes digitaalseks tõendiks e-kirjad (**kood 3**), mis olid peamiselt Gmaili (Google Mail) teenuse vahendusel saadetud.

Neljas toimikus oli tõendiks kõnelogid (**kood 4**), mis olid toimikus kuvatõmmisena, fotona või koguni menetluses osaleja enda koostatud Microsoft Exceli tabelina. Eelkõige selliste tõendite puhul tasub usaldusväärsuse seisukohast kaaluda, kas oleks võimalik samu andmeid taotleda algallikast ehk sideettevõtjalt. Ühes toimikus oli tõendiks pangatehingu väljavõte (**kood 5**), täpsemalt kuvatõmmis sellest. Sealjuures polnud niivõrd oluline tehing ja selle asjaolud, vaid ülekande selgitusse kirjutatud tekst.

Lisaks oli neljas toimikus tõendiks internetilehekülje (nt Facebooki) postitus (**kood 6**), kust nähtusid ahistava jälitamise asjaolud. Menetluses osalejad esitasid muuhulgas enda tehtud videosalvestisi (**kood 7**), helisalvestisi (**kood 8**) ning fotosid (**kood 9**). Muu dokumendi (**kood 10**) all peetakse silmas toimikutes olnud lepinguid, arveid jms, mis annavad informatsiooni tõendamiseseme asjaolude kohta ning mille menetluses osaleja on edastatud digitaalsel kujul.

Eeltoodust nähtub, et digitaalsed tõendid võivad ühe konkreetse kuriteokoosseisu puhul olla küllaltki erinevad ning neid võib leida praktiliselt igalt poolt. Buzarovska Lazetik ja Koshevaliska (vt lõputöö lk 9) on välja toonud erinevad võimalikud digitaalsed tõendid ning mainivad muuhulgas erinevaid dokumente, e-kirju, internetilehekülgede postitusi, kõnelogisid jpm, mis kõik esinesid ka analüüsitud toimikutes.

Tabel 3. Kategooria 2. Digitaalse tõendi edastamise viis menetluses osaleja poolt (2023, autori koostatud)

KATEGOORIA 2	KOOD		ESINEMINE TOIMIKUTES
DIGITAALSE TÕENDI EDASTAMISE VIIS MENETLUSES OSALEJA POOLT	1	Mobiiltelefon koos tõenditega	8
	2	Mälupulk koos tõenditega	4
	3	E-kirjaga	11
	4	Elektroonilise süüteoteate/avalduse lisana	4

Kategooria 2 vastab teisele uurimisküsimusele ning sellega seoses toodi välja erinevad viisid, kuidas menetluses osalejad menetlejale digitaalseid tõendeid edastavad (vt tabel 3). Edastamise viis on oluline, sest see, millisel kujul tõend menetlejani jõuab, võib mõjutada tõendi usaldusväärsust ning samuti seda, kas ja kuidas tõendit vormistama peaks. **Kood 1** ehk mobiiltelefon koos tõenditega tähistab olukorda, kus menetluses osaleja andis menetlejale ajutiselt üle oma mobiiltelefoni, milles olid olulised digitaalsed tõendid (esines kaheksa toimiku puhul 13-st). Menetleja tutvus telefonis olevate fotode, videosalvestiste, kõnelogide, internetilehekülgede postituste, SMS sõnumite ning erinevate suhtlusrakenduste sõnumitega. Peamine viis nende tõendite talletamiseks oli järgmine: menetleja fotografeeris oma mobiiltelefoniga menetluses osaleja mobiiltelefonis olevaid digitaalseid tõendeid ning talletas fotod CD või DVD plaadile. Pärast vaatlust anti mobiiltelefon menetluses osalejale tagasi.

Nelja toimiku puhul nähtus, et menetluses osaleja kogus võimalikud digitaalsed tõendid oma isiklikule mälupulgale ning andis mälupulga menetlejale üle (**kood 2**). Mälupulgale olid talletatud näiteks fotod, helisalvestised, videosalvestised ning kuvatõmmised e-kirjadest, SMS sõnumitest ja suhtlusrakenduse sõnumitest. Siinkohal saab tuua välja olulise erinevuse mälupulga (ja teiste andmekandjate) ning mobiiltelefoni vahel. Kui menetluses osaleja annab üle mälupulga, siis on ta juba teinud tõendite hulgas teatud valiku ning näiteks sõnumite puhul on mälupulgale talletatud vaid kuvatõmmised vestlustest – uurijal puudub sellisel juhul võimalus reaalselt algkujul olevate sõnumitega tutvuda. Mobiiltelefoni puhul on uurijal siiski võimalus ise telefonis või suhtlusrakenduses olevaid sõnumeid lugeda ning metaandmeid vaadata ja talletada. Sellisel juhul on tõendite usaldusväärsus mõnevõrra suurem, kui pelgalt kuvatõmmiste

puhul. Ehkki ka mobiiltelefoni puhul tuleb arvestada, et selles olevaid tõendeid on võib-olla muudetud ning need pole enam autentsed.

Kood 3 ehk e-kiri tähendab, et menetluses osaleja on digitaalsed tõendid edastanud e-kirja teel otse uurija e-postile – seda esines 11 toimiku puhul 13-st. E-kirja teel edastatavad tõendid võivad samuti olla kuvatõmmised erinevatest sõnumitest, e-kirjadest ja kõnelogidest, samuti fotod, videosalvestised ja muud dokumendid. Ühel juhul saatis menetluses osaleja e-kirja teel näiteks kuvatõmmised pangaülekannete väljavõtetest. Mitme toimiku puhul oli kannatanu edastanud kahtlustatava poolt saadetud e-kirjad otse – st ei teinud e-kirjast kuvatõmmist, vaid edastas (ingl k *forward*) e-kirja teel menetlejale kahtlustatava poolt saadetud e-kirja. Sellisel juhul tuleb silmas pidada, et e-kirja edastamine teisele isikule muudab osaliselt e-kirja päises olevaid metaandmeid. Samuti ei saa sellisel juhul kindel olla, kas e-kiri on autentne või on edastaja kirja sisu mingis osas muutnud.

Neljas toimikus oli elektroonilise süüteoteate/avalduse väljatrükk, mille lisana oli kannatanu edastanud digitaalsed tõendid (**kood 4**). Kui kannatanu teatab kuriteost elektroonilise avaldusega, siis on tal võimalik lisada muud olulist materjali, olgu selleks kuvatõmmised sõnumitest ja e-kirjadest, fotod, dokumendid jms. Sellisel juhul on samuti tegemist kuvatõmmistega, mille kannatanu on ise valikuliselt teinud, ning sellega peab arvestama tõendite usaldusväärsuse hindamisel.

Seega ilmnes 13 toimiku analüüsimisel, et menetluses osalejad edastavad menetlejale digitaalseid tõendeid neljal erineval moel. Igal neist on omad miinused, kuid nende hulgast võib siiski kõige usaldusväärsemaks pidada seda, kui menetluses osaleja annab üle oma mobiiltelefoni ning uurija talletab selles olevad digitaalsed tõendid.

Tabel 4. Kategooria 3. Digitaalse tõendi vormistus toimikus (2023, autori koostatud)

KATEGOORIA 3	KOOD		ESINEMINE TOIMIKUTES
DIGITAALSE TÕENDI VORMISTUS TOIMIKUS	1	Vaatlusprotokoll	13
	2	Ülekuulamise protokolli lisa	5
	3	Õiend	1
	4	Pole eraldi vormistatud	3

Kategooria 3 on oluline, et saada vastus kolmandale uurimisküsimusele ehk selgitada välja, millised puudused esinevad digitaalsete tõendite vormistamisel. Selleks oli omakorda oluline välja selgitada, millisel viisil menetlejad digitaalseid tõendeid vormistavad (vt tabel 4). **Kood 1** ehk vaatlusprotokoll oli erinevatest variantidest kõige sagedasem – igas analüüsitud toimikus esines vähemalt üks asitõendi vaatlusprotokoll, ühes toimikus oli lisaks teabesalvestise vaatlusprotokoll. Oma olemuselt on tegemist samasuguste protokollidega, uurimistoiminguks on vaatlus ning selle toiminguga saadavaks tõendiks on vaatlusprotokoll. Peamiselt oli vaatluse objektiks mobiiltelefon või mälupulk, aga oli vaadeldud ka menetluses osaleja poolt e-kirja teel edastatud materjali.

Viies toimikus oli digitaalne tõend vormistatud ülekuulamise protokolli juurde selle lisana (**kood 2**). Selliselt olid vormistatud näiteks uurija tehtud fotod menetluses osaleja mobiiltelefonist (mida kood 1 puhul vormistati vaatlusprotokolliga) ning menetluses osaleja poolt edastatud kuvatõmmised sõnumitest või e-kirjadest. Peab arvestama, et sellisel kujul olev kuvatõmmis või foto ei saa olla eraldiseisev/iseseisev tõend. Olukorras, kus kriminaalasi lahendatakse üldmenetluses ning kõik osapooled kuulatakse kohtus uuesti üle, ei ole võimalik pöörduda eraldi tõendi juurde, mis vormistati kohtueelses menetluses läbiviidud ülekuulamise juurde lisana. Lisaks tuleb siinkohal arvestada Riigikohtu seisukohaga, et menetluses osaleja poolt üle antud digitaalseid tõendeid tuleks käsitleda asitõendina või dokumendina ning vormistada vastavalt (vt lõputöö lk 14). Ülekuulamise protokolli lisa võib olla toimingu käiku ja tulemusi kajastav salvestis, mis tekib ülekuulamise käigus. Seega tuleks sellisel viisil menetluses osaleja poolt esitatud digitaalsete tõendite vormistamist vältida.

Ühe toimiku puhul 13-st esines olukord, kus digitaalset tõendit kajastati üksnes õiendiga ning täiendav vormistamine puudus (**kood 3**). Täpsemalt oli tegemist videosalvestisega. Õiendis toodi välja, et kannatanu edastas salvestise e-kirja teel, samuti on lühidalt kirjeldatud videosalvestisest nähtuvat. Selline viis digitaalse tõendi vormistamiseks on siiski ebakorrektne – selleks, et tuua välja videosalvestise sisu ja kriminaalasjas tähtsust omavad asjaolud, tuleb videosalvestist vaadelda ning toiming vaatlusprotokolliga vormistada. Vastasel juhul ei ole tegemist tõendiga.

Lisaks oli kolm toimikut, milles poldud digitaalseid tõendeid üldse eraldi vormistatud (**kood 4**). Selline olukord esines menetluses osaleja poolt saadetud e-kirjade puhul. On

oluline välja tuua, et Riigikohtu praktika kohaselt saab e-kirju aktsepteerida dokumendina, mis tähendab, et neid ei olegi tarvis tingimata eraldi vormistada (vt lõputöö lk 15). Siiski tuleb meeles pidada, et juhul, kui e-kirja usaldusväärsuse või muude asjaolude osas tekivad küsitavused, peab olema võimalik neid kontrollida. Toimikutest ei nähtunud, milliseid ettevaatusabinõusid oli menetleja rakendanud, et selleks olukorraks valmistuda.

Kolmanda kategooria analüüsimisel selgus, et digitaalseid tõendeid on vormistamistatud neljal erineval viisil. Kõige sagedasem oli digitaalse tõendi vaatlemine ning vaatlusprotokolliga vormistamine. Samuti oli toimikutes e-kirju, mis võivad olla käsitatavad dokumendina ning mida ei pea seetõttu täiendavalt vormistama. Küll aga on ebakorrektne vormistada õiendi või ülekuulamise protokolliga selliseid digitaalseid tõendeid, mida tegelikult peaks eraldi vaatlema.

Tabel 5. Kategooria 4. Puudused (vaatlusprotokolli) vormistamisel

KATEGOORIA 4	KOOD		ESINEMINE TOIMIKUTES
PUUDUSED (VAATLUSPROTOKOLLI) VORMISTAMISEL	1	Pole kasutatud koopiat	12
	2	Tõendi teekond pole jälgitav	5
	3	Metaandmeid ei ole kajastatud	8
	4	Vaadeldava objekti andmed/ tunnused puudulikud	5
	5	Puudused vaatluse käigu kajastamisel	5

Järgnev tekst on tööst eemaldatud AvTS § 35 lg 1 p 5[1] alusel (vt täies mahus tööd).

Kood 2 tähistab tõendi jälgitavust – täpsemalt on välja toodud, et tõendi jälgitavusega on probleeme viies toimikus 13-st. See tähendab, et vaatlusprotokollist (või üldiselt toimikust) ei nähtunud seda, millal, kuidas või kust vaadeldav objekt kriminaalasja juurde jõudis või mida sellega tehti. Tõendi jälgitavus on tõendi usaldusväärsuse seisukohast väga oluline (vt lõputöö lk 18), seetõttu on katkendlik või puudulik jälgitavuse ahel küllaltki problemaatiline. Ülejäänud toimikutes oli jälgitavus tagatud näiteks üleandmise-vastuvõtmise aktiga või muu menetluses osaleja poolt kirjutatud avaldusega, millest nähtus, et ta annab vabatahtlikult uurijale üle oma mobiiltelefoni või mälupulga. Samuti oli välja toodud see, mida tõendiga tehti ning mis sai tõendist pärast vaatlust.

Metaandmetes seisneb digitaalsete tõendite põhiline väärtus (vt lõputöö lk 10). Toimikute analüüsimisel selgus, et 13-st toimikust kaheksas ei olnud tõendite vaatlusel metaandmeid kajastatud (**kood 3**). Olukorras, kus menetluses osaleja on menetlejale edastanud kuvatõmmised e-kirjast või sõnumist, ei olegi võimalik näha originaalseid metaandmeid. Sellisel juhul on võimalik tutvuda ainult kuvatõmmise metaandmetega, kuid kuvatõmmise sisu kohta ei pruugi see kuigi palju öelda. Samas esines olukordi, kus vaadeldavaks objektiks oli mobiiltelefon, mille galeriis olevaid fotosid vaatluse käigus vaadeldi, kuid mille puhul metaandmeid välja ei toodud (mida sellisel juhul oleks olnud võimalik iseenesest teha).

Siiski esines ka toimikuid, kus olid digitaalse tõendi metaandmed vaatluse käigus välja toodud – näiteks foto puhul faili nimi, suurus, formaat, samuti foto tegemise kuupäev, asukoht, seade ja muud foto tegemisega seotud andmed. Võimalusel tulekski digitaalseid tõendeid vormistada selliselt, et nähtuksid metaandmed, mis tõendi väärtust ja usaldusväärsust tõstavad.

Kood 4 tähistab olukorda, kus vaadeldava objekti andmeid või tunnuseid oli puudulikult kirjeldatud, ning seda esines kokku viies toimikus 13-st. See tähendab, et näiteks mobiiltelefoni vaatluses ei toodud korrektselt välja telefoni marki, mudelit, identifitseerivat seerianumbrit või väliseid tunnuseid. Seega ei ole vaatlusega korrektselt

fikseeritud, millist objekti üldse vaadeldakse. Andmekandja tunnuste kajastamine vaatlusprotokollis on siiski oluline (vt lõputöö lk 22).

Lisaks andmekandja tunnuste kajastamisele on oluline kirjeldada võimalikult detailselt vaatluse käiku. Viies toimikus 13-st esinesid vaatluse käigu kirjeldamisel puudused (**kood 5**) – st vaatluse käiku oli kajastatud pealiskaudselt, mistõttu ei olnud protokolli põhjal võimalik toimingu sisust aru saada. Näiteks esines vaatlusprotokoll, kus kajastusid fotod või kuvatõmmised, kuid ei nähtunud, kuidas andmekandjat vaadeldes nendeni jõuti või mida konkreetselt vaatluse läbiviija tegi. Vaatluse käigu detailne kajastamine on siiski oluline, et tagada korratavuse põhimõte (vt lõputöö lk 18). Tuleb tagada võimalus läbiviidud toiminguid kontrollida – samadel tingimustel samu meetodeid kasutades peaks jõudma sama tulemuseni. Selleks tuleks aga vaatluse tingimusi ja meetodeid piisava täpsusega kirjeldada.

Seega ilmnes 13 toimiku analüüsimisel viis peamist puudust, mida digitaalse tõendi vaatlemisel või vaatluse vormistamisel tehti. Tõendiga ümberkäimisel ei kasutatud koopiat ning esines toimikuid, milles ei olnud tõendi teekond jälgitav. Samuti ei kajastatud metaandmeid või ilmnesid puudused vaadeldava objekti või vaatluse käigu kirjeldamisel. Lisaks võib puudusena välja tuua selle, et mõnes toimikus oli digitaalne tõend vormistatud ülekuulamise protokolli lisana või õiendiga.

2.3. Järeldused ja ettepanekud

Töö uurimisprobleemile (kuidas menetluses osalejate poolt esitatud digitaalseid tõendeid korrektselt ja usaldusväärselt vormistada?) vastuse leidmiseks püstitati kolm uurimisküsimust. Vastates **esimesele uurimisküsimusele** (Mis on digitaalne tõend?) saab uuringu tulemuste alusel väita, et digitaalne tõend võib olla mis tahes digitaalne teave, mida saab konkreetses kriminaalasjas tõendina kasutada. Uuringu tulemuste põhjal selgus, et digitaalseks tõendiks võivad olla näiteks suhtlusrakenduse või SMS sõnumid, e-kirjad, telefoni kõnelogid, postitused internetilehekülgedel, videosalvestised, helisalvestised, fotod, väljavõtted pangatehingutest või muud dokumendid. Ehkki uuringus oli valimiks ainult üks kuriteokoosseis, mis pole oma olemuselt otseselt arvutisüsteemidega seotud, siis kasutati selle raames väga palju erinevaid digitaalseid tõendeid.

Eeltoodu seostub teooriaosas välja toodud Hsieh väitega, kelle hinnangul võib tänapäeval digitaalseid tõendeid leida peaaegu kõikjalt (vt lõputöö lk 9). Samuti toovad Laurits ja Kasper välja, et tavatu pole olukord, kus kuriteo toimepanemine ei ole otseselt arvutisüsteemidega seotud, kuid olulised tõendid asuvad just arvutisüsteemides (vt lõputöö lk 8). Uuringu tulemustest selgunud erinevad võimalikud digitaalsed tõendid seostuvad teooriaosas välja toodud definitsiooniga, mille kohaselt on digitaalne tõend igasugune digitaalsel kujul loodud, töödeldud, salvestatud või edastatud teave, mida saab kasutada kohtus tõendamiseseme asjaolude selgitamisel (vt lõputöö lk 9).

Teise uurimisküsimuse (Kuidas menetluses osalejad digitaalseid tõendeid esitavad?) vastus põhineb samuti dokumendianalüüsi tulemustel. Uuringu tulemuste alusel saab väita, et menetluses osalejad esitavad digitaalseid tõendeid e-kirja teel ning elektroonilise süüteoteatega või avaldusega, samuti annavad üle enda mobiiltelefoni või mälupulga, kuhu on tõendid talletatud. See seostub teoorias välja toodud Hsieh väitega, et võimalikud digitaalsete tõendite allikad võivad muuhulgas olla mobiiltelefonid, mälupulgad, serverid, arvutid jpm (vt lõputöö lk 9). Seega võib menetluses osaleja esitada digitaalseid tõendeid küllaltki erinevatel viisidel. Uurija ülesanne on võimalusel menetluses osalejat juhendada, et tõend jõuaks kriminaalasja juurde võimalikult usaldusväärse ja autentsena.

Vastates **kolmandale uurimisküsimusele** (Millised puudused esinevad digitaalsete tõendite vormistamisel?) saab uuringu tulemuste põhjal ühe aspektina välja tuua, et tõendi vormistamiseks valitakse ebakorrektne meetod, nagu ülekuulamise protokoll või õiend. See läheb vastuollu teooriaosas välja toodud Riigikohtu seisukohaga, mille kohaselt peaksid menetluses osalejate poolt esitatud digitaalsed tõendid olema käsitatavad asitõendi või dokumendina ning sealjuures tuleb neid ka vastavalt vormistada (vt lõputöö lk 13). Muuhulgas peab arvestama, et kui mingi foto või muu salvestis on vormistatud ülekuulamise protokolli lisana, siis peaks see kajastama ülekuulamise käiku ja tulemusi – menetluses osalejate poolt edastatud kuvatõmmised jms seda ei kajasta.

Teise aspektina saab välja tuua, et tõendite vormistamisel ei järgita digitaalsete tõendite käitlemise põhimõtteid. Uuringu tulemustest selgus, et tõendi vaatlusel ei ole kasutatud koopiat, vaid on vaadeldud originaaltõendit või menetluses osaleja poolt loodud kuvatõmmist. See läheb vastuollu teooriaosas välja toodud Hsieh väitega, mille kohaselt ei tohiks vaadelda ja analüüsida originaaltõendit, vaid tuleb luua koopia, mille abil on võimalik tagada tõendite puutumatus ja usaldusväärsus (vt lõputöö lk 18). Samuti on

koopia tegemine oluline, et tagada autentsus, mille tähtsust on rõhutanud Lall, Öpik ja Tohter – autentsus näitab, et tõend on ehtne ja terviklik ning selle sisu ei ole muudetud (vt lõputöö lk 18).

Lisaks selgus, et mitmes toimikus ei olnud piisavalt kajastatud jälgitavuse ahelat – st toimikust või vaatlusprotokollist ei nähtunud, kuidas digitaalne tõend kriminaalasja juurde jõudis. Siiski kinnitab Hsieh, et arvestades digitaalse tõendi habrast ja muutlikku loomust on jälgitavuse ahela tagamine usaldusväärsuse seisukohast hädavajalik (vt lõputöö lk 18). Muuhulgas võib puudustena välja tuua, et digitaalse tõendi vaatlemisel ei kajastatud metaandmeid ning vaatluse käiku või vaadeldavat objekti ei olnud piisavalt kirjeldatud. Metaandmed annavad digitaalsele tõendile olulise väärtuse ning nende kajastamine aitab tagada tõendi autentsust (vt lõputöö, lk 10). Vaatluse käigu või vaadeldava objekti ebapiisav kirjeldamine läheb vastuollu korratavuse põhimõttega, mille kohaselt peab samadel tingimustel samade meetoditega olema võimalik saavutada sama tulemus. Teooriaosas on välja toodud Johnsoni seisukoht, et korratavuse tagamiseks tuleb kõik digitaalsete tõenditega teostatud toimingud korrektselt fikseerida ja dokumenteerida (vt lõputöö lk 18).

Üldiselt seostuvad eelpool mainitud puudused teooriaosas välja toodud Tehveri väitega, mille kohaselt võib olla mõneti keeruline digitaalsete tõendite liigitamine kriminaalmenetluse seadustikus loetletud tõendiliikide alla ning see omakorda tekitab segadust tõendite vormistamisel (vt lõputöö lk 13). Samuti pole Eesti kriminaalmenetluse seadustikus sätestatud digitaalsete tõendite kogumise korda või muud sellega seonduvat, mis võib selgitada vormistusega seonduvaid puudusi ja arusaamatusi.

Kokkuvõtteks saab **uurimisprobleemi** (Kuidas menetluses osalejate poolt esitatud digitaalseid tõendeid korrektselt ja usaldusväärselt vormistada?) vastusena välja tuua, et esmalt tuleb tagada tõendiallika usaldusväärsus ning teisalt peab järgima digitaalsete tõendite käitlemise põhimõtteid. Menetluses osalejate poolt esitatud tõendite puhul on uurijal keeruline kontrollida, kas tõendiga on eelnevalt manipuleeritud. Mõistagi oleks usaldusväärsem taotleda andmeid algallikast (näiteks kõnelogide puhul sideettevõtjalt), kuid kui see pole mingil põhjusel võimalik või osutub liiga keeruliseks, siis tuleks vähemalt lasta digikriminalistilt teha koopia menetluses osaleja poolt üle antud seadmes olevatest andmetest. See aitab tagada tõendi usaldusväärsuse, sest digikriminalist kasutab toiminguteks spetsiaalseid tarkvarasid ning muuhulgas on tal võimalik kustutatud

andmeid taastada. Edasi tuleks sõltuvalt tõendi sisust vormistada see dokumendina või asitõendina. Sealjuures peab arvestama digitaalsete tõendite käitlemise põhimõtetega, nagu autentsus, jälgitavus, korratavus ning kriminalistikaline usaldusväärsus.

Uuringu tulemuste alusel esitatakse kolm **ettepanekut**.

1. Korraldada digitaalsete tõendite käitlemise teemalisi koolitusi, mida viiksid läbi digikriminalistid koostöös prokuröridega ning mis oleksid suunatud Politsei- ja Piirivalveameti prefektuuride ja jaoskondade uurijatele. Koolitused võiksid muuhulgas olla suunatud digitaalsete tõendite vormistamisele ning eesmärk oleks tagada usaldusväärne ja korrektne vormistamine ka olukordades, kus uurija ei kaasa digikriminalisti. Oluline on luua praeguse seaduse kontekstis ühtne arusaam ja menetluspraktika, et menetluskvaliteeti tõsta.
2. Täiendada politseiteenistuse õppekava ning lisada õppekavasse senisest suuremas mahus digikriminalistikaga seonduvaid loenguid ja praktilisi tunde, mis võimaldaksid juba hariduse omandamise faasis saada põhjalikumad teadmised digitaalsete tõendite käitlemisega seonduvast. Eesmärk on luua olukord, kus tööd alustaval noorel ametnikul oleksid piisavad alusteadmised ja oskused, et tagada digitaalsete tõendite korrektne ja usaldusväärne käitlemine.
3. Lisaks digitaalsete tõendite käitlemise juhendile, mis on suunatud digikriminalistidele, tuleks luua ametlik juhend uurijatele, et tagada võimalikult korrektne ja usaldusväärne tõendite vormistamine ka juhul, kui digikriminalisti ei kaasata. Juhendi võiks luua Politsei- ja Piirivalveameti ning Prokuratuuri koostöös.

KOKKUVÕTE

Käesoleva töö eesmärk oli välja selgitada menetluses osalejate poolt esitatud digitaalsete tõendite vormistamise põhimõtted ja kitsaskohad ning teha ettepanekuid olukorra parandamiseks. Lõputöö kokkuvõtteks saab öelda, et eesmärk sai täidetud.

Lõputöös püstitati uurimisprobleem, kuidas menetluses osalejate poolt esitatud digitaalseid tõendeid korrektselt ja usaldusväärselt vormistada. Uurimisprobleemi täpsustamiseks ja eesmärgi täitmiseks püstitati kolm uurimisküsimust.

1) Mis on digitaalne tõend?
2) Kuidas menetluses osalejad digitaalseid tõendeid esitavad?
3) Millised puudused esinevad digitaalsete tõendite vormistamisel?

Ühtlasi püstitati kolm uurimisülesannet. Esimene ülesanne oli analüüsida digitaalse tõendi olemuse ja vormistamise teoreetilisi lähtekohti ning õiguslikke probleeme. Teine ülesanne oli analüüsida Põhja prefektuuri menetluses olnud KarS § 157^3 ehk ahistava jälitamise kriminaalasjade toimikuid, et selgitada välja digitaalsete tõendite vormistamisel esinevad probleemid. Kolmandaks uurimisülesandeks oli teha teooria ja uuringu tulemuste alusel järeldusi ja ettepanekuid menetluspraktika ühtlustamiseks.

Teooriaosa esimeses alapeatükis anti ülevaade digitaalse tõendi olemusest, teises alapeatükis toodi välja digitaalsete tõenditega seonduvad õiguslikud probleemid ning kolmandas alapeatükis analüüsiti digitaalsete tõendite vormistamise teoreetilisi lähtekohti. Empiirilises osas toodi välja uuringu tulemused ning järeldused ja ettepanekud.

Lõputöö eesmärgi täitmiseks viidi läbi kvalitatiivne empiiriline uuring. Andmekogumismeetodina kasutati dokumendianalüüsi ning andmeanalüüsimeetodina rakendati kvalitatiivset sisuanalüüsi. Uuringu sisuks oli kohtutoimikute analüüsimine, mille eesmärk oli saada vastused püstitatud uurimisküsimustele.

Nii teoreetiliste lähtekohtade kui ka uuringu tulemuste analüüsimisel saadi vastused kolmele uurimisküsimusele. Digitaalne tõend on igasugune digitaalsel kujul loodud, töödeldud, salvestatud või edastatud teave, mida saab kasutada tõendamiseseme

asjaolude selgitamiseks – nagu uuringu tulemustest selgus, siis võib selleks muuhulgas olla e-kiri, suhtlusrakenduse sõnum, SMS sõnum, foto, video- või helisalvestis, internetileheküljel olev postitus, kõnelogi jpm. Menetluses osalejad esitavad digitaalseid tõendeid peamiselt e-kirja teel või elektroonilise süüteoteatega või avaldusega, samuti annavad menetluses osalejad üle oma mobiiltelefoni või muu andmekandja (nt mälupulga) koos tõenditega.

Seoses digitaalsete tõendite vormistamisega selgus, et probleem seisneb esiteks ebakorrektses vormistamise meetodis (nt vormistatakse tõend ülekuulamise protokolli lisana) ning teiseks selles, et ei järgita digitaalsete tõendite käitlemise nõudeid. Tõendite vaatlemisel ei kasutata koopiaid, samuti esineb puudusi tõendite jälgitavuses, metaandmete kajastamises ning korratavuse ja autentsuse tagamises.

Seega saadi vastus uurimisprobleemile – menetluses osalejate poolt esitatud digitaalsete tõendite korrektseks ja usaldusväärseks vormistamiseks on eelkõige oluline järgida digitaalsete tõendite käitlemise põhimõtteid ning vormistada tõend sõltuvalt selle sisust kas asitõendina või dokumendina. Lisaks tuleb juhendada menetluses osalejat, et saada temalt tõend võimalikult autentsena. Võimalusel ja vajadusel tuleb kasutada digikriminalisti teenuseid.

Eeltoodule tuginedes saab öelda, et lõputööle seatud eesmärk sai täidetud. Töö tulemustest lähtuvalt toodi välja kolm ettepanekut. Esiteks, võiks korraldada Politsei- ja Piirivalveameti prefektuuride ja jaoskondade uurijatele digitaalsete tõendite teemalisi koolitusi, mida viiksid läbi prokurörid ja digikriminalistid ning mille eesmärk oleks luua ühtne arusaam digitaalsete tõendite käitlemisest. Teiseks, tuleks täiendada politseiteenistuse õppekava ning lisada õppekavasse suuremas mahus digikriminalistikaga seonduvaid loenguid ja praktilisi tunde, mis annaksid hariduse omandajale vajalikud teadmised ja oskused, et tulevikus töötades korrektselt ja usaldusväärselt digitaalsete tõenditega ümber käia. Kolmandaks, tuleks luua digitaalsete tõendite käitlemise juhend, mis on suunatud uurijatele – eesmärk on tagada võimalikult korrektne ja usaldusväärne tõendite käitlemine ka sellisel juhul, kui digikriminalisti toimingutesse ei kaasata.

Käesoleva lõputöö praktiline väärtus seisneb põgusas ülevaates, mis anti Põhja prefektuuri digitaalsete tõendite vormistamisega seonduvast menetluspraktikast. Töö

tulemusi võib arvesse võtta näiteks Politsei- ja Piirivalveameti tulevaste koolituskavade planeerimisel ja politseiteenistuse õppekava arendamisel. Laiema ülevaate saamiseks teeb lõputöö autor ettepaneku digitaalsete tõenditega seonduvat tulevikus uurida ka teiste prefektuuride ja üksuste vaates. Võimalusel tasub digitaalsete tõendite käitlemisega seonduvat uurida laiemalt, mitte ainult vormistuslikust aspektist. Ühtlasi pakuks lisaväärtust erinevate koolitusvõimaluste teemaline uuring digitaalsete tõendite kontekstis, et toetada menetluspraktika arengut Politsei- ja Piirivalveametis.

SUMMARY

The thesis is written on the topic „Formalisation of Digital Evidence Submitted by Persons Participating in the Proceedings in North Prefecture“. The thesis is written in Estonian and contains an English summary. The research consists of 48 pages. There has been used 53 different sources of which 27 are in Estonian and 26 are in English.

The aim of this research was to find out the principles and problems about the formalisation of digital evidence submitted by the persons participating in the proceedings and make proposals to improve the situation. The research problem was raised as a question: how to correctly and reliably formalise digital evidence submitted by the persons participating in the proceedings. In order to achieve this goal, three research questions were asked: what is digital evidence; how do persons participating in the proceedings submit digital evidence; what kind of problems may occur while formalising digital evidence.

Three research tasks had been set up to achieve the goal. Firstly, to analyse theoretical starting points and legal issues about the nature and formalisation of digital evidence. Secondly, to analyse criminal cases about Penal Code § 157^3 (harassing pursuit) that had been proceeded by North Prefecture to find out problems that might have been occured while formalising digital evidence. Thirdly, to make conclusions and proposals based on theory and research results to harmonise procedural practice. There was conducted a qualitative empirical study. Document analysis was used as data collection method and the method of data analysis was qualitative content analysis.

The results of research revealed that there can be many different digital evidence in one specific criminal offence. There were different digital evidence such as as text messages, e-mails, video recordings, audio recordings, photos, phone logs, web page posts etc. There were some problems with the formalisation of digital evidence. In some cases, the chain of custody was incomplete. There were also problems with ensuring repeatability, reliability and forensic soundness because no forensic copy was used. In some cases, there were problems with reflecting the inspection. In conclusion, based on theory and research results it is possible to bring out how to formalise digital evidence submitted by parties to proceedings correctly and reliably. It is important to follow the principles of handling digital evidence – the chain of custody, repeatability, authenticity and forensic soundness.

Based on the results, three proposals were made to harmonise procedural practice. Firstly, it is important to organise trainings for investigators on handling of digital evidence – trainings could be conducted by digital forensic specialists and prosecutors and the aim of the trainings would be to ensure reliable and correct formalisation of digital evidence even in these kind of situations where investigator does not involve digital forensic speacialist.

Secondly, it is important to improve curriculum of the police service and add lectures and practical lessons related to the digital forensics. The goal is that new police officers would already have basic knowledge and skills to ensure correct and reliable handling of digital evidence.

Thirdly, in addition to the manual for handling digital evidence, which has already been created for digital forensic specialists, an official manual for investigators should also be created to ensure the correct and reliable formalisation of digital evidence even if investigator does not involve digital forensic speacialist in the proceedings. If these proposals and the aspects of formalising digital evidence (which were mentioned before) are considered, the digital evidence can be formalised correctly and reliably.

VIIDATUD ALLIKATE LOETELU

Alas, M., 2013. *Digitaalsete tõendite kogumine ja käitlemine internetis toimepandud autoriõiguste rikkumiste menetlemisel. Lõputöö.* Muraste: Sisekaitseakadeemia.

Ali, M., Ismail, A., Elgohary, H., Darwish, S. & Mesbah, S., 2022. A Procedure for Tracing Chain of Custody in Digital Imange Forensics: A Paradigm Based on Grey Hash and Blockchain. *Symmetry*, 14(2).

Bellasio, J., Silfversten, E., Leverett, E., Knack, A., Quimbre, F., Blondes, E. L., Favaro, M. & Paoli, G. P., 2020. *The Future of Cybercrime in Light of Technology Developments.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/media/300/download [Kasutatud 18.10.2022].

Blažič, J. & Klobučar, T., 2020. Investigating crime in an interconnected society: will the new and updated EU judical environment remove the barriers to justice? *International Review of Law, Computers & Technology*, 34(1), pp. 87–107.

Bowen, G., 2009. Document Analysis as a Qualitative Research Method. *Qualitative Research Journal*, 9(2), pp. 27–40.

Buzarovska Lazetik, G. & Koshevaliska, O., 2013. Digital Evidence in Criminal Procedures -A Comparative Approach-. *Balkan Social Science Review*, 2, pp. 63–82.

Casey, E., 2011. *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet.* Amsterdam: Elsevier Academic Press.

Cole, M. D. & Quintel, T., 2018. Transborder Access to e-Evidence by Law Enforcement Agencies. *University of Luxembourg Law Working Paper*, 2018-010, pp. 1–20.

Ćosić, T., Motyka, V., Raspor, M., Sajid, S., Devrnja, N., Dobrev, P. & Ninković, S., 2022. Comprehensive Phytohormone Profiling of Kohlrabi during In Vitro Growth and Regeneration: The Interplay with Cytokinin and Sucrose. *Life*, 12(10).

De Busser, E., 2018. The Digital Unfitness of Mutual Legal Assistance. *Security & Human Rights*, 28(1-4), pp. 161–179.

Euroopa Komisjon, 2019. *Recommendation for a council decision authorising the opening of negotiations in view of an agreement between the European Union and the United States of America on cross-border access to electronic evidence for judicial cooperation in criminal matters.* [Võrgumaterjal] Leitav: https://commission.europa.eu/system/files/2019-02/recommendation_council_decision_eu_us_e-evidence.pdf [Kasutatud: 24.10.2022].

Europol, 2021. *Serious and organised crime threat assessment.* [Võrgumaterjal] Leitav: https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf [Kasutatud 18.10.2022].

Graves, M. W., 2014. Digital Archaeology: The Art and Science of Digital Forensics. Michigan: Addison-Wesley.

Hannon, M. J., 2014. An Increasingly Important Requirement: Authentication of Digital Evidence. *Journal of the Missouri Bar*, 70(6), pp. 314–323.

Hirsjärvi, S., Remes, P. & Sajavaara, P., 2004. *Uuri ja kirjuta*. Tallinn: Kirjastus Medicina.

Hsieh, R., 2023. Digital (Multimedia) Evidence and Computer Forensics – A Holistic View. *Forensic Science Review*, 35(1), pp. 8–13.

Johnson, T. A., 2006. *Forensic Computer Crime Investigation*. Boca Raton: CRC Press.

Justiitsministeerium, 2015. Kriminaalmenetlusõiguse revisjoni lähteülesanne. [Võrgumaterjal] Leitav: https://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf [Kasutatud: 23.10.2022].

Kalmus, V., Masso, A. & Linno, M., 2015. *Kvalitatiivne sisuanalüüs*. [Võrgumaterjal] Leitav: http://samm.ut.ee/kvalitatiivne-sisuanalyys [Kasutatud 10.11.2022]

Kasper, A. & Laurits, E., 2016. Challenges in Collecting Digital Evidence: A Legal Perspective. Rmt: T. Kerikmäe & A. Rull, toim-d. *The Future of Law and eTechnologies*. Cham: Springer, pp. 195–233.

Kergandberg, E. & Pikamäe, P., 2012. *Kriminaalmenetluse seadustik. Kommenteeritud väljaanne.* Tallinn: Juura.

Kergandberg, E., 2013. Eesti kriminaalmenetlus: mõned rindeteated. *Juridica*, 2013(4), lk 249–256.

Kriminaalasi A.P. (P.) süüdistuses KarS § 120 järgi (2009) 3-1-1-5-09

Kriminaalasi K. K. süüdistuses KarS § 184 lg 2^1 ja M. R-i süüdistuses KarS § 184 lg 2 p-de 1 ja 2 järgi (2022) 1-20-1208.

Kriminaalasi L. H. Süüdistuses KarS § 118 p-de 1, 2 ja 3 järgi (2006) 3-1-1-142-05

Kriminaalasi T. T. Süüdistuses KarS § 266 lg 1, § 257 ja § 323 järgi (2005) 3-1-1-104-05

Kriminaalmenetluse seadustik (2003) RT I, 22.12.2021, 45.

Krotoski, M. L., 2011. Effectively Using Electronic Evidence Before and at Trial. *Obtaining and Admitting Electronic Evidence*, 59(6), pp. 52–71.

Kurm, M., 2016. *Tõendite kogumisel dubleerimise vältimine kohtu- ja kohtueelses menetluses.* [Võrgumaterjal] Leitav: https://www.just.ee/media/1232/download [Kasutatud: 21.01.2023].

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

Lall, A., Tohter, M. & Öpik, R., 2021. Some Aspects of Digital Forensics in the Republic of Estonia. *17. Medzinárodný Kongres Kriminalistika A Forenzné Vedy: Veda, Vzdelávanie, Prax*, pp. 133–146.

Laurits, E., 2015. Mõned probleemid arvutisüsteemi läbiotsimisel. Rmt: A. Parmas, P. Randma, S. Laos, T. Lillsaar, J. Kallin, S. Lind, I. Tamm, M. Mõttus, M. Metslaid & L. Lomp toim-d. *Kohtute aastaraamat 2015*. Tallinn: Dada, lk 135–151.

Lopez, E. M., Moon, S. Y. & Park, J. H., 2016. Scenario-Based Digital Forensics Challenges in Cloud Computing. *Symmetry*, 8(10).

Luuk, M., 2017. *Digitaalsete tõendite kasutamise erisused. Magistritöö.* Tartu: Tartu Ülikool.

Olber, P., 2021. The Impact of Computer Forensics on Polish Criminal Procedure Development. *17. Medzinárodný Kongres Kriminalistika A Forenzné Vedy: Veda, Vzdelávanie, Prax*, pp. 158–167.

Olle Koki (Kokk) kriminaalasi süüdistuses KarS § 141 lg 1 järgi (2009) 3-1-1-21-09.

Osula, A.-M., 2017. Täidesaatev jurisdiktsioon ja piiriülene kaugläbiotsimine. *Juridica*, 2017(8), lk 559–566.

Patton, M. Q., 2002. Qualitative Research & Evaluation Methods. Thousand Oaks: Sage Publications.

Politsei- ja Piirivalveamet, 2022. *Digitaalsete tõendite käitlemise juhend*.

Prayudi, Y. & SN, A., 2015. Digital Chain of Custody: State of the Art. *International Journal of Computer Applications*, 114(5).

Prokuratuur, 2017. *Arvamus kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõule (KrMS revisjon)*.

[Võrgumaterjal] Leitav: https://www.just.ee/media/1371/download [Kasutatud: 20.10.2022].

Prokuratuur, 2018. *Menetlusökonoomia põhimõtted*. [Võrgumaterjal] Leitav: https://www.prokuratuur.ee/et/menetlusokonoomia-pohimotted [Kasutatud: 28.01.2023].

Raudsepp, G., 2018. *Digitaalsete tõendite kogumise ja kasutamise perspektiivikus kriminaalmenetluses. Magistritöö.* Tartu: Tartu Ülikool.

Riigikogu, 2001. *Arvutikuritegevusvastane konventsioon. Välisleping. RT II 2003, 9, 32*.

Savona, E. U., & Mignone, M., 2004. The Fox and the Hunters: How IC Technologies Change the Crime Race. *European Journal on Criminal Policy and Research*, 10(1), pp. 3–26.

Siseministeerium, 2021. *Siseturvalisuse arengukava 2020–2030.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/media/748/download [Kasutatud 17.10.2022].

Tara, H. & Mishra, A., 2021. A Comparative Study of Digital Forensic Tools for Data Extraction From Electronic Devices. *Journal of Punjab Academy of Forensic Medicine & Toxicology*, 21(1), pp. 97–104.

Tartu Ülikool, 2013. *Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses*. [Võrgumaterjal] Leitav: https://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/analuus_isikute_pohioiguste_tagamisest_ja_eeluurimise_kiirusest_kriminaalmenetluses.pdf [Kasutatud 17.10.2022].

Tehver, J., 2016. *Digitaalsete tõendite kasutamise võimaldamine*. [Võrgumaterjal] Leitav: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf [Kasutatud: 17.10.2022].

Valjarevic, A. & Venter, H. S., 2015. A Comprehensive and Harmonized Digital Forensics Investigation Process Model. *Journal of Forensic Sciences*, 60(6), pp. 1467–1483.

Õunapuu, L., 2012. *Valimid kvantitatiivsetes ja kvalitatiivsetes uurimustes.* Tartu Ülikool. [Võrgumaterjal] Leitav *:* https://dspace.ut.ee/bitstream/handle/10062/27764/index.html [Kasutatud: 10.11.2022].

Õunapuu, L., 2014. *Kvalitatiivne ja kvantitatiivne uurimisviis sotsiaalteadustes*. Tartu Ülikool. [Võrgumaterjal] Leitav: http://dspace.ut.ee/bitstream/handle/10062/36419/ounapuu_kvalitatiivne.pdf [Kasutatud 09.01.2023].

Ühinenud Rahvaste Organisatsiooni Peaassamblee, 2022. *Compilation of Proposals and Contributions Submitted by Member States on the Provisions on Criminalization, the General Provisions and the Provisions on Procedural Measures and Law Enforcement of a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.* [Võrgumaterjal] Leitav: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Second_session/Documents/V22_1AC.pdf [Kasutatud 04.01.2023].

TABELITE JA JOONISTE LOETELU