Sisekaitseakadeemia
Sisejulgeoleku instituut

Rando Savitski

AVALIKE ANDMETE KASUTAMINE KRIMINAALMENETLUSES

Magistritöö

Juhendaja:
Anu Baum, MA
Kaasjuhendaja:
Jaanika Puusalu, PhD

Tallinn 2023

MAGISTRITÖÖ ANNOTATSIOON

Sisejulgeoleku instituut	Juuni 2023
Töö pealkiri eesti keeles: „Avalike andmete kasutamine kriminaalmenetluses“.	
Töö pealkiri võõrkeeles: „Open source data use in criminal proceedings“	
Magistritöö eesmärgiks on leida lahendused, kuidas avalike andmete kasutamine muudab efektiivsemaks kriminaalmenetlusi. Töö eesmärgi saavutamiseks püstitati neli uurimisülesannet: analüüsida teaduskirjanduse abil, mis on avalikud andmed ning kuidas neid kogutakse ja analüüsitakse; analüüsida avalike andmete kasutamise õiguslikke piiranguid kriminaalmenetluse vaates; viia läbi kvalitatiivne uuring ekspertide seas leidmaks kitsaskohti ja võimalikke lahendusi, kuidas avalikke andmeid kriminaalmenetlustes kasutada; teaduskirjanduse ja empiirilise uuringu analüüsi tulemusi sünteesides esitada ettepanekud avalike andmete kasutamise rakendamiseks kriminaalmenetlustes. Magistritöös kasutati kvalitatiivset uurimisviisi, kus andmekogumise meetodiks oli poolstruktureeritud ekspertintervjuud. Kvalitatiivse sisuanalüüsi teostamiseks kasutati andmeanalüüsiprogrammi NVivo 1.7. Magistritöö tulemusena selgus avalike andmete kasutamise praegune praktika ning samuti avalike andmete kasutamise kitsaskohad kriminaalmenetlustes. Nende põhjal tegi magistritöö autor rakendatavaid ettepanekuid. Lisaks toodi ära võimalikud edasised uurimissuunad.	
Lisad: puuduvad	
Võtmesõnad: avalikud andmed, kriminaalmenetlus	
Võõrkeelsed võtmesõnad: *OSINT, OSINT in criminal proceedings, OSINT investigation*	
Säilitamise koht: Sisekaitseakadeemia raamatukogu	
Töö autor: Rando Savitski	
Olen koostanud magistritöö iseseisvalt. Kõik magistritöö koostamisel kasutatud teiste autorite tööd, seisukohad, kirjalikest allikatest ja mujal allikates saadud info on nõuetekohaselt viidatud. Olen nõus oma magistritöö avaliku osa avaliku ligipääsuga avaldamisega elektroonilises keskkonnas.	
Allkiri: /allkirjastatud digitaalselt/	Kommentaar (soovi korral)
Vastab magistritöö nõuetele	
Juhendaja: Anu Baum	Allkiri: /allkirjastatud digitaalselt/
Kaasjuhendaja: Jaanika Puusalu	Allkiri: /allkirjastatud digitaalselt/
Kaitsmisele lubatud	
Kolledži direktor/instituudi juhataja: Erkki Koort	Allkiri: /allkirjastatud digitaalselt/

SISUKORD

MÕISTETE JA LÜHENDITE LOETELU

***Bayesi* teoreem** – kirjeldab sündmuse tõenäosust tuginedes eelnevale teadmisele sündmustest, mis võivad olla sündmusega seotud (Joyce, 2003).

CEPOL – *European Union Agency for Law Enforcement Training* (ingl k) – Euroopa Liidu Õiguskaitsekoolituse Amet.

CIA – *Central Intelligence Agency* (ingl k) – Luure Keskagentuur Ameerika Ühendriikides.

Darknet – Tumeveeb, mille kasutamiseks on vajalik kasutada eritarkvara ning võimaldab kasutajatel jääda anonüümseks (Graham & Pitman, 2020, p. 594).

EIK – Euroopa Inimõiguste Kohus.

EUROPOL – *European Police Office* (ingl k) Euroopa Politseiamet.

Googeldama = guugeldama – Google'i otsimootori abil internetist millegi kohta infot otsima (Sõnaveeb, 2022).

Google Dorking = Google hacking – Google häkkimine, on meetod, mis suudab leida lihtsate otsingupäringute abil raskesti leitavat teavet, pakkudes otsingustringe, mis kasutavad täpsema otsingu meetodit (Medewar, 2023).

GDPR –*General Data Protection Regulation* (ingl k) **–** 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).

GEOINT – *Geospatial Intelligence* (ingl k) **–** georuumilise info (sh kujutised) ja muude luureandmete lõimimisel saadav luureteave, mis kirjeldab, hindab ja kujutab visuaalselt geograafiliste orientiiridega tegevusi ja füüsilise keskkonna omadusi. (Militerm, 2022a).

HUMINT – *Human intelligence* (ingl k) – inimallikalt laekunud teave. (Office of the Director of National Intelligence, 2022).

IKT – info- ja kommunikatsioonitehnoloogia.

IMINT – *Imagery Intelligence* (ingl k) – pilt- või kujutisluure, mis on reprodutseeritud elektrooniliselt või optiliste vahenditega filmil, elektroonilistel kuvaritel või muul andmekandjal (Office of the Director of National Intelligence, 2022).

IMSI – *International Mobile Subscriber Identity* (ingl k) **–** Rahvusvaheline mobiiliabonendi tunnus, on rahvusvaheliselt standarditud unikaalne number mobiiliabonendi tuvastamiseks (Euroopa Komisjon, 2022a).

IMSI-catcher – *International Mobile Subscriber Identity catcher* (ingl k) – Rahvusvahelise mobiiliabonendi tunnuse püüdja – tehnoloogiline seade, mille abil on võimalik teatud piirkonnas töötavate ja signaale vastuvõtvate mobiiltelefonide jälgida ning teha kindlaks nende asukohta (Phantom Technologies, 2023).

Office of the Director of National Intelligence – Ameerika Ühendriikide Rahvusliku Luure Direktoraadi kantselei (Office of the Director of National Intelligence, 2023)

OSINT – *Open Source Intelligence Techniques* (ingl k) – Andmed, mis on kogutud avalikult kättesaadavatest allikatest ja mida kasutatakse luurekontekstis.

KrMS – Kriminaalmenetluse seadustik.

MASINT – *Measurement and Signature Intelligence* (ingl k) – luureteave, mis on saadud anduritelt kogutud andmete teaduslikul ja tehnoloogilisel analüüsimisel ning mille eesmärk on tuvastada allika, emitteri või saatja erijooni ja hõlbustada seeläbi nende mõõtmist ja tuvastamist (Militerm, 2022b).

PPA – Politsei- ja Piirivalveamet.

SIGINT – *Signal Intelligence* (ingl k) – Signaalluure ehk erinevate signaalide pealtkuulamine: kogu sideluure, elektrooniline luure ja välismaiste instrumentide signaalide luure (Office of the Director of National Intelligence, 2022).

Social Engineering – inimeste psühholoogiline manipulatsioon vajalike andmete või juurdepääsu saamiseks (Anderson, 2008, p. 18).

SISSEJUHATUS

Interneti kasutamine on tänapäeval saanud lahutamatuks osaks meie igapäevasest elust. Digitaaltehnoloogia on plahvatuslikult kasvanud ning selle kasutamine on globaliseerunud. See tähendab, et suur osa inimkonnast on kasutusele võtnud erinevad nutiseadmed, tänu millele on neil juurdepääs sotsiaalvõrgustikele, erinevale teabele ning meelelahutusele (Economic Commission for Latin America and the Caribbean, 2021, p. 7). Uuringute järgi kasutab noorem põlvkond peamiselt internetti sotsiaalseteks tegevusteks ning meelelahutuseks (Dogruer, *et al.,* 2011, p. 607). Lisaks on võimalik internetti kasutada veel mitmel erineval moel, näiteks uudiste lugemiseks, informatsiooni otsimiseks, ostude tegemiseks, e-posti lugemiseks. Iga kord, kui internetti kasutada, jääb sellest maha mitmeid digitaalseid jälgi. Digitaalseid jälgi, mida me internetti maha jätame, saab liigitada aktiivseteks (andmed, mida me ise sisestame internetis: sotsiaalmeedia postitused, saadetud e-kirjad ja küpsiste tingimustega nõustumised) ja passiivseteks (andmed, mida me jätame maha enda tahtest sõltumata: IP aadressid, asukoha informatsioon fotodel või küpsised, mida veebilehekülje meie seadmetele saadavad) (Mayda, 2022, p.1034).

Õiguskaitseasutused saavad oma töös kasutada erinevaid riiklikke andmebaase, et saada infot kuriteo toimepannud isikute ja teiste kriminaalmenetlust läbivate isikute kohta. Kuritegude uurimise puhul on oluline järgida kriminaalmenetluse seadustikku, et kogutud tõendid oleksid saadud seaduslikult. Kriminaalmenetluse seadustiku (edaspidi: KrMS) § 62 sätestab, et tõendamiseseme asjaoludeks on kuriteo toimepanemise aeg, koht ja viis ning muud kuriteo tehiolud. Lisaks on tõendamisesemeks kuriteokooseis, kuriteo toimepannud isiku süü ning kuriteo toimepannud isikut iseloomustavad andmed ja muud tema vastutust mõjutavad asjaolud. Tõendiks on kriminaalmenetluseseadustiku järgi kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu-, kohtuistungi- ja jälitustoimingu protokoll või videosalvestis. Samuti on tõendiks muud dokumendid ning foto(d) või film(id) või muu teabetalletus. Tõendite kogumisel on oluline jälgida, et tõendeid kogutakse viisil, mis ei riiva kogumises osaleja au ja väärikust, ei ohusta tema elu või tervist ega tekita põhjendamatult varalist kahju. (Kriminaalmenetluse seadustik[1], 2003)

Interneti ja seal olevate andmete puhul on oluline, et ka õiguskaitseasutused oskaksid neid enda jaoks õigesti ära kasutada. Üheks võimalikuks viisiks koguda tõendeid kriminaalmenetluses, on võimalus koguda andmeid ja tõendeid kuriteo toimepanija kohta avalikult kättesaadavatest allikatest ehk inglise keeles *Open Source Intelligence Techniques* (edaspidi: *OSINT*) meetodil. *OSINT* andmed on sisuliselt kõik andmed, mida on võimalik kõigil inimestel avalikult internetis koguda.

Riiklikest võimalustest erinevad *OSINT* meetodil kogutud andmed eelkõige selle poolest, et riigi enda poolt kogutud andmed moodustavad kogumi erinevatest riiklikest registritest, näiteks Kinnistusraamat, Äriregister, Rahvastikuregister jne. Samuti on riigil olemas andmed, mida inimesed on neile ise andnud näiteks dokumente taotledes. Ametniku poolt erinevaid päringuid tehes on kriminaalmenetluse raames võimalik teada saada andmeid isikute kohta, mis on olemas eraettevõtjatel, näiteks panga päringud ja päringud erinevate kliendikaartide kasutamise kohta. Oluline on siinkohal välja tuua, et ametniku võimalused kriminaalmenetluse raames andmeid kätte saada piirduvad enamasti riigi territooriumiga. Väljaspool riigi territooriumit asuvaid andmeid on võimalik päringutega kätte saada ainult sellisel juhul, kui andmete valdajaja/omanik neid vabatahtlikult väljastab või tehes õigusabi taotluse teise riiki lootuses, et teine riik sellele vastab. *OSINT* puhul on andmed avalikult internetist kättesaadavad, näiteks kui inimene lisab müügikuulutuse portaali, siis on võimalik kõigil saada kätte kuulutuses loetletud andmed, hoolimata selle portaali keelest, asukohast jms.

Käesolev magistritöö tegeleb eelkõige kriminaalmenetlusliku probleemi lahendamisega. Kriminaalmenetlused, olenevalt menetlusest, on oma olemuselt mahukad ja keerulised ning hõlmavad endas mitmeid erinevaid toiminguid ning päringuid, mille tegemine võib võtta palju ajalist ressurssi ning veel rohkem võib aega võtta päringute vastuste ootamine. Kriminaalmenetluses on tihti kriminaalmenetluslikud protseduurid omavahel ajalises sõltuvuses s.o on vaja teha mitmeid teineteisele järgnevaid omavahel sõltuvuses olevaid päringuid vajalike andmete saamiseks. Kriminaalmenetluse eesmärgiks on teha kindlaks kuriteo toimepanemise fakt ning kui see on leidnud kinnitust, on oluline selgeks teha, kas on piisavalt tõendeid kahtlustatavale süüdistuse esitamiseks (European e-justice, 2023).

Kriminoloogid on leidnud, et kuritegevus on kui sotsiaalne fenomen, kus isikut mõjutavad tema individuaalsed isikuomadused, aga ka sotsiaalsed tegurid nagu inimsuhted ja elukeskkond (Siegel, 2010, p. 4). Nende tegurite kindlaks tegemiseks on vajalik vaadelda laiemat pilti, mis tähendab, et on vajalik kindlaks teha ka võimalike kahtlustatavate käitumine digitaalmaailmas. *OSINT* meetod annab võimaluse koguda tõendeid ning leida kriminaalmenetluseks vajalikke andmeid kiiremini sh aitab leida keskkondi, kuhu teha päringuid, mis annab võidu kriminaalasja kohtueelsele uurimisele kuluvas ajas ja järgib menetlusökonoomika põhimõtteid.

Sisejulgeolekualaselt seisneb magistritöö aktuaalsus selles, et avalike andmete kasutamine võimaldab tõhusamalt läbi viia kohtueelset uurimist digitaliseerinud ühiskonnas. Kuritegevuse, eriti organiseeritud kuritegevuse ja raske peitkuritegevuse olemus on muutumises (Siseministeerium, 2021, lk 29). Kurjategijad orienteeruvad kiiresti ümber vähem tulusamalt valdkonnalt tulusamatele valdkondadele, võttes seejuures kasutusele uusi tehnoloogiaid, mis mitmekesistavad nende võimalusi (Siseministeerium, 2021, lk 29). Nende võimalustena saab välja tuua uudsed viisid suhtlemiseks, aga ka tumeveebi kasutamise kuritegude toimepanemiseks. Selleks, et kurjategijatega sammu pidada, peavad õiguskaitseasutused käima ajaga kaasas ning võtma kasutusele uusi võimalusi kuritegude ennetamiseks, tõendamiseks ja avastamiseks. Siseturvalisuse arengukava aastateks 2020–2030 seab eesmärgiks, et siseturvalisuse tagamisel ollakse uuendusmeelsed, kasutatakse tarku ja innovaatilisi lahendusi (Siseministeerium, 2021, lk 17). *OSINT* meetodi kasutamine on uudne, tark ja innovaatiline võimalus, kuidas koguda andmeid kuritegude ja kurjategijate kohta. Samuti näeb Politsei- ja Piirivalveameti (edaspidi: PPA) strateegia 2030 ette, et võitluses raske peitkuritegevusega arendatakse analüüsivõimekust kasutades digiteerimisest ning sotsiaalmeedia levikust tulenevaid võimalusi, lisaks rakendatakse sihistatud teabe kogumist nii avalikest, kui ka varjatud allikatest (Politsei- ja Piirivalveamet, 2019, lk 32).

Lisaks saab välja tuua magistritöö teema olulisuse selles, et Euroopa Inimõiguste kohus (edaspidi: EIK) on hakanud piirama andmete kogumisi ja kogutud andmete väljastamist, mida on siiani kriminaalmenetlustes laialdaselt kasutatud. Selline EIKi ja ka Eesti Riigikohtu viimaste aegade suundumus suurendab veelgi antud magistritöö teema olulisust ja aktuaalsust, sest *OSINT* vahendite abil kogutavad andmed võimaldavad leida

uusi lahendusi kuritegude efektiivseks avastamiseks. Näitena saab välja tuua olukorra, kus riigikohus on leidnud, et sideettevõtjalt saadud andmete protokollid pole lubatavad tõendid, kui vastava loa andmete küsimiseks on välja andnud prokuratuur, mis kuni Riigikohtu otsuseni oli tavapärane praktika (H.K. kriminaalasi karistusseadustiku § 199 lg 2 p 5, 8, 9, § 213 lg 2 p 1, § 323 lg 1 järgi, 2021). Riigikohus viitab oma otsuses Euroopa Kohtu (2021) eelotsusele C-746/18, milles juhitakse tähelepanu, et vastava loa andmete küsimiseks peab andma kohus või sõltumatu haldusasutus, kuid prokuratuur, kes juhib kohtueelset menetlust ja esindab vajadusel riiklikku süüdistust ei ole kriminaalmenetluses neutraalne. Kohtud juhivad lahendites tähelepanu probleemile, et sideettevõtjatelt küsitakse välja liiga paljusid andmeid ning nende andmete järgi võib isiku põhiõiguste riive olla põhjendamatult suur arvestades konkreetset kriminaalmenetlust. Näiteks telefonikõne tegemisel salvestub sidemasti asukoht, millega on mobiiltelefon parasjagu ühenduses ning selle järgi on võimalik teha kindlaks millises piirkonnas isik kõne tegemise hetkel oli.

Sideettevõtjalt saadud andmete protokollid ehk kõnekeeles „kõnede eristused“ on siiani olnud kriminaalmenetlustes laialdaselt kasutuses võitluses raske kuritegevuse vastu. Sageli on aidanud kõnede eristus kinnitada kahtlustavate seotust sündmusega. Samuti on aidanud võimalikul kahtlustataval pääseda kahtlustusest, kuna kõnede eristus kinnitab isiku ütlusi, et sel võimalikul perioodil viibis isik teises piirkonnas ning suhtles ja kohtus teiste inimestega. Nüüd saab loa sideettevõtjatelt andmete küsimiseks välja anda kohus. Menetlusliku poole pealt tähendab see seda, et menetleja esitab kõnede eristuse saamiseks põhjendatud taotluse prokurörile, kes vaatab taotluse üle ning kui see on põhjendatud, siis esitab prokurör enda koostatud põhjendatud taotluse kohtule. Kohtunik omakorda hindab saabunud taotluse sisu ning teeb otsuse, kas prokuröri taotlus on põhjendatud või mitte ning seejärel võtab vastu otsuse kas väljastada luba või mitte. Iga lisalüli kriminaalmenetluses muudab selle riigile kallimaks ning pikendab menetlemisele kuluvat aega.

Seega võib avalike andmete kasutamine olla üheks uueks ja innovaatiliseks meetodiks, mis võib täiendada tekkivat tühimikku ning luua uusi võimalusi tõendite ja informatsiooni kogumiseks kriminaalmenetlustes. Lisaks võib see muuta kriminaalmenetlusi kiiremaks ja efektiivsemaks, mis teeb menetluse riigile odavamaks.

Magistritöö **uudsus** seisneb ennekõike selles, et autorile teadaolevalt pole varasemalt Eestis sellisel teemal magistritööd kirjutatud ega ka sellises võtmes teemat uuritud. See oleks Eestis esmakordne uurimine ning arvestades avalikus veebis olevat informatsiooni kogust, ka vajalik. Varasemalt on Tallinna Tehnikaülikooli Infotehnoloogia teaduskonnas tehtud magistritöö „Huvide konflikti tuvastamine tuginedes avaandmetele nelja kohaliku omavalituse näitel“, kus magistritöö autor Kristo Kiipus jõudis tulemuseni, et avalikke andmeid kasutades on asjakohaste IT-lahenduste toel võimalik automaatselt tuvastada huvide konflikti- ja korruptsiooniolukordi kohalike omavalitsuste tegevustes (Kiipus, 2018).

Käesoleva magistritöö keskne **uurimisprobleem** on: kuidas on võimalik kasutada avalikke andmeid kriminaalmenetlustes tõhusamalt ja rohkem?

Uurimisprobleemist tulenevalt püstitati järgmised **uurimisküsimused**:

1) Millised andmed on avalikud andmed?
2) Milline on praegune praktika avalike andmete kogumisel, analüüsimisel ja vormistamisel kriminaalmenetlustes?
3) Kuidas on võimalik avalikke andmeid kasutada kriminaalmenetluses ning millist lisaväärtust annab nende kasutamine kriminaalmenetlusele?
4) Millised õiguslikud piirangud on avalike andmete kasutamisel kriminaalmenetlustes?

Magistritöö **eesmärgiks** on leida lahendused, kuidas avalike andmete kasutamine muudab efektiivsemaks kriminaalmenetlusi. Eesmärgi saavutamiseks on püstitatud järgmised **uurimisülesanded:**

1) Analüüsida teaduskirjanduse abil, mis on avalikud andmed ning kuidas neid kogutakse ja analüüsitakse.
2) Analüüsida avalike andmete kasutamise õiguslikke piiranguid kriminaalmenetluse vaates.
3) Viia läbi kvalitatiivne uuring ekspertide seas leidmaks kitsaskohti ja võimalikke lahendusi, kuidas avalikke andmeid kriminaalmenetlustes kasutada.
4) Teaduskirjanduse ja empiirilise uuringu analüüsi tulemusi sünteesides esitada ettepanekud avalike andmete kasutamise rakendamiseks kriminaalmenetlustes.

Magistritöö raames viiakse läbi empiiriline uuring, mille eesmärgi saavutamiseks kasutatakse **kvalitatiivset uurimisviisi**. Kvalitatiivne uurimisviis võimaldab läbi viia intervjuusid, vaatlusi ning dokumentide tõlgendusi, mis annavad võimaluse leida mustreid ja teemasid erinevate käitumiste selgitamistel (Patton, 2015, p. 48). Empiirilise uuringu raames kogutakse andmeid tegelike nähtuste ja fenomenide kohta. Arvestades, et magistritöö on seotud kriminaalmenetluse valdkonnaga, siis uurimuses kasutatakse eesmärgistatud valimi (ingl k *Purposive Sampling)* põhimõtteid (Teddlie & Yu, 2007, p. 80; Neuman, 2014, pp. 273–274).

Kvalitatiivse uuringu valim koosneb oma ala ekspertidest, kes on oma igapäevatöös kasutanud *OSINT*it ning nendega viidi läbi poolstruktureeritud ekspertintervjuud (Flick, 2014, pp. 212-213). Poolstruktureeritud intervjuu küsimused koostati magistritöö teoreetilise osa ja uurimisküsimuste põhjal, mille eesmärgiks on ekspertide poolt antud vastusest saada vastused uurimisküsimustele 2 ja 3.

Magistritöö koosneb kahest peatükist. Esimeses peatükis määratletakse avalike andmete mõiste ja olemus ning andmete kogumise ja analüüsi vajadus ning nende õiguslikud alused. Vaadeldakse teoreetilist poolt, milles analüüsitakse teadusartiklites ja teoreetilises kirjanduses välja toodud võimalusi. Teadusartiklite ja teoreetilise kirjanduse leidmiseks kasutati EBSCO, SAGE, Taylor & Francis ja ResearchGate andmebaase. Andmebaasides kasutati otsingusõnu: *OSINT, OSINT investigation, OSINT+LEA, Digital Forensics, OSINT+police, big data forencsics, big data*. Kohtulahendite otsimiseks kasutati Riigi Teataja kohtulahendite otsingusüsteemi, kus märksõnadeks olid: jälitustegevus, jälitustoimingud, politseiagent, tõendi lubatavus.

Teises peatükis keskendutakse empiirilisele uuringule, tutvustatakse metodoloogiat ning leitakse vastuseid uurimisküsimustele. Empiirilise uuringu käigus viiakse läbi poolstruktureeritud ekspertintervjuud ja uurimisküsimustele vastuste saamiseks analüüsitakse neid. Teoreetilise peatüki ja empiirilise uuringu analüüsist ning sünteesist lähtudes pakutakse välja võimalikke lahendusi, kuidas kriminaalmenetlusi menetlevatel ametnikel on võimalik avalikke andmeid kasutada, et kriminaalmenetlused oleksid efektiivsemad.

Käesoleva magistritöö uuringu ja analüüsi tulemusena valmib ülevaade avalike andmete kogumisest, nende kasutamisest kriminaalmenetluses ning õiguslikest raamidest nende andmete kasutamiseks. Sellest magistritööst saavad kasu eelkõige õiguskaitseasutuste ametnikud, kes tegelevad kriminaalmenetlustega, saamaks juurde ideid, kuidas on võimalik avalike andmete kasutamisega oma tööd teha efektiivsemalt, integreerides seda praeguste praktikatega. Magistritöö autor soovib avaldada tänu oma juhendajatele Anu Baum ja Jaanika Puusalu, kes osutasid suurt tuge ja abi käesoleva töö õigeaegseks valmimiseks.

1. AVALIKE ANDMETE KASUTAMINE

Avalike andmete kasutamine võib olla üks olulistest komponentidest õiguskaitseasutuste töös, kui seda osata õigesti ära kasutada. Saadud andmed võivad aidata lahendada kuritegusid või tuvastada ning anda olulist informatsiooni kriminaalmenetlustes olulist rolli omavate isikute kohta. Samuti võivad avalikud andmed aidata näha saabuvaid trende ning olla sisendiks olukordade ja ohuhinnangute ülevaadete teostamiseks. Esimene peatükk tutvustab avalike andmete kasutamise võimaluste ja kitsaskohtade teoreetilist diskusiooni kriminaalmenetluse vaates.

Esimeses alapeatükis määratletakse, mida käesolevas töös mõistetakse avalike andmete all ning kuidas avalikud andmed on kujunenud oluliseks teabe hankimise võimaluseks. Alapeatükk on jaotatud kolmeks punktiks: esimeses punktis tuuakse välja avalike andmete kogumise ajalugu; teises punktis tuuakse välja, kuidas erasektoril on võimalik avalikke andmeid kasutada; kolmandas punktis selgitatakse, kuidas avalikud andmed sobivad kriminaalmenetlusse. Alapeatükis kasutatakse terminit *OSINT*, kuna tegemist on rahvusvaheliselt kasutatava lühendiga. Terminit *OSINT* kasutatakse avalike andmete sünonüümina. Teises alapeatükis antakse ülevaade avalike andmete kasutamisest julgeoleku vaates. Kolmandas alapeatükis saab ülevaate avalike andmete kogumisest kriminaalmenetlustes. Neljas alapeatükk keskendub sellele, millist kasu avalikest andmetest saavad õiguskaitseasutused. Viies alapeatükk annab õigusliku ülevaate avalike andmete kogumisest ja kasutamisest kriminaalmenetlusest, eelkõige sotsiaalmeediast andmete kogumisest ning andmelekete kasutamisest kriminaalmenetlustes. Kuuendas alapeatükis antakse ülevaade, kuidas on võimalik kasutada tehnoloogilisi vahendeid avalike andmete kasutamisel kriminaalmenetlustes.

1.1. Avalike andmete kujunemine oluliseks teabe hankimise võimaluseks

Peatüki eesmärgiks on anda ülevaade, kuidas avalikud andmed on kujunenud oluliseks teabe hankimise võimaluseks. Andmete all mõeldakse käesolevas magistritöös informatsiooni, mida on võimalik internetist koguda kõigil inimestel (Eesti Keele Instituut, 2023a). Inglise keelses kasutatakse andmete puhul, mis on kogutud avalikult

kättesaadavatest allikatest, terminit *OSINT* (ingl *Open Source Intelligence Techniques*). Eestis on defineeritud terminit *OSINT* andmekaitse ja infoturbe leksikonis, kui teabe kogumist ja tuletamist avalikest allikatest (Andmekaitse ja infoturbe leksikon, 2022).

Teaduslikus kirjanduses defineeritakse terminit *OSINT*t, kui andme kogumise meetodit, mis on saadud avalikult kättesaadavast teabest, mida kogutakse, analüüsitakse ja levitatakse õigeaegselt asjakohasele sihtrühmale konkreetse luureülesande täitmiseks (Johnson, 2007, p. 129; Schaurer & Ströger, 2013, p. 53; Williams & Blum, 2018, p. 8). Inglise keelses kirjanduses kirjeldatud *OSINT*t, ka kui protsessi, mis hõlmab endas nii era- kui ka avaliku sekotri käes olevaid avalikke allikaid ning lisaks erinevaid interneti ja sotsiaalmeedia keskkondi (Yeboah-Ofori & Brimicombe, 2017, p. 87). Termin *OSINT* võeti esmalt kasutusele luureagentuuride poolt.

OSINTi teostamisel on vaja pidada kinni kolmest kriteeriumist. Esimene neist on informatsioon, mis on jagatud kas isikute või organisatsioonide poolt avalikult, seda kas tasuta või tasuliselt (ajaleheartiklid, avalikud riiklikud registrid jne). Teiseks kriteeriumiks on andmete kogumise seaduslikkus, mis tähendab, et andmeid ei ole kogutud informatsiooni varastades või kompromiteerides IT süsteeme, nendesse varjatult sissetungides või kasutades ära sotsiaaltehnoloogiat (ingl k „*social engineering*“, inimeste psühholoogiline manipulatsioon vajalike andmete või juurdepääsu saamiseks (Anderson, 2008, p. 18; Saks, 2020, lk 45)). Sotsiaaltehnoloogia kasutamise näitena saab välja tuua, et helistatakse huvipakkuva ettevõtte töötajale ja esinetakse IT abina, öeldes, et on vaja teha turvauuendusi, mille tulemusena annab töötaja heas usus oma arvutile ligipääsu võimaluse ning selle kaudu saadakse andmed kätte. Kolmandaks kriteeriumiks on andmete valideerimine ehk allikakriitilisus, et ei tehtaks kogutud andmetest valesid järeldusi. (Lutai, 2020, p. 97)

1.1.1 Avalike andmete kogumise ajalugu

Avalike andmete sihipärane kogumine sai alguse 1940ndatel, kui Ameerika Ühendriigid hakkasid monitoorima ja analüüsima välisriikide ringhäälingute propaganda programme, milleks loodi asutus nimega Välisringhäälingu seireteenistus (ingl k *The Foreign Broadcast Monitoring Service*). Sihipärast tegevust rahastati kaitse-eelarvest. Külma sõja ajal andis avalike andmete kogumine ja analüüsimine strateegilise eelise vaenlase ees. Nii

oli võimalik teavet saada vastase sõjaväe võimekuse kohta, poliitiliste kavatsuste ning rahva meelsuse osas. Kogutud andmete analüüside põhjal oli võimalik varakult prognoosida potentsiaalseid ohtusid ning anda asjakohaseid hoiatusi. (Lutai, 2020, p. 96; Schaurer & Ströger, 2013, p. 53; Williams & Blum, 2018, pp. 4–6)

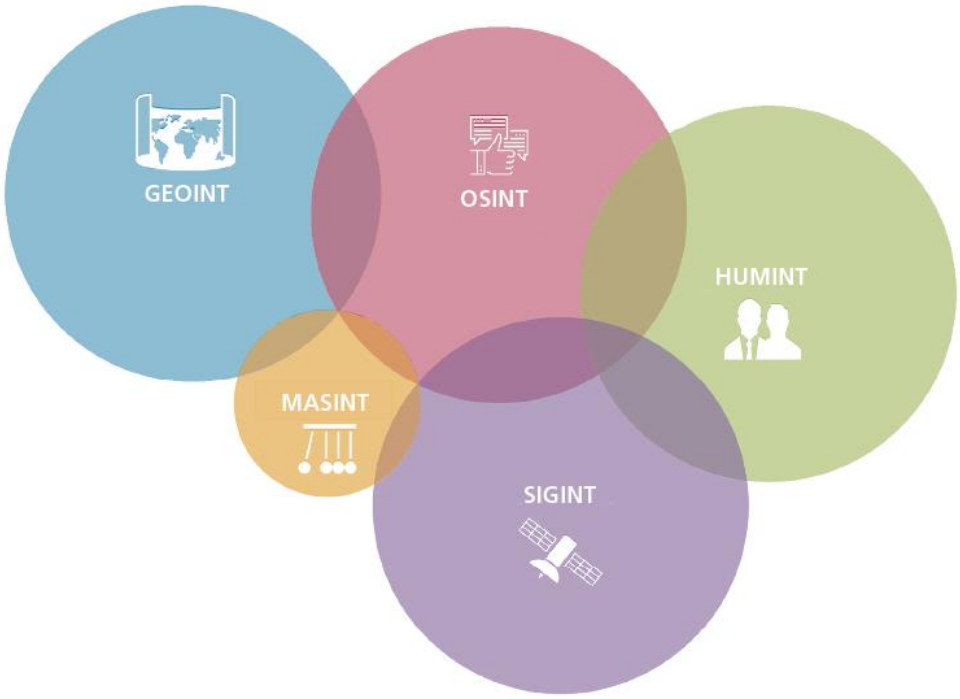
Personaalarvutite ja interneti levikuga sai luurekogukondadele selgeks, et *OSINT*i roll on oluliselt suurem kui algselt eeldati ning selle tähtsus tulevikus pigem kasvab kui kahaneb. Seda eelkõige sellepärast, et tekkisid suure mahuga digitaalsed salvestusruumid, võimekad otsingumootorid ja lairiba sidevõrgud. Oma rolli *OSINT*i tähtsuse suurendamisel mängisid ka meediaväljaanded, mis muutusid üha digitaalsemaks. See kõik päädis sellega, et 01.11.2005 loodi Ameerika Ühendriikides *Open Source Center* (Avalike andmete keskus), mis aastal 2015 nimetati ümber *Open Source Enterprise*ks (Avalike andmete asutus) ja liideti CIA allüksusega *Directorate for Digital Innovation* (Digitaalse innovatsiooni direktoraat), mille peamiseks rolliks jäi avalike andmete kogumine, saadud andmete analüüsimine ning sellest saadud teabe edastamine vajalikele luureasutustele. (Aftergood, 2015; Central Intelligence Agency, 2016, p. 28; Williams & Blum, 2018, pp. 4–6)

Interneti levikust hoogu saanud meedia digitaliseerimine ning sotsiaalmeedia platvormide tekked on andnud olulise tõuke *OSINT* kasutamiseks ning seda ennekõike tavalistele inimestele ning erasektorile. Enne interneti levikut oli mingil määral samuti võimalik inimeste kohta andmeid saada, kuid kindlasti mitte nii kiiresti ja põhjalikult kui praegu. See oleks tähendanud erinevate arhiivide läbi vaatamist ning suurel hulgal erinevate päringute tegemist ametiasutustesse, mis tavalisele inimesele tähendaks tohutut ajakulu ning tekiks küsimus, kas saadav kasu kaalub üle selleks kuluva aja. Samuti ei saanud kunagi kindel olla, mis andmeid üldse on võimalik leida ning kas päringutele üldse vastatakse.

Office of the Director of National Intelligence on välja toonud kuus peamist luureallikat, milleks on *SIGINT, IMINT, MASINT, HUMINT, OSINT ja GEOINT* (Office of the Director of National Intelligence, 2022). Kõik eelpool loetletud luureallikad on kindlalt piiritletud: *SIGINT* ehk signaaliluure tähendab nii side- kui ka elektroonilist luuret, seega andmeid saadakse signaalide pealtkuulamise kaudu, olenemata kuidas andmeid

edastatakse (Office of the Director of National Intelligence, 2022); *IMINT* ehk pilt- või kujutisluure, tähendab luureteavet, mille aluseks on erineval teel saadud pildid ja kujutised ning selle eesmärgiks on täiendada muudest allikatest saadud luureteavet (Eesti Keele Instituut, 2022); *MASINT* ehk andurluure, tähendab erinevatelt anduritelt kogutud andmete teaduslikku ja tehnoloogilist analüüsimist (Militerm, 2022b); *HUMINT* ehk inimluure, tähendab inimallkatelt saadud teavet (Office of the Director of National Intelligence, 2022); *GEOINT* ehk georuumiline luureteave, tähendab georuumilise info ja muude luureandmete lõimumisel saadavat luureteavet konkreetse asukoha kohta (Militerm, 2022a).

Kuigi erinevatel luureallikatel on kindlalt piirid, ei välista see asjaolu, et neil võib olla ühiseid jooni (vt. joonis 1, lk 17). Kuigi kõikidel luureallikatel ühiseid jooni ei ole, arvatakse sellegipoolest, et kõige suurem kattuvus teiste luureallikatega on *OSINT*il. Näiteks kommertssatelliidid on juba valmis pakkuma piisavalt hea kvaliteediga pilti, mis loob *OSINT*i ühise seose *GEOINT*iga. Lisaks on kommertssatelliidid varustatud erinevate anduritega ning peaaegu kogu maakera on kaetud erinevate meteoroloogiliste anduritega ning nendest saadavat teavet on võimalik seostada *MASINT*iga. Sotsiaalmeedia arenguid on võimalik siduda nii *HUMINT*i kui ka *SIGINT*iga. Sotsiaalmeediast pärit teavet on võimalik siduda *HUMINT*iga, kuna andmed on sisestatud inimeste poolt ning sealt saadud andmete kogumine annab arusaamu ja vaatenurki üksikisiku kohta, kellel on ainulaadne juurdepääs või kes saab anda kogukonna või riigi elanike esinduslikke vaatenurki. Samuti on sotsiaalmeedia sarnane *SIGNIT*iga, kuna sotsisaalmeediast on võimalik koguda teavet elektrooniliste vahenditega, mida analüüsides võib tuvastada huvipakkuvaid seoseid või kriitilist huvipakkuvat kommunikatsiooni. Oluline on, et kõiki neid andmeid on võimalik koguda avalikult, ilma et oleks vaja teha nende andmete saamiseks erinevaid päringuid keskkondade haldajatele. (Dawson, *et al.*, 2018, pp. 159–160; Williams & Blum, 2018, pp. 7–8)



Joonis 1. Luureallikate kattuvus üksteisega (Williams & Blum, 2018, p. 9).

Lisaks Ameerika Ühendriikidele on *OSINT* tähtsust tajunud veel paljud teised riigid, eelkõige nende riigikaitsega seotud riiklikud asutused. Prantsusmaa kaitse- ja riikliku julgeoleku strateegia näeb ette kaitsetööstuse ja tehnoloogilise baasi tugevdamist, mis tähendab koostööd teadusringkondadega ning süstemaatilist avalike allikate kasutamist (French Republic Presidency, 2017, pp. 63–72). Venemaa riiklik julgeoleku strateegia seab prioriteediks panustamise innovatsiooni ja uude tehnoloogiasse (Venemaa president, 2015, p. 17). Lisaks on Venemaal infoturbe doktriin, mis näeb ette tehnilist luuret (Venemaa president, 2016). Jaapani julgeoleku strateegia näeb *OSINTi* arendamist ette, kui kriitilist valdkonda, kuna koos *HUMINTi, SIGNITi ja IMINTi* allikatega tagab see järjepideva süsteemi. Veel on julgeolekustrateegiates näinud *OSINTi* vajalikkust Kanada, Inglismaa, Holland ja Hiina (Bereziuk, 2016, pp. 4–6). Kuna Ameerika Ühendriike saab pidada üheks NATO eestvedajaks, siis tänu sellele on *OSINT*i olulisust teadvustatud ka NATOS tervikuna ning selle jaoks on välja antud käsiraamat, mille eesmärgiks on teha liitlaste vahelisi ühiseid informatsioonikogumise treeninguid (NATO, 2001). Lisaks on EUROPOL teadvustanud *OSINT*i tähtsust, eelkõige võitlemaks küberkuritegevusega ning loonud *OSINT Dashboard*i, mille eesmärgiks on koguda kokku kübermaailmas

toimunud olulisi sündmusi (Europol, 2021). Veel on *OSINT*i kasutamisel saadavate andmete tähtsust teadvustanud Euroopa Komisjon, seda eelkõige käimas oleva Ukraina-Venemaa sõja raames (Euroopa Komisjon, 2022b).

Eelpool toodud luureliikidel on seoseid ka kriminaalmenetluse läbiviimise meetodite, taktika ja vahenditega. *HUMINTi* puhul pole saladus, et ka õiguskaitseasutused tegelevad inimallikatelt pärit informatsiooni kogumisega, olgu selleks teave kuriteo kohta või siis mõne konkreetse isiku kohta, kes võib olla otseselt või kaudselt seotud kuritegevusega. *SIGNIT*ga saab seose tuua telefonide pealtkuulamisega, olgu selleks siis kõnede või saadetud sõnumite salajane pealtkuulamine või -vaatamine (Leavell, 2007, p. 15). Lisaks saab *SIGNITga* seose tuua ka *IMSI-catcher*-ga, kui on vajalik tuvastada ühes konkreetses asukohas kindlal ajahetkel asuvaid mobiiltelefone (Ooi, 2015, pp. 10–17). *IMSI-catcher*-i puhul on tegemist tehnoloogilise seadmega, mille abil on võimalik teatud piirkonnas töötavate ja signaale vastu võtvate mobiiltelefonide jälgimine ning nende asukoha kindlaks tegemine (Phantom Technologies, 2023). *IMINT*it kasutatakse kriminaalmentlustes suhteliselt sageli, kuna on vajalik analüüsida ja vaadelda erinevaid turvakaamerate salvestusi või erinevaid fotosid, tuvastamaks kriminaalmenetlustes vajalikku teavet.

1.1.2. Avalike andmete kasutamise võimalus finantssektori näitel

Tänapäeval kasutatakse laialdaselt *OSINTit* ka väljaspool militaarvaldkonda. *OSINT* on leidnud oma koha nii avalikus kui ka erasektoris. Erasektoris on *OSINT* andmete kasutamiseks leitud erinevaid viise. Näiteks finantssektor saab kasutada avalike andmeid vajalike uurimiste läbiviimiseks, kuid saab kasutada ka töötajate värbamisel taustakontrolli tegemiseks, konkurentide analüüsimiseks ning partnerite usaldusväärsuse kontrollimiseks (Popel, 2022). Magistritöö autori hinnangul tuleb *OSINT*i kasutamisoskus kasuks just finantssektorile, kuna neil on KYC (ingl k *Know Your Customer*) ehk kliendi tundmise kohustus, mille eesmärgiks on kaitsta finantsasutusi kelmuste, korruptsiooni, rahapesu ja terrorismi rahastamise eest (Swift, 2023a). KYC on protsesside kogum, mis annab pankadele ja teistele finantsasutustele kohustuse tuvastada ja kinnitada nende organisatsioonide ja isikute identiteet, kellega nad äri teevad ning aitab tagada, et tegutsetakse seaduslikult (Swift, 2023b). „Tunne oma klienti“ nõuded tulenevad erinevatest rahvusvahelistest regulatsioonidest nagu CRS (ingl k „*Common*

Reporting and Due Diligence Standard“, eesti keeles „ühtne aruandluse ja hoolsusmeetmete standard“) ja FATCA (USA seadus ingl k *„Foreign Account Tax Compliance Act”*, eesti keeles „välismaiste kontode maksukuulekuse seadus“). Samuti kohalikest seadustest nagu rahapesu ja terrorismi rahastamise tõkestamise seadus, rahvusvahelise sanktsiooni seadus ja maksualase teabevahetuse seadus (Rahapesu ja terrorismi rahastamise tõkestamise seadus[1], 2017; Rahvusvahelise sanktsiooni seadus ja maksualase teabevahetuse seadus, 2019; Maksualase teabevahetuse seadus[1], 2014; OECD, 2014; IRS, 2023).

CRS on standard maksuasjades finantsteabe automaatseks vahetamiseks erinevate jurisdiktsioonide vahel, mille eesmärgiks on vähendada isikute maksukohustuse kõrvalehoidumisest oma kodukoha jurisdiktsioonis (OECD, 2014, pp. 9–11). FACTA on USA seadus, mis nõuab välismaistelt finantsasutustelt ja muudelt välismaistelt finantssektori välistelt üksustel aruandeid USA kontoomanike valduses olevate välisvarade kohta või nende suhtes kinnipeetavate maksete kohta (IRS, 2023).

1.1.3. Avalike andmete sobivus kriminaalmenetlusse

Võttes arvesse, et paljusid andmeid on võimalik internetist avalikult kätte saada, võib seda nimetada digitaliseerinud ühiskonna tunnuseks. Kõigil inimestel, kellel on juurdepääs arvutile ja internetile, on võimalik vaadata erinevaid satelliidipilte, mis on tehtud kommertssatelliitide poolt ja saada nendelt erinevaid andmeid, mida soovi korral on võimalik iseseisvalt analüüsida. Näiteks vaadata ilmakaarti ning teha ennustusi saabuvate ilmaolude kohta. Veel võib lugeda erinevate ajakirjanduslike väljaannete uudiseid, kombineerides neid sotsiaalmeediast saadud infoga ning teha järeldusi toimunud või tulevate sündmuste kohta. Samasugune võimalus on ka kriminaalasju menetleva asutuse uurijal, kui teadvustada milliseid avalikke andmeid võib vaja minna kriminaalasja lahendamisel.

Avalike andmete sihipärane kogumine võib anda eelise teiste ees, olgu selleks võit lahingus või konkurendist suurema kasumi saavutamine (Wells & Gibson, 2017, p. 85). Seega ei tohi avalike andmete kasutamise väärtust kriminaalmenetlustes alahinnata. Kasutades kriminaalmenetlustes oskuslikult avalikult kogutud andmeid, võib saada kuriteouurimisel olulist teavet, mida on vajadusel võimalik kasutada ka tõendina.

Arvestades asjaolu, et internetis on saadaval palju eri liiki informatsiooni, mida on võimalik koguda erineval viisil (nii seaduslikult, kui ka ebaseaduslikult), siis selleks, et saada aru millised andmed on seaduslikud avalikud andmed, on vajalik määratleda avalike andmete kogumise piirid, seda eriti kriminaalmenetlusi silmas pidades. *OSINT* eksperdid Florian Schaurer ja Jan Stöger (2013, p. 54) on leidnud, et illegaalselt saadavaid andmeid ei saa käsitleda *OSINTna.* Seetõttu mõeldakse käesolevas magistritöös avalike andmete kogumise all ainult seaduslikke viise andmete kogumiseks, mis tähendab, et andmete saamiseks ei ole eemaldatud või välditud andmete valdaja poolt seatud kaitsevahendeid Karistusseadustiku (edaspidi: KarS) § 217 (Arvutisüsteemile ebaseaduslikult juurdepääsu hankimine) mõistes (Karistusseadustik[1], 2001). Kaitsevahendi all mõistetakse eelpool toodud paragrahvis meetodit, mille arvutisüsteemide valdaja on seadnud arvutisüsteemile, et vältida teiste isikute poolt juurdepääsu hankimist arvutisüsteemile või juurdepääsu vähemalt olulisel määral raskendada (Sootak & Pikamäe, 2021, lk 730). See on oluline, kuna kriminaalmenetluses on tähtis koguda tõendeid ja kriminaalmenetluses olulisi andmeid seaduse alusel. Kriminaalmenetluses on tõendi seaduslikkuse nõu eriti range, kuna kriminaalmenetluses on riive isiku õigustele eriti intensiivne ning võib kahtlustatava jaoks lõppeda vabadusekaotusega ja vara konfiskeerimisega.

Kokkuvõtvalt saab öelda, et avalike andmete kogumine algas Teise maailmasõja ajal ning algselt tegelesid sellega riiklikud luureasutused, et saada teavet vaenlaste kohta. Interneti ja tehnoloogia levikuga on avalike andmete kasutamine jõudnud ka väljaspoole luureasutusi ning tänapäeval teadvustavad selliste andmete kogumise ja analüüsimise vajalikkust ka erasektor ja riiklikud õiguskaitseasutused. Avalike andmete õige ja sihipärane kasutamine annab õiguskaitseasutustele võimaluse tuvastada erinevaid julgeolekuohtusid.

1.2. Avalike andmete kasutamine julgeoleku vaates

Julgeolekuteooria on valdkond, mis uurib julgeoleku ja julgeolekuohtudega seotud teemasid ning püüab leida võimalusi, kuidas suurendada ühiskonna julgeolekut ja vähendada julgeoleku ohutegureid (Delehanty & Steele, 2009, pp. 523–524). Julgeoleku teoreetilisi käsitlusi saab jagada kaheks – traditsioonilised- ja kriitilised lähenemisviisid

(Demirkol, 2023, p. 23). Kui traditsioonilised lähenemised võtavad analüüsi lähtepunktina maailma sellisena, nagu see on, siis kriitilised teooriad osutavad maailmakorra konstitutsioonile. See tähendab, et teoreetiliselt tuletatud teadmised maailma kohta ei ole objektiivsed ega neutraalsed, vaid põhinevad normatiivsetel valikutel, millel on olemuslikud poliitilised tagajärjed (Browning & McDonald, 2013, p. 238). Kriitilistest julgeolekuanalüütikutest (ingl *Critical Security Studies*) on nähtavaimaid koolkondi kolm, milleks on Kopenhaageni, Pariisi ja Aberystwyth ehk Walesi koolkonnad (Behera, *et al.*, 2021, p. 9; Walklate, *et al.*, 2019, p. 61).

Kopenhaageni koolkonna järgi on julgeolek jagatud sektoriteks – militaarne, majanduslik ja sotsiaalne sektor (Buzan, *et al.*, 1998, p. 22). Hilisemalt on jõutud järeldusele, et sektorite arv ei saa olla piiratud, kuna puuduvad konkreetsed kriteeriumid, mis suudavad sektoreid kindlalt ära piiritleda ning seetõttu kujunevad sektorid välja läbi reaalse kasutuse julgeolekustamise diskursuses (Albert & Buzan, 2011, p. 414). Koolkonna puhul tuleb esile valitsusväliste toimijate tähtsus julgeoleku keskkonnas, kus julgeolekuohtusid esitatakse kõneakti kaudu auditooriumile selleks, et nad oleksid valmis taluma erakorralisi meetmeid, mis tavaolukorras ei oleks vastuvõetavad (Wæver, 2011, pp. 468–469). Kõneakti on võimalik kirjeldada sedasi, kus julgeolekukeskkond ise ei ole võimeline piiritlema reaalset ohtu ning ohu kirjeldamine läbi kõneakti ongi julgeolekustava tegevus (Buzan, *et al.*, 1998, p. 26). Aberystwythi ehk Walesi koolkond uurib „teaduslike kontseptsioonide ja poliitiliste tegevuskavade" taga olevat poliitikat, samuti riigi ja sõjaväe detsentreerimist kui „referentsobjekte" kaalumaks laiemat hulka mõjutajaid ja objekte selleks, et uurida ohukogemusi valdavalt normatiivsete lähenemisviiside alusel ehk nad politiseerivad julgeolekut, sealhulgas julgeolekuintellektuaale, eetilises mõttes (Samier, 2015, p. 690). Pariisi koolkond omakorda tegeleb julgeolekustamisega läbi julgeolekupraktikute, kus julgeolekustamisel ei oma riigipiirid enam rolli ning olulisel kohal on tehnoloogia kasutamine (Behera, *et al.*, 2021, pp. 9–10; Danewid, 2022, p. 24).

Siseministeeriumi allasutused: Häirekeskus, Politsei- ja Piirivalveamet, Päästeamet, Kaitsepolitseiamet, SMIT ja Sisekaitseakadeemia (Siseministeerium, 2023b). Nendest asutustest tegelevad kriminaalmenetlustega oma pädevuste piires Politsei- ja Piirivalveamet ning Kaitsepolitseiamet. Lisaks viivad kriminaalmenetlust läbi KrMS § 31

lg 1 järgi Maksu- ja Tolliamet, Konkurentsiamet, Sõjaväepolitsei, Keskkonnaamet ning Justiitsministeeriumi vanglate osakond ja vangla (Kriminaalmenetluse seadustik[1], 2003). Võttes arvesse, et Eesti kuulub Euroopa Liitu ja Schengeni viisaruumi, millega on loodud kõikidele Euroopa Liidu elanikele sisuliselt piirkontrollita vaba liikumine, annab see võimaluse ka kurjategijatel vabalt liikuda ning lihtsamini tegutseda piiriüleselt. Lisaks tehnoloogia ja interneti arenguga on kurjategijatel oluliselt lihtsam panna toime kuritegusid teistes riikides. Saab öelda, et kuritegevuses ei oma enam riigipiirid rolli, mistõttu on uurimisasutustel oluline suhelda teiste riikidega ning teha rahvusvahelist koostööd. Rahvusvaheline koostöö on seatud üheks kriminaalpoliitika prioriteediks, mille raames tehakse koostööd süütegude ennetamisel, tõkestamisel, avastamisel ja menetlemisel, sealhulgas ekspertiisides ning kasutatakse tehnoloogiat (Kriminaalpoliitika põhialuste aastani 2030 heakskiitmine, 2020). Õiguskaitseasutuste koostöö raames on võimalik tabada piiriüleseid kuritegusid toimepanevaid isikuid ning läbi selle tagatakse parem sisejulgeolek.

Eesti julgeolekupoliitika alustes on välja toodud, et turvalisuse ja põhiseadusliku korra kaitseks on vajalik rohkem tähelepanu pöörata infotehnoloogilistele lahendustele ja tõhustada infoturbemeetmeid. Lisaks tuuakse välja, et ohud on järjest mitmekesisemad ning riigipiiride ülesus on muutnud turvalisuse tagamise keerulisemaks. Ohtude ennetamiseks ja tõkestamiseks on vajalik koguda ja töödelda asjakohast teavet, tõkestada vaenulikku luure- ja mõjutustegevust ning teha selleks nii riigisisest kui ka rahvusvahelist koostööd. (Riigikogu, 2017, lk 12)

Avalike andmete kasutamine julgeolekuohtude tuvastamisel võib olla oluline mitmel viisil, eriti kaasaegses maailmas, kus digitaalsetel andmetel on suur roll ning kui võtta arvesse pilveteenuseid ja sotsiaalmeedia levikut, on hakanud riikide piirid nii öelda hägustuma. Arvestades, et internet on globaalne ning see on piiriülene, siis sobitub antud magistritöö teemaga julgeolekuteoreetilistest lähenemistest kõige paremini Pariisi koolkond, kuna nende seisukohtade järgi ei oma julgeolekustamisel riigipiirid rolli ning oluline roll on tehnoloogiliste võimaluste kasutamisel. Koolkonna käsitluse järgi on piirid sisejulgeoleku ja välimise julgeoleku vahel hägustumas, tänu millele on siseriiklike õiguskaitseorganitel tarvis vastaseid otsida nii öelda piiri tagant, mis rõhutab õiguskaitseasutuste vajadust tegemaks rahvusvahelist koostööd julgeolekuküsimuste

lahendamiseks (Bigo, 2000, p. 320–321). Lisaks rõhutab Pariisi koolkonna eestvedaja Jef Huysmans (2006, p. 8), et sisejulgeoleku valdkonna ehitamine sõltub olulisel määral tehnoloogilistest ja tehnokraatlikest protsessidest.

Arvestades tänapäeva maailma digitaliseerumise käigus tekkivat tohutut andmete hulka, on julgeoleku vaates oluline osata neid andmeid eesmärgipäraselt kasutada. Siinkohal saab välja tuua Pariisi koolkonna esindajate Claudia Aradau ja Tobias Blanke seisukoha, kus digitaalne tehnoloogia ja algoritmid on julgeoleku praktikaid ümber kujundanud, mille tõttu on vajalik osata leida anomaaliad massandmete seast, kasutades selleks erinevaid algoritme (Aradu & Blanke, 2017, pp. 19–20).

Pariisi koolkond on julgeoleku normaalsust defineerinud läbi julgeoleku professionaalide, kasutades selleks tehnoloogiat, mille abil tagada ja hallata sotsiaalseid probleeme. Julgeoleku professionaalide all näeb koolkond julgeolekupraktikuid nagu sõjaväelased, sandarmid, immigratsiooniametnikud, politseinikud, kes osalevad aktiivselt julgeolekuprobleemide määratlemises. Samuti näeb koolkond, et julgeoleku tagamiseks võetakse järjest rohkem kasutusele tehnoloogiaid, mis on mõeldud inimeste kontrollimiseks ja jälgimiseks. Tõhusaks meetodiks, tagamaks ühe riigi julgeolekut, on vajalik jälgida kindlat isikute gruppi, kes võib selle riigi julgeolekut ohustada. See tähendab, et julgeolekustamisega seotud ohtude defineerimine läheb poliitilistelt institutsioonidel üle julgeoleku professionaalidele, kes kasutavad ohtude maandamiseks tehnoloogilisi lahendusi. Julgeoleku professionaalidena defineerib koolkond peamiselt avalikest asutustest, nagu politsei ja sõjavägi, pärit eksperte. (Bigo, 2000, pp. 328–330; Bigo, 2002, p. 64; Bigo, 2008, p. 14; C.A.S.E, 2006, p. 457)

Pariisi koolkonna puhul ei jagata julgeolekut erinevateks distsiplinaarseteks objektideks, mille kaudu saaks julgeolekut piiritleda ühe kindla kehtestatud korra järgi. Selle asemel on julgeoleku terminit kasutatud väga erinevate valdkondade kirjeldamiseks praktikas, mida ei saa koondada ühte põhikategooriasse. Julgeoleku terminite piiritlemine ei peitu ekspertide teadmistes, vaid võitluses ja hierarhiates nende diskursiivsete tegevuste sees ja nende võitlemisel kindla tõe üle. Tõeväite kontrollimise viiside analüüsimine ja nende omavaheline konkurents saab olema aluseks julgeoleku küsimuse defineerimisel. See hõlmab ka julgeolekuvaldkonnaga tegelevate isikute endi kogemusi. Kõik inimesed, olgu

nad siis otseselt või kaudselt seotud turvalisuse analüüsimisega, on kesksel kohal. (Bigo & McCluskey, 2018, pp. 5–6)

Võttes arvesse sise- ja välisjulgeoleku ohtusid on need viinud olukorrani, kus erinevate riikide julgeolekuasutused peavad tegema omavahel koostööd ning see on pannud aluse rahvusvahelistele julgeolekuprofessionaalide võrgustike tekkimisele ehk piiriülest koostööd peavad tegema nii luureasutused, politsei kui ka sõjavägi (Balzacq, *et al*., 2010, p. 6). Tõhustamaks riikide kriminaalpolitseilist koostööd, on koostöö tegemiseks loodud erinevaid rahvusvahelisi organisatsioone nagu EUROPOL Euroopas ja INTERPOL ülemaailmselt. Lisaks toimub ülemaailmselt otsene suhtlus erinevate õiguskaitseasutuste vahel. Politsei rahvusvaheline koostöötegevus ühtib otseselt Pariisi koolkonna vaatega. Koolkond näeb julgeolekuga tegelemist läbi julgeolekupraktikute (politseinikud, sõjaväelased, luureasutuste ametnikud), kus suur roll tegelemaks julgeolekuohtudega on rahvusvahelisel koostööl.

Siinkohal saabki tuua välja paralleeli kriminaalmenetlusega, kui uuritakse piiriüleseid kuritegusid. Piiriüleste kuritegude menetlemisel peavad siseriiklikud õiguskaitseasutused suhtlema ja tegema koostööd ning vahetama informatsiooni välisriigi õiguskaitseasutustega, samuti võib olla vajalik luua ühiseid töörühmi või uurimisrühmi, eesmärgiga viia edukalt läbi kriminaalmenetlusi.

Digitaalsete tehnoloogiate kasutamine on rahvusvahelise koostöö lahutamatu osa. Euroopa õiguskaitseasutused on selleks võtnud kasutusele infovahetuse süsteemi SIENA, mis on turvaline teabevahetuse kanal, mida saavad kasutada Euroopa Liidu liikmesriikide õiguskaitseasutused, Europoli sideohvitserid, eksperdid, analüütikud ja kolmandad osapooled, kellega EUROPOL koostööd teeb (EUROPOL, 2022a). Võitlemaks ülemaailmselt kuritegevuse kui julgeolekuohu vastu, on INTERPOLil 19 erinevat spetsiifilist andmebaasi (INTEPOL, 2022a). Lisaks on Euroopa Liidus loodud asutus nimega CEPOL, mille eesmärgiks on tagada ühendusse kuuluvate riikide õiguskaitseasutuste ühtne koolitamine (CEPOL, 2022a).

Selleks, et julgeoleku eksperdid käiksid ajaga kaasas ning suudaksid üha muutuvas digitaliseerunud maailmas hakkama saada, viivad INTERPOL kui ka CEPOL läbi erinevaid *OSINT* alaseid koolitusi (CEPOL, 2022b; INTRPOL, 2022b). Antud koolituste

eesmärgiks on tõsta uurimisasutuste ametnike teadlikkust ja oskusi tegelemaks avalike andmetega ning samuti vahetada kontkate teiste riikide ametnikega, eesmärgiga tõhustada rahvusvahelist koostööd. Koolitustel saadud teadmisi ja oskusi on võimalik rakendada kriminaalmenetluste uurimisel.

Kaasaegne maailm on täis digitaalset tehnoloogiat, mis on paljude inimeste harjumusi muutnud ning andmete digitaliseerimisega ja sotsiaalmeedia levikuga on paljud andmed muutunud avalikult kättesaadavateks. Selleks, et orienteeruda avalikes andmetes ning tuvastada erinevaid anomaaliaid ja võimalikke julgeolekuohtusid, on vajalik kasutada erinevaid tehnoloogilisi võimalusi ja algoritme. Avalike andmete kogumisel ja nende analüüsimisel on võimalik tuvastada tundmatuid ning tuntuid kahtlustatavaid ning koostada nende kohta profileeritud riskianalüüse, mis on olulised tuvastamaks, kui palju mõni persoon võib ohustada sisejulgeolekut. Tehnoloogiate kasutamise olulisust kuritegude avastamisel ja uurimisel kinnitab ka teiste riikide praktika. Nii on näiteks Ühendkuningriigi valitsus välja toonud, et massandmete monitoorimisel on võimalik tuvastada kõrge riskiga ohtusid ning samuti on võimalik tuvastada uusi seni tundmatuid kurjategijaid (Aradu & Blanke, 2017, p. 3). Õiguskaitseasutustel on oluline käia ajaga kaasas ning leida uudseid ja kaasaegseid viise, kuidas rakendada tänapäeva digitaalmaailma võimalusi kriminaalmenetlustes.

1.3. Avalike andmete kogumine kriminaalmenetlustes

Kriminaalmenetluse peamine eesmärk on kuriteo fakti tuvastamine ja kui kuriteo fakt leiab kinnitust, siis tõendite kogumine eesmärgiga tuvastada kahtlustatav ja talle süüdistuse esitamine (European e-justice, 2023). Õiguskantsler on avaldanud, et tõe väljaselgitamine on oluline üldine huvi kriminaalmenetlustes (Madise, 2021). Ühe võimalusena, kuidas kriminaalmenetluses tõde välja selgitada, saab välja tuua avalike andmete kasutamist. Selleks, et avalikke andmeid oleks võimalik kasutada, on vaja neid esmalt koguda ning kogutud andmeid vajadusel analüüsida.

Kui ilmnevad kuriteo tunnused, siis on uurimisasutus ja prokuratuur kohustatud alustama kriminaalmenetlust, kui puuduvad KrMS alusel kriminaalmenetlust välistavad asjaolud (Kriminaalmenetluse seadustik1, 2003, § 6). Vastavalt KrMS § 194 lg 1 on

kriminaalmenetluse ajendiks kuriteoteade või kuriteole viitav muu teave. See tähendab, et kriminaalmenetluse alustamiseks ei pea tingimata olema kuriteoteadet (KrMS § 195), vaid selleks võib olla ka avalikest allikatest pärit teave. Täiendavalt on võimalik avalikest allikatest saada ka muud olulist informatsiooni, mis võib omada tõenduslikku või taustteavet toimunud kuriteo või kriminaalmenetlusega seotud isikute suhtes. Seetõttu on oskuslik andmekorje kriminaalmenetlustes olulisel kohal.

Kriminaalmenetluses algab andmekorje ennekõike lähteülesande püstitamisega, kus määratletakse ära andmete kogumise eesmärk ning kust ja kuidas on võimalik vajalikke andmeid hankida. Andmekorje puhul on oluline teha vahet kas andmeid kogutakse taustteabe saamise eesmärgil või tõendi saamise eesmärgil. Oluline on arvestada, et nii taustteabe kui ka tõendi saamise eesmärgil andmete kogumine peab toimuma konkreetse kriminaalasja huvides. Tõendi puhul, eriti kui tõend pärineb avalikest allikast, on oluline, et tõendi kogumise protsess oleks jälgitav, mis tähendab, et kriminaalmenetluse teised osapooled saavad samu samme korrates jõuda samale tulemusele. Taustteabe kogumise tulemusel on võimalik planeerida järgnevaid tegevusi kriminaalmenetluses vajalike andmete saamiseks, olgu selleks näiteks sihistatud päringu tegemine või olemasoleva ressursi sihipärane kasutamine. Avalike andmete kasutamisel on oluline veenduda allika usaldusväärsuses või kui seda ei ole võimalik teha, siis olla allikakriitiline. Seetõttu on vajalik avalikke andmeid kogudes meeles pidada, et ainult ühest kohas saadav teave ei pruugi olla oluline, kuid kombineerides erinevaid allikaid võib saada suhteliselt tervikliku ja usaldusväärse pildi (Kozera, 2020, p. 44).

Üldiselt saab nimetada avalike andmete kogumist kriminaalmenetluse raames üheks elementaarsemaks teabe kogumise meetodiks, kuna avalikku teavet on võimalik koguda reaalajas, teabele on enamasti lihtne pääseda ligi ning seda kõike madalate kuludega (Hwang*, et al.,* 2022*,* p. 1). Samas ainult andmete kogumisest kriminaalmenetluses otsuste tegemiseks ei pruugi piisata, saadud andmeid on vaja põhjalikult analüüsida, et nende põhjal oleks võimalik võtta vastu menetluslikke otsuseid.

Üldjuhul, kui räägitakse avalike andmete kasutamisest, siis sageli mõeldakse selle all ainult *googeldamist*, mistõttu ei suhtuta avalike andmete kogumisse tihti sama tõsiselt kui läbi erinevate päringute või muude toimingutega saadud andmetesse. Tihti ei teadvustada,

et kui kasutada *Google* otsingusüsteemi õigesti, näiteks *Google Dorking* meetodit, siis võib leida oluliselt rohkem informatsiooni, kui tavaliste otsingutega. *Google Dorking* on meetod, mida tuntakse ka nimetusega *google hacking* ning selle meetodi puhul on tegemist otsingumeetodiga, mis tähendab lisakäskude ja parameetrite sisestamisega on võimalik saada infot, mis tavalise otsinguga ei ole leitav (Propastop, 2021). *Google Dorking*'ut nimetatakse üheks avalike andmete otsimise meetodi peamiseks osaks (Černý & Potančok, 2023, p. 5). Kuid lisaks *Googlele* on veel palju teisi otsingumootoreid ning neil kõigil on omad positiivsed ning negatiivsed küljed. Seega on oluline teada erinevaid otsingumootoreid ja tunda otsingute teostamist efektiivistavaid tööriistu. Otsingumootorite kasutamisel on oluline eelnevalt mõelda läbi milliseid märksõnu ja millisel viisil otsingute tegemisel kasutada. Täiendavalt otsingumootoritele, mille abil avalikku infot otsida, on võimalik teostada sihistatumaid otsinguid sotsiaalmeedia kanalites, foorumites, registrites jne. Lisaks on kõigil isikutel, kasutades vastavat rakendust, võimalik teostada avalike andmete otsinguid tumeveebis. Avalike andmete kasutamise olulise poolena saab välja tuua veel, et andmeid on võimalik koguda suurel hulgal ja erinevatest allikatest, peaaegu reaalajas, mis teeb teabe hankimise oma loomult odavaks ja efektiivseks (Hwang, *et al.*, 2022, p. 4; Pastor-Galindo, *et al.*, 2020, pp. 2159–2160).

Avalike andmete kasutamisel on sageli vaja saadud andmeid analüüsida, mis on oma olemuselt metodoloogiline protsess ning mille lahutamatuks osaks on allikakriitilisus ja *Bayesi* teoreemi (*Bayesi* teoreem – kirjeldab sündmuse tõenäosust tuginedes eelnevale teadmisele sündmustest, mis võivad olla sündmusega seotud) põhimõtetel andmete hindamine. Tihti võib andmete rohkus internetis ja sotsiaalmeedias nihutada empiirilise fookuse piire, seetõttu on oluline arvestada reegliga, et „90% kõigest on jama", mis tähendab, et suur hulk saada olevast ja avalikult kogutud andmetest pärit informatsioonist ei pruugi omada mittemingisugust tähtsust. (Lutai, 2020, p. 106; Hauter, 2021, pp. 2–3)

Vaatamata avalike andmete rohkusele internetis ning asjaolule, et kõik ei pruugi olla tõsi, on nende kasutamine kriminaalmenetluses siiski oluline seetõttu, et andmeid on võimalik koguda peaaegu kõige kohta. Teavet otsides ja kogudes on oluline arvestada ka riiklike registritega (vt. tabel 1), kust on võimalik saada kvaliteetseid andmeid isikute ja vara kohta. Kuigi uurimisasutustel on tööalaselt enamikele riiklikele registritele vajalik

juurdepääs tagatud, on tegemist siiski avalike andmetega, kuna neile registritele on võimalik igal isikul ligi pääseda kas tasuta või tasudes riigilõivu.

Tabel 1. Eesti riiklikud registrid (autori koostatud)

Riigilõivuga registrid	**Tasuta kasutamiseks registrid**
Rahvastikuregister – põhjendatud juhtudel	Eesti avaandmete portaal – isikustamata andmed
Karistusregister	Kohtulahendite andmebaas
Kinnistusraamat	Avaliku sektori dokumendiregistrid
Eesti äriregistri detailpäringud	Eesti äriregistri lihtpäringud
Euroopa äriregister	Mootorsõidukite info läbi transpordiameti „sõiduki taustakontrolli“
	Transpordiameti õhusõidukite register
	Laevakinnistusraamat
	Maa-ameti kaardirakendused
	Maa-ameti fotoladu
	Ehitisregister
	Ametlikud Teadaanded

Riiklike registrite puhul saab tuua välja, et tasuta kasutamiseks on üldjuhul registrid, milledes ei kuvata isikuandmeid (andmed on registris isikustamata kujul). Juhul kui soovitakse riiklikest registritest isikustatud andmeid, on päringud üldjuhul riigilõivustatud ning kõik päringud logitakse registripidaja poolt, et andmete väärkasutamise korral oleks võimalik tuvastada registrist andmeid pärinud isikut. Registritesse teostavate päringu logimise kohustus tuleneb isikuandmete kaitse seadusest ja Euroopa isikuandmete kaitse üldmäärusest (Euroopa Parlamendi ja Nõukogu, 2016). Riigi Infosüsteemide Amet on loonud selleks „Andmejälgija“, mis on liidestatud avaliku sektori infosüsteemidega ning mille eesmärgiks on pakkuda kodanikule selget ülevaadet tema andmetega sooritatud toimingutest (Riigi Infosüsteemide Amet, 2022).

Kohti, kust avalike andmeid kriminaalmenetluse tõhusaks läbiviimiseks koguda on mitmeid. Lisaks riiklikele registritele on andmeid avalikult võimalik koguda ka näiteks sotsiaalmeediaplatvormidelt ja erinevatest internetiportaalidest. Praegusel sotsiaalmeediaajastul, kus paljud inimesed jagavad endast ja oma tegevustest kõike, võib eeldada, et inimesed loobuvad oma privaatsusest vabatahtlikult selles osas, mida nad endast avalikult postitavad. Kasutajate postituste levikule aitavad kaasa ka sotsiaalmeediaplatvormide erinevad algoritmid. Oluline on siinkohal mõista, et sotsiaalmeediaplatvormide ärimudel nõuab, et neil oleks võimalikult palju kasutajaid, kes toodaksid platvormile erinevat sisu, mida oma kasutajatele näidata (Rohn, 2015, p. 1050). Seetõttu võib kasutaja postitus levida laiemalt kui algselt planeeritud. Sellest johtuvalt on paljudel sotsiaalmeediaplatvormidel kasutajate privaatsuspoliitikad väga pikad ja kirjutatud väga keerulises juriidilises keeles, mille tõttu suur hulk inimesi ei oska või ei tea, kuidas erinevatel platvormidel oma andmeid teiste eest kaitsta või panna piiranguid andmete osas, mida nad ei soovi kogu maailmale avaldada. (Edwards & Urquhart, 2015, p. 303). Lisaks olenevalt platvormist ei pruugi kasutaja saada valida, milliseid andmeid ja kellega ta jagada soovib. Näiteks Facebookis saab kasutaja varjata ainult teatud tüüpi andmeid, kuid nimi ja profiilipilt on nähtav kõigile (Rønn & Søe, 2019, p. 366). Mõned kontod võivad mõnel sotsiaalmeediaplatvormil olla märgitud privaatseteks, seetõttu on oluline menetleja oskus kasutada neid andmeid, mida on võimalik avalikult kätte saada.

Sotsiaalmeediaplatvorm Facebook sattus aastal 2015 ja 2018 skandaali seoses andmete jagamisega *Cambridge Analytica*'le, mille tulemusena saadi ligipääs kümnete miljonite kasutajate andmetele ning saadud andmete alusel profileeriti kasutajaid, mida kasutati erinevate valimiskampaania reklaamide tegemiseks (Duisembina, *et al.*, 2018, pp. 95–96). See skandaal näitas, kuidas tänapäeval on võimalik avalike andmete väärkasutamisega õõnestada demokraatia põhimõtteid ning kuidas eraettevõtted suudavad manipuleerida kasutajatega, mistõttu andis see kaasus tõuke Euroopa isikuandmete kaitse üldmääruse (edaspidi: IKÜM) vastuvõtmiseks 2016. aastal, mis jõustus 25.05.2018. IKÜM-i üheks eesmärgiks on tagada ja ühtlustada füüsiliste isikute põhiõiguste ja -vabaduste kaitset isikuandmete töötlemise toimingutel (Euroopa Parlament ja Nõukogu, 2016). Sisuliselt reguleerib IKÜM kuidas isikuandmeid võib töödelda nii avalikus kui ka erasektoris. On oluline rõhutada, et IKÜM ei keela andmete kogumist, kui andmed olid andmesubjekti poolt ilmselgelt avalikustatud (Kotsios, *et al*.,

2019, p. 9). On oluline, et avalike andmete kogumisel tuleb uurimisasutustel järgida IKÜM sätestatud isikuandmete töötlemise põhimõtteid, et andmete kogumine oleks eesmärgipärane, proportsionaalne, seaduspärane ning minimaalne st andmeid kogutakse nii vähe kui võimalik ja nii palju kui vaja.

Sotsiaalmeedia annab võimaluse saada sihistatud teavet inimeste eelistuste, uskumuste ja tegevuste kohta (Dover, 2020, p. 225). *Cambridge Analytica* juhtum ilmestab, kuidas sotsiaalmeedias avaldatud andmeid tõlgendades ja analüüsides on võimalik keskkonna kasutajaid profileerida näiteks selleks, et sihistatud reklaamikampaaniaga muuta nende poliitilisi eelistusi. Inimeste profiilide loomine võib olla kasulik ka kriminaalmenetlust läbivate subjektide kohta. Selliste profiilide koostamine annab kriminaalmenetluses täiendavad võimalused kahtlustatava kriminaaltulu tuvastamiseks ja vastavalt kuriteole ka võimalikku teavet laiendatud konfiskeerimise planeerimiseks. Ainult traditsioonilisi vahendeid kriminaalmenetluses kasutades (päringud erinevatest registritest, pankadest, vajadusel erinevad jälitustoimingud) on võimalik kriminaaltulu kohta teabe kogumine ja isiku profiili koostamine keeruline ning äärmiselt ajamahukas, mis teeb kogu kriminaalasja menetlemise pikaks ja riigile kulukaks ning see ei ühti menetlusökonoomia põhimõtetega.

Teave erinevatest Interneti foorumitest võib tulla kasuks eeskätt küberkuritegude uurimisel. Neis keskkondades vahetavad informatsiooni, teadmisi ja ka kogemusi kuritegude sooritamisest erinevad häkkerid ning arvutientusiastid (Warkentin, *et al.*, 2022, p. 325). Foorumites ja sotsiaalmeediaplatvormidel teavet kogudes on oluline mõista erinevaid kõnepruuke – lööklauseid, slängi, lühendeid, märksõnu, mida konkreetne uuritav isik või isikute grupp võib kasutada (Dawson, *et al.*, 2018, p. 160; Patton, *et al.*, 2017, p. 2). Seda on oluline teada, kuna erinevad generatsioonid ning erineva profiiliga ja huvidega inimesed kasutavad erinevaid väljendeid või sõnu tähistamaks mingit tegevust või eset.

Avalike andmete oskuslikul kogumisel kriminaalmenetluses on oluline roll, kuna läbi avalike andmete on võimalik saada teavet, mida riiklikes registrites ei pruugi olla. Samuti võib avalikes allikatest sh. sotsiaalmeediaplatvormidelt saada olulist taustteavet isikute kohta, mida on võimalik kasutada sihistatud päringute tegemiseks või kriminaalmenetluse

edukaks läbiviimiseks järgmiste oluliste tegevuste planeerimiseks. Lisaks võib avalikest allikatest saadud teave olla oluline olukorra- ja ohuhinnangute koostamisel. Olukorra- ja ohuhinnangud on olulised, et oleks ühtne ülevaade riiki mõjutavatest kuritegelikest trendidest ning saamaks aru, milliste trendidega tegelemiseks on olemas olevat ressurssi mõistlikum kasutada. Olukorra ülevaadete ja ohuhinnangute alusel on võimalik välja töötada vajalikud ennetusmeetmed, sest iga ära hoitud kuritegu on riigile odavam, kui selle menetlemine. Peale menetlus jaoks vajaliku info saamise on võimalik avalikest allikatest saada andmeid, mis tulevad kasuks õiguskaitseasutustele.

1.4. Avalike andmete kasulikkus õiguskaitseasutustele

Õiguskaitseasutustena (kasutatakse terminit ka „õiguskaitseorgan“) saab käsitleda asutusi, mis kaitsevad riigi sisemist korda (Eesti Keele Instituut, 2023b). Käesolev alapeatükk annab ülevaate eelkõige politseilisest küljest, kuid avalike andmete saadavat kasu on võimalik rakendada ka laiemalt. Ühe võimalusena saab tuua välja, et avalike andmete abil on võimalik saada ülevaadet konkreetse piirkonna – ilma avalike andmete kasutamiseta ei pruugi politseil olla täielikku ülevaadet, kuna inimesed ei teavita alati politseid õigusrikkumistest (kuritegudest), kuid kurdavad toimunud sündmusest sotsiaalmeedias. Teise võimalusena on võimalik koguda infot kriminaalmenetlustes tähtsust omavate isikute kohta, olgu selleks nende suhtlusringkonna kindlaks tegemine, elustiili ja harjumuste kaardistamine või muude oluliste andmete teada saamine (Chainey & Berbotto, 2021, pp. 274–276). Veel võib avalike andmete kasutamine õiguskaitseasutustele olla oluline valmistudes lähenevateks kriisideks, olgu selleks siis mõni viirus või lähenev loodusnähtus, kus analüüsides erinevaid avalike allikaid on võimalik teha otsuseid, kuidas saabuva kriisiga võimalikult hästi toime tulla, planeerides selleks õiguskaitseasutuste poolt vajalikke tegevusi ning ressurssi (Briggs, *et al.,* 2022, pp. 991–994). Viimase puhul saab näitena tuua 9. mai võidupüha, kus politsei monitoorib ka sotsiaalmeediat tuvastamaks võimalikke provokaatoreid.

Avalike andmete kasutamise kasuks räägib ka asjaolu, et avalike andmete kasutamine võimaldab kasutada õiguskaitseasutusel enda ressursse efektiivsemalt. Siinkohal saab näitena välja tuua, et iga asukoha üle vaatamiseks ei ole vaja alati füüsiliselt kohale minna, vaid selleks saab kasutada erinevaid avalikke kaardirakendusi nagu näiteks

Google Maps, kus on olemas tänava vaade või Maa-ameti Fotoladu. Samuti on ressurssi võimalik paremini planeerida erinevate tulevaste sündmuste nt. meeleavalduste jaoks, kui monitoorida asjakohaseid sotsiaalmeedia kanaleid, saamaks aru osalejate ja korraldajate kavatsusi ning seisukohti (Rønn & Søe, 2019, p. 367; Dover, 2020, p. 226). Oluline on välja tuua, et üks infokillukene ei pruugi alati otseselt tähendada midagi, aga kui panna kokku erinevad infokillud, võib saab suhteliselt hea ülevaatliku pildi juhtumist või olukorrast ning kui sinna juurde lisada kontekst, mille raames andmeid koguti, on võimalik panna kokku tervikpilt õiguskaitseasutuse huvisfääri kuuluva olukorra või sündmuse kohta (Kozera, 2020, p. 44). See tähendab, et avalikud andmed võivad aidata mõista ja hinnata saabuvaid või olnud sündmusi, samuti kuritegevuse mustreid ning leida seoseid erinevate kuritegude vahel. Siinkohal tuleb arvestada asjaoluga, et internetis on andmeid väga palju ning see tähendab, et ka infomüra võib palju olla.

Avalike andmete kasutamine annab õiguskaitseasutustele võimaluse kaitsta inimesi väärkohtlemise, seksuaalvägivalla, identiteedivarguste, terrorismi ja muude kuritegude eest (Hwang, *et al.,* 2022, pp. 4–5). Seda on võimalik teha, kui monitoorida sotsiaalmeedia platvormidel õigeid märksõnu ja fotosid (Ndubueze, 2021, p. 23). Kuid õigete märksõnade leidmine võib osutuda problemaatiliseks. Eelkõige nähakse probleemina seda kas politsei, kui üks õiguskaitseasutustest, suudab aru saada noorte lingvistilisest stiilist sotsiaalmeedias, mida mõjutab lisaks kultuuriline, rahvuslik ning sotsiaalne taust (Patton, *et al.,* 2017, p. 2). Siin saab näitena välja tuua narkokuritegudega seotud isikute kõnepruugi, kus „kallis“ tähendab kokaiini ning „odav; ants“ tähendab amfetamiini. See kõik paneb politsei, kui asutuse korralikult proovile. Seda ennekõike sellepärast, et PPAs oli 2021. aastal keskmine politseiametniku vanus 40 eluaastat (Siseministeerium, 2021, lk 22). Nii võib probleemiks kujuneda asjaolu, et üha vananevate töötajaskonnaga PPA ei pruugi suuta piisavalt monitoorida õigeid sotsisaalmeedia platvorme ning seal olevast sisust õigel ajal õigesti aru saada. Eriti kui arvestada asjaoluga, et sotsiaalmeediat kasutab eelkõige just noorem generatsioon (Yimer, 2021, p. 1).

Juba aastal 2018 viitas Riley Murray (2018), et sotsiaalmeediat saab pidada üheks peamiseks allikaks avalike andmete kogumisel. Statista statistikaportaali andmetel, on sotsiaalmeedia kasutajaid maailmas 4,7 miljardit ning Milose poolt tehtud uuringu järgi

on Eestis sotsiaalmeedia kasutajaid 986 000, mis on ligi kolmveerand kogu rahvastikust (Dixon, 2022; Mesipuu, 2021). Nende numbrite valguses ei pruugigi Murray väide eksida. Samas leitakse, et politseil on veel palju õppida, kuidas kasutada sotsiaalmeedias leiduvaid võimalusi (Fallik, *et al.,* 2020, p. 210). Ameerika Ühendriikides on suurematel politseijaoskondadel oma sotsiaalmeedia kanalid, mida kasutatakse informatsiooni jagamiseks ning kogukonnaga suhtlemiseks (Boateng & Chenane, 2020, p. 267). Ka PPA on esindatud sotsiaalmeedias, kus mitmetel erinevatel üksustel (nt. Facebookis: Politsei- ja Piirivalveamet, Liiklusjärelevalvekeskus, Keskkriminaalpolitsei, prefektuuridel ja jaoskondadel) on omad kanalid. Lisaks on sotsiaalmeedias PPA esindajatena kasutajakontod veebikonstaablitel ja mitmetel üksuse juhtidel (nt. Twitteris: Urmet Tambre, Rait Pikaro, Taavi Kirss, Pirko Pärila, Maarja Punak jne).

On oluline teha vahet kogukonnaga suhtlemisel sotsiaalmeedia vahendusel ning õiguskaitseasutuste tööks vajalike andmete kogumisel. Kogukonnaga suhtlemisel on võimalus anda välja informatsiooni, mis puudutab kindlat piirkonda või kõiki riigi elanike aga ka küsida teavet sündmuse või olukorra kohta, mille lahendamisel või olukorrast selgema pildi saamiseks on õiguskaitseasutusel vaja elanikkonna abi. Kui õiguskaitseasutused monitoorivad sotsiaalmeedias avaldatut, annab see neile võimaluse tuvastada kuritegelike võrgustike tegevusi ja nendesse kuuluvaid isikuid ning koostada saadud teabe pinnalt võrgustike profiile. Monitoorimisel saadud andmete analüüsi tulemused võimaldavad politseil paremini planeerida tegevusi, millega kuritegelike võrgustike tegevusi pärsitakse või likvideeritakse.

Õiguskaitseasutustel tuleb alati olla leidlik ning seda ka andmete kogumisel. Alati ei pea ise kõiki andmeid koguma, vaid võib teha mõningad andmed avalikuks, et saada inimestelt vastu teavet ning see võib aidata keerulisemaid menetlusi kiiremini menetleda. EUROPOL on näidanud siin eeskuju, mis puudutab avalikke andmete kogumist.

EUROPOL alustas aastal 2017 projektiga „*Stop Childe Abuse – Trace an Object“*. Projekti eesmärgiks on paluda avalikkuse abi raskete lastevastaste kuritegude menetlemisel, kus mõni süütu vihje, olgu selleks kas šampooni pudel või ajakirja kaas, saaks aidata lahendada kuritegu. Selleks on EUROPOL teinud lehekülje, kuhu lisatakse objekte, mis on pärit pildilt või videost, mida soovitakse tuvastada, eesmärgiga tuvastada

pildi või video tegemise asukoht või riik, kus sündmus toimus. 2021. aasta juuli seisuga on EUROPOL saanud üle 27 300 vihje, 115 puhul tuvastati riik, kus kuritegu toime pandi, 23 last on tuvastatud ning päästetud ohtlikust keskkonnast ning 5 süüdlast on tuvastatud ning süüdi mõistetud. Kuna EUROPOLi projekt on olnud edukas, siis alustas Austraalia Föderaalne Politsei sarnase projektiga märtsis 2021. (EUROPOL, 2022b)

Avalike andmete oskuslik kasutamine ja teadmine, kuidas kogutud andmeid analüüsida võib tulla õiguskaitseasutustele kasuks ka keerulisemate juhtumite lahendamisel. Siin on õiguskaitseasutustele olnud eeskujuks uurivajakirjandus, kes on suutnud lahendada ning tõe välja tuua keerulistes sündmustes. Ühe märkimisväärse näitena võib välja tuua rahvusvahelise uuriva ajakirjanike kollektiivi „Bellingcat“, mille üks tuntumaid ja märkimisväärsemaid uuringuid oli Malaysian Airlines-i lennu MH17 allatulistamine Ukrainas Donbassi piirkonnas juulis 2014, kus nad suutsid avalike andmeid kasutades ära tõestada Venemaa sõjaväe seotuse lennuki allalaskmisega enne ametliku uuringu lõppu (Allen, *et al.,* 2014, p. 3; Bellingcat, 2022). 17.11.2022 avaldas Haagi Ringkonnakohus kohtuotsuse, milles jõudis sisuliselt samale järeldusele, millele „Bellingcat“ viitas ning mõistis süüdi kolm isikut, kes olid seotud MH17 allatulistamisega (de Rechtspraak, 2022). See on hea näide, millise tulemuseni on võimalik jõuda, kui osata avalikke andmeid õigesti otsida, neid tõlgendada ja saadud andmeid oskuslikult analüüsida.

Üldiselt võib öelda, et avalike andmete kasutamine õiguskaitseasutuste töös võib olla oluline töövahend, mis aitab neil mõista ja tõrjuda kuritegevust ning pakkuda üldsusele turvalisemat keskkonda. Lisaks sellele on võimalik jälgida ja hinnata oma töö tulemuslikkust ja mõõta, kui edukalt on suudetud mingis piirkonnas kuritegevuse tõkestamisega toime tulla. EUROPOLi näitel on võimalik oskuslikult kasutada avalikkuse abi, kui jagada killukesi tõenditest, mille avaldamine otseselt ei kahjusta käimasolevat menetlust, kuid mille abil on võimalik tuvastada raskete peitkuritegude ohvreid ja võimalikke kuritegude toimepanijaid. Oluline on, et kasutamaks interneti võimalusi õiguskaitseasutuste tööks vajalike andmete kogumisel ei tohi vaadata mööda ka õiguslikust poolest.

1.5. Avalike andmete kogumise ja kasutamise õiguslik vaade kriminaalmenetlustes

Avalike andmete kasutamisel kriminaalmenetluses on oluline järgida kehtivat õiguslikku raamistikku ning olla kursis uute regulatiivsete suundumuste arenguga. Õigusliku raamistiku järgimine on oluline, et kogutud tõendid oleksid kohtus kasutatavad. Selleks, et tõendid oleksid kohtus kasutatavad, peab kogu andmete kogumise protsess olema läbipaistev ehk peab olema arusaadav, kust ja kuidas on andmeid kogutud. Käesolevas alapeatükis toob magistritöö autor välja võimalikud õiguslikud probleemkohad sotsiaalmeediast andmete kogumisel ning lekkinud andmete kasutamisel. Mõlemal juhul eksisteerib nii-öelda „hall ala“ selles osas, kust läheb õiguslik piir andmete kogumisel ja kasutamisel. „Hall ala“ tuleneb eelkõige õigusaktide tõlgendamise küsimusest, eriti sotsiaalmeedia kontekstis. Menetluslikus mõttes saab jagada andmete kogumise protsessi kaheks, milleks on teabe kogumine järgnevate tegevuste planeerimiseks ning tõendite kogumine. „Hall ala“ liigitubki pigem teabe kogumisse. Teabe kogumise protsessist kriminaalmenetlusse enamasti jälgi maha ei jää, järelikult eksisteerib oht, et rikutakse pahaaimamatult seadust. Enamasti on teabe kogumise eesmärk saada täiendavat teavet kriminaalasja kohta, mille tulemustest johtuvalt on võimalik planeerida järgnevaid menetluslikke taktikaid või toiminguid. Lekkinud andmete puhul saab „halli alana“ käsitleda andmete kasutamist, kuna need andmed võivad pärineda süüteo toimepanemisest.

1.5.1. Sotsiaalmeediast andmete kogumine

Alati on oluline jälgida, milliseid tõendeid konkreetses kriminaalasjas on vajalik koguda ning see käib ka sotsiaalmeedia kohta. Kogudes avalikke andmeid kriminaalmenetluse raames, on oluline, et järgitakse menetlusnorme, mida Eestis sätestab eelkõige KrMS ning lisaks on oluline arvestada kehtivate Euroopa kohtu ja Eesti Riigikohtu lahenditega.

Kogudes andmeid, kus inimene on tuvastatud või tuvastatav, võib tekkida õiguslik dilemma. Ühelt poolt on avalikult kättesaadavad andmed kõigile kasutamiseks, kuid teiselt poolt tekib konflikt inimõiguste aspektist. Euroopa Inimõiguste ja põhivabaduse kaitse konventsiooni artikkel 8 järgi on igaühel õigus sellele, et austatakse tema era- ja perekonnaelu ja kodu ning sõnumite saladust ning ametivõimud ei sekku sellesse muidu,

kui kooskõlas seadustega (Euroopa Inimõiguste ja põhivabaduse kaitse konventsioon, 1950). Probleemi olemus seisneb selles, et kuigi andmed on justkui kõigile avalikult kättesaadavad, on igal inimestel õigus ka privaatsusele. EIK on toonud välja, et inimestel on õigustatud ootus mõningale privaatsusele isegi siis, kui nad liiguvad avalikus ruumis (Von Hannover v. Germany, 2004). Avaliku ruumi mõistet saab laiendada ka internetis toimuva kohta, kui sealne tegevus on kõigile vabalt nähtav. Isegi kui inimesed mõistavad, et postitades midagi avalikult internetti, siis ei eelda nad, et seda postitust näeb terve maailm, rääkimata õiguskaitseasutustest (Koops, 2013, p. 657). Lisaks on EIK öelnud, et avaliku võimu poolt üksikisiku eraeluga seotud andmete säilitamine ja kasutamine ilma, et antaks isikule võimalus selle teabe ümberlükkamiseks, kujutab endast sekkumist eraelupuutumatusele tagatud õigusesse (Rotaru v. Romania, 2000).

Kriminaalmenetluses saab menetlustoiminguid jagada kaheks, milleks on avalikud menetlustoimingud ning mitte avalikud menetlustoimingud. Sotsiaalmeedia puhul võib tekkida vajadus koguda mõningaid tõendeid enne avalikke menetlustoiminguid, kuna võib eksisteerida risk, et vajalikud tõendid kaovad. Avalikeks menetlustoiminguteks saab nimetada kõiki toiminguid, mida teostades on kahtlustataval juba teada, et tema suhtes käib kriminaalmenetlus ning tema vastu kogutakse tõendeid. See omakorda annab kahtlustatavale võimaluse kõrvaldada sotsiaalmeediast teda süüstavaid andmeid. Alati võib muidugi loota, et kahtlustatav on koostööaldis ning aitab igati kaasa kriminaalmenetlusele kiirele uurimisele ning loovutab vabatahtlikult kõik andmed, mis on menetluse läbiviimiseks menetlejale vajalikud. Kuna karistusõiguslikult kahtlustatav ei pea enda kohta süüstavaid andmeid jagama, siis on mõistlik teha enne avalikke menetlustoiminguid kõik vajalikud toimingud ära. Kogudes sotsiaalmeediast andmeid on oluline, et kohtueelsel uurimisel ei ületataks tahtmatult piiri, kust edasine tegevus läheb jälitustoimingute alla.

Eksimise kohaks võib olla sotsiaalmeedia keskkondadest avalike andmete kogumine. Sotsiaalmeedias on enamasti kahte tüüpi kontosid – avalikud kontod, mille sisu on kõigile avalikult kättesaadav ning privaatsed kontod, millel olevat sisu saab näha ainult konto omaniku loal ja ulatuses. Selleks, et privaatsel kontol olevat sisu näha, võib olla vajalik pääseda konto omaniku sõbralisti. Kui uurija esineb enda õige nimega ning saavutab seeläbi sobilikule kontosisule juurdepääsu, siis probleeme ei teki, kuna identiteeti pole

muudetud ega loodud konto omanikule valearusaama. Kuid kui uurija ei saa esineda enda õige nimega kontoga ning on vajalik kasutada „libakontot“ („libakonto“ all mõeldakse kontot, mis ei ole kasutaja enda nimega konto ning kasutatud on väljamõeldud identiteeti), siis on tegemist jälitustoiminguga, kuna uurija identiteet on muudetud ning sellega luuakse kontoomanikule vale ettekujutus.

Juhul, kui tekib vajadus teostada jälitustoiminguid, on esmalt vajalik kindlaks teha nende teostatavuse lubatus. Selleks on vajalik vaadata KrMS § 126^2 lg 2 sätestatut, kus on kirjas kõik KarS-i paragrahvid, kus on lubatud teostada jälitustoiminguid. Samas on KarS-s loetletud mitmeid kuritegusid, kus jälitustoimingute tegemine ei ole lubatud, kuid kus on võimalik tõendeid hankida sotsiaalmeediast. Sotsiaalmeediast vajalike tõendite kogumiseks võib vaja minna „libakontot“, mis juriidilises mõttes on variidentiteedi kasutamine. Kui tavalise inimese puhul pole õigusaktides reguleeritud „libakonto“ kasutamist (välja arvatud teise isiku identiteedi vargus KarS § 157^2 mõistes), siis politsei puhul tähendab see seda, et tarvis on prokuratuuri poolt väljastatud jälitustoimingu luba jälitustoiminguks, mida kvalifitseeritakse KrMS §-i 126^9 järgi politseiagendi kasutamiseks (Kriminaalmenetluse seadustik, 2003). Kui prokuratuur väljastab politseiagendi kasutamise loa, siis on politseiametnikel võimalik teostada variidentiteeti kasutades toiminguid loas määratud ulatuses.

Siinkohal võibki tekkida õiguslik dilemma, kui näiteks uuritakse kuritegu, milles ei ole lubatud kasutada jälitustoiminguid, kuid võimalikud tõendid on sotsiaalmeedias olemas. Dilemma tekib just siis, kui õiguskaitseasutusel on vajalik luua konto mõnda sotsiaalmeediaplatvormi andmete nägemiseks (nt sotsiaalmeediaplatvormil VKontakte ei näe sisu, kui sa ei ole registreeritud kasutaja) ning uurija ei taha või ei saa luua vajalikku keskkonda oma personaalse nimega kontot. Ilma kontota ei ole võimalik andmeid näha ning seetõttu ei ole ka algselt teada, kas selles keskkonnas on tõendeid, mida on vaja koguda või mitte. Dilemma seisnebki asjaolus, et kui „libakontot“ luua ei tohi, siis võivad jääda vajalikud andmed, ka tõendid, kogumata. Kriminaalmenetluse ökonoomikast lähtudes ei ole alati mõistlik alustada jälitustoimikut ning taotleda vajalikke jälitustoimingu lubasid selleks, et veenduda kas sotsiaalmeediast leidub antud kriminaalasja menetlemiseks vajalikke tõendeid. Siinkohal võib öelda, et praegusel sotsiaalmeedia ajastul on KrMS § 126^9 säte iganenud ning vajaks kaasajastamist.

Järgmine õiguslik küsimus, mis võib tekkida sotsiaalmeediast andmete kogumisega kriminaalmenetluse huvides, on see, kui kogutakse konkreetselt andmeid kriminaalmenetluses olulist rolli omava isiku suhtes. Probleemne koht seisneb selles, kas tegemist on varjatud jälgimisega või mitte. KrMS § 126^5 järgi on varjatud jälgimine jälitustoiming, mille teostamiseks annab loa prokuratuur. Ühelt poolt inimene jagab oma andmeid avalikult sotsiaalmeedias, mis on kõigile vabalt näha. Teiselt poolt uurimisasutus kogub neid samu andmeid süstematiseeritult ning vajadusel vormistab nendest tõendeid. Andmete kogumine justkui toimub inimese eest varjatult ning tal puudub võimalus saadud teabe ümberlükkamiseks. Kehtiva seaduse kohaselt ongi hetkel ebaselge, kas selline tegevus ületab jälitustoimingu piiri või mitte.

Põhiseaduse § 26 järgi ei tohi riigiasutused sekkuda kellegi perekonna- ega eraellu muidu, kui seaduses sätestatud juhtudel ja korras (Eesti Vabariigi põhiseadus, 1992). EIK käsituses hõlmab eraelu ka avaliku informatsiooni kogumist ja talletamist (Rotaru v. Romania, 2000). Jälitustoimingud võivad olla oma olemuslikult isikute eraelu riivavad ning seetõttu on oluline, et kõik toimingud kriminaalmenetluse huvides oleksid algusest peale seaduslikud. Riigikohtu otsuses nr. 3-1-1-22-10 punktis 14.4 on öeldud, et kriminaalmenetluse läbiviimine ametiisiku poolt on riigivõimu teostamine ning kohtueelset menetlust läbiviiv ametiisik on seotud kehtiva kriminaalmenetlusõigusega ega saa jätta seda rakendamata ning eriti rangelt tuleb seda järgida jälitustegevuses (V. R., T. S & A. P. kriminaalasi karistusseadustiku §-de § 293, 295 ja 297 järgi, 2010). Selle otsusega ütleb riigikohus konkreetselt, et kriminaalmenetluste läbiviimisel tuleb rangelt järgida seaduseid, mis tähendab, et siinkohal ei tohi eksida ka avalikest andmetest info kogumisega. Lisaks on Riigikohus öelnud oma otsuse nr. 3-1-1-63-08 punktis 13.2, et jälitustoimingute puhul on tegemist spetsiifiliste menetlustoimingutega tõendite kogumiseks ning neid iseloomustab varjatus jälitustoimingutele allutatud isikute ees, mis tähendab, et jälitustoimingud võivad riivata isiku põhiõigusi intensiivsemalt kui mis tahes muu uurimistoiming ning sellest tulenevalt on isikul takistatud KrMS § 34 (Kahtlustatava õigused ja kohustused) loetletud õiguste realiseerimine (A. K. & R.P kriminaalasi karistusseadustiku § 184 järgi, 2008). Sellega annab Riigikohus mõista, et jälitustoiminguid tehes puudub inimesel võimalus ennast õigel ajal kaitsta. Võrdluseks võib välja tuua olukorra, kus isik jagab oma sotsiaalmeedia kontol ennast süüstavat informatsiooni, mida ta ei teeks juhul, kui teaks, et on politsei poolt jälgitav.

1.5.2. Andmelekete kasutamine

Avalike andmete puhul tuleb arvestada ka andmeleketega, mis omakorda tekitab õigusliku dilemma, kui lekkinud andmeid kasutatakse uurimisasutuste töös. Andmelekke all mõeldakse käesolevas töös andmeid, mis on andmevaldaja tahte vastaselt avalikuks tehtud. Ühelt poolt võib andmelekete puhul olla tegemist varastatud teabega, mis on avaldatud kas siis tumeveebis või mõnes teises keskkonnas, kuid on kõigile soovijatele kättesaadav. Teiselt poolt võib saadud teave olla oluline lüli kuriteo toimumise kohta, mille põhjal on võimalik alustada kriminaalmenetlust või saada vajalikke andmeid menetluse lahendamiseks. Kuriteo lahendamise puhul saame näitena tuua erinevate keskkondade lekkinud kasutajanimed ja paroolid, mida kasutades on võimalik jõuda võimaliku kahtlustatavani, kes on toime pannud küberkuriteo või kelmuse internetis. Sellisele tulemusele on võimalik jõuda oskusliku andmeanalüüsi tulemusena, kui võrrelda omavahel erinevaid lekkinud andmebaase kasutajanimede ja paroolide osas. Võimaliku kuriteo tunnuste kohta lekkinud andmetest saab välja tuua „Panama paberite“ juhtumi, mis paljastas vähemalt 35 praegust ja endist maailma juhtivat isikut ning üle 300 praeguste ja endiste poliitikute ülemaailmseid seoseid *Offshore* tehingutega (Bhuiyan, 2023, p. 246). „Panama paberite“ skandaalile reageeris ka Euroopa Parlament, luues eraldi komisjoni, kelle ülesandeks oli hinnata Euroopa Komisjoni ja liikmesriikide tegevust võitluses rahapesu ja maksudest kõrvalehoidumisega (Euroopa Parlament, 2016). Lisaks on teada, et Saksamaa on seoses rahapesuga alustanud vähemalt ühe uurimise antud lekke põhjal (Koovit, 2018).

Andmelekete puhul saab probleemina välja tuua nende kasutamise tõendina. Ühelt poolt saab öelda, et lekkinud andmed oma olemuselt võivad liigituda KarS § 202 alla, milleks on süüteo toimepanemise tulemusena saadud vara omandamine, hoidmine ja turustamine (Karistusseadustik[1], 2001, § 202). Varana saab käsitleda ka rahaliselt hinnatavate õiguste ja kohustuste kogumit nii majanduslikus varamõistes kui ka juriidlises varamõistes (Sootak & Pikamäe, 2021, lk 694). Samas KrMS § 63 lg 2 järgi võib kriminaalmenetluse asjaolude tõendamiseks kasutada ka käesoleva paragrahvi lõikes 1 loetlemata tõendeid, välja arvatud juhul, kui on tegemist kuriteo või põhiõiguse rikkumise teel saadud tõendiga (Kriminaalmenetluse seadustik[1], 2003). Seejuures on Tartu Ringkonnakohus öelnud, et kriminaalmenetluse seadustikus pole otsest keeldu rajada mingit menetlustoimingut

sellisele informatsioonile, mis sai menetlejale teadlikuks mõne seaduserikkumise tõttu ning tuleks küsida, kas olukord on samasugune ka siis, kui info ebaseaduslikult hankijaks oli riik, mitte eraisik (V. S. kriminaalasi KarS § 300^1 lg 2 järgi, p. 111, 113). Omakorda on Riigikohus öelnud, et tõendi lubatavuse üle otsustamiseks on vajalik hinnata rikutud normi eesmärki ja seda, kas selliseid tõendeid poleks saadud, kui normi ei oleks rikutud ning tõend on lubamatu üksnes sellisel juhul, kui tõendi kogumise korda on oluliselt rikutud (H. K. kriminaalasi KarS § 199 lg 2 p-de 5, 8 ja 9, § 213 lg 2 p 1 ning § 323 lg 1 järgi, p. 58; R. K. väärteoasi liiklusseaduse § 74^{19} järgi, 2005, p.7.4). Lisaks on Riigikohus öelnud, et kriminaalmenetlusevälise toiminguga kogutud tõendi kasutamine võib olla lubamatu siis, kui selle saamisel ei ole järgitud KrMS §-s 64 sätestatud tõendite kogumise üldtingimusi (R.F. kriminaalasi KarS § 361 lg 1 järgi, 2011). Siinkohal võib justkui eeldada, et lekkinud andmeid võib kriminaalmenetluses kasutada, kuna uurimisasutus ise ei riku andmete saamisel KrMS § 64 välja toodud norme, kui uurimisasutus saab andmed kohast, mis on kõigile ligipääsetav. Seega kui lekkinud andmeid saada mõne menetlustoiminguga nagu läbiotsimisel saadud arvuti läbivaatamise teel, siis sellist probleemi ei teki, sest erinevate kriminaalmenetluste vahel on tõendite ristkasutamine lubatud.

Üldjoontes saab öelda, et avalike andmete kogumisel ja kasutamisel kriminaalmenetluse raames Eestis olulisi õiguslikke piiranguid ei ole. Oluline on, et andmete kogumisel teadvustataks, et neid kogutaks kriminaalmenetluse raames eesmärgipäraselt ning ei rikutaks kehtivaid õigusnorme. Õigusnormide järgimine muutub eriti oluliseks siis, kui avalike andmete kogumisel ja analüüsimisel võetakse kasutusele tehnoloogilised vahendid. Seda eelkõige sellepärast, et tehnoloogiliste vahenditega on võimalik teostada massilist andmete kogumist nii meediast kui ka sotsiaalmeediast ning kui hakata saadud andmeid inimeste vastu valimatult ära kasutama, võidakse õõnestada inimeste usaldust erinevate sotsiaalmeediaplatvormide suhtes (Southerton & Taylor, 2020, p. 2).

1.6. Tehnoloogilised vahendid avalike andmete kasutamisel kriminaalmenetlustes

Kriminaalmenetlused oma olemuselt võivad olla väga mahukad ning keerulised. Mahukate ja keeruliste kriminaalasjade puhul võib olla tegemist suurte andmehulkadega,

millest on vaja üles leida olulised andmed ja andmeid omavahel võrrelda. Suuri andmehulki võib sageli saada läbi erinevate päringute, kuid samuti on võimalik andmeid koguda internetist.

Internetist avalike andmete kogumiseks ning analüüsimiseks on loodud erinevaid tarkvaralisi ja tehnoloogilisi lahendusi, mis lihtsustavad tööprotsessi ning aitavad aega kokku hoida, mis muidu kuluks andmete käisitsi otsimisele ning nende analüüsimisele. Kohad, kust võib leida kriminaalmenetluseks olulisi avalikke andmeid, on erinevad ajakirjanduslikud portaalid, erinevad blogid, foorumid, avalikud dokumendid, erinevad sotsiaalmeediaplatvormid, teadusartiklid, satelliidipildid ja kaardid, erinevad avalikud andmebaasid ning muud interneti allikad (Quick & Choo, 2018, p. 560; Settanni, *et al.*, 2017, p. 172). Tihtilugu võib asja keeruliseks teha see, et avalikud andmed võivad sisaldada ka mitmeid erinevaid tehnoloogilisi elemente (domeenid, veebiaadressid, protokollid, pealised, koodid, skriptid, IP aadressid, sertifikaadid, kasutajanimed jpm), mis nõuavad kasutajalt häid infotehnoloogilisi oskuseid (Rahwan, 2022, p. 5). Selleks, et nendest kõikidest erinevatest avalike andmete allikatest andmeid kokku koguda, on loodud erinevaid tarkvaralisi ja tehnoloogilisi lahendusi. Tarkvaraliste ja tehnoloogiliste lahenduste abil saadavad suurtest andmehulkadest on vajalik eraldada ebaolulised andmed, et andmeid oleks võimalik edasi analüüsida (Pai & Prasad, 2021, p. 7). Samuti on võimalik suure andmehulgaga töötades kindlaks teha korrelatsioone konkreetsete andmekogumite vahel, et tuvastada mustreid, mille alusel on võimalik teostada ennustatavat analüüsi (Katz, 2020, p. 2). Analüüsitud andmetest on võimalik teha selgemaid järeldusi edasiste tegevuste planeerimiseks või saada menetluse jaoks vajalikke tõendeid.

Avalike andmete tööriistade kasutamisest võib näitlikustamiseks välja tuua Maailma Terviseorganisatsiooni loodud süsteemi nimega "*Hazard Detection and Risk Assessment System*" (eesti keeles: ohtude avastamise ja riskihindamise süsteem), mis kasutab ülevaate saamiseks veebipõhiseid epideemia jälgimise tööriistu nagu Medisys, GPHIN, HealthMap, Promed-mail ning palju teisigi. GPHIN (ingl k *The Global Public Health Intelligence Network*) on poolautomaatne hoiatussüsteem, mis skaneerib globaalseid meediaallikaid üheksas erinevas keeles, otsides kindlaid märksõnu, fraase ja muid potentsiaalseid märke võimalikust epideemiapuhangust ning on võimeline tootma 2000

kuni 4000 igapäevast aruannet ning andma automaatset häiret. Kuna info hulk, mida kogutakse, on suur, siis järelduste tegemiseks kasutatakse erinevaid algoritme. Tehnoloogia kasutamine on ennast ka õigustanud, kuna tänu GPHIN, ProMED ja HealthMap on saadud hoiatusi mõningate suurte haiguspuhangute kohta. (Bernard, *et al.,* 2018, p. 510)

Eelpool toodud näide on küll väga spetsiifiliselt ühe valdkonna põhine ning ei ole otseselt seotud käesoleva magistritöö teemaga, kuid see ilmestab, mida on võimalik saavutada erinevaid automatiseerituid lahendusi kasutades. Iga töö või valdkonna jaoks ei ole sellist lahendust veel loodud, eriti veel konkreetselt kriminaalmenetluste vajadusi arvestades. Menetluse eripärast olenevalt on vajalik kasutada erinevaid tarkvaralisi lahendusi. Paljud võimekad tarkvaralised lahendused on tasulised ja kallid nagu „Maltego“, „SEON“, „Lampyre“, „SpiderFoot“ ning eeldavad kasutajalt häid infotehnoloogilisi oskuseid. Kuid siiski on olemas ka palju vabavaralisi lahendusi. Üheks kohaks, kust on võimalik leida sobivaid vabavaralisi lahendusi on veebilehekülg „*OSINT Framework*“, mille fookuseks on koondada kokku kõik tasuta saadaolevad tööriistad ja allikad, et viia edukalt läbi andmeotsinguid (OSINT Framework, 2022). Lisaks on „Bellingcat“ koondanud mitmeid erinevaid võimekaid tarkvaralisi lahendusi nende hallatavasse „*Google Sheet*“ keskkonda aadressil „https:// bit.ly/bcattools“.

Inglismaal Kenti ülikoolis avaldati 2022. aastal uuring, kuidas riiklikud arvutiturbeintsidentidele reageerimise meeskonnad kasutavad avalikke andmeid ja tasuta saadavaid tarkvarasid oma töös. Uuringus viidi läbi poolstruktureeritud ekspertintervjuud 25. osalisega 13. erinevast riigist. Kõik uuringus osalenud leidsid, et avalike andmete kasutamine ja tasuta saadaolevate tarkvarade kasutamine tuleb nende töös kasuks. Samuti leidsid mitmed uuringus osalenud eksperdid oma tööle tuginedes, et mitmete tasuta saadavalolevate tarkvaradega on võimalik saada sama tulemus, mida on võimalik saada tasulise tarkvaraga. (Kassim, *et al.,* 2022, pp. 264–268)

Ameerika Ühendriikide ülikoolide teadlased avaldasid aastal 2017 uuringu, mis puudutab terroristlike organisatsioone Aafrikas. Uuringu eesmärgiks oli leida, kuidas on võimalik tuvastada äärmuslaste käitumist internetis. Andmed, mida uuringus kasutati, olid kogutud avalikest allikatest ning nende analüüsimiseks kasutati erinevaid tarkvaralisi lahendusi ja

programmeerimiskeeli nagu *The Metasploit Community Edition (CE), Python, R, RapidMiner* ja *KNIME.* Uuringu fookuseks võeti terroristlikud grupeeringud Al-Shabaab ja Boko Haram ning keskenduti nende sotsiaalmeediakontode tuvastamisele. Uuringu tulemusena tõdeti, et tehnoloogilised vahenditega on võimalik tuvastada mitmeid tõenduslike seoseid kontodega, kuid andmete kinnitamiseks on oluline, et inimene vaatab kõik olulised seosed üle ning annab enda hinnangu sobivuses. (Dawson, *et al.,* 2017, pp. 159–163*)*

Nagu eelmises lõigus oli välja toodud, et tehnoloogiliste vahenditega on võimalik leida sotsiaalmeediast piisavalt tõendeid teatud kontode seotuse kohta terroristlike võrgustikega, siis see näitab kui oluline roll on sotsiaalmeedial avalike andmete kogumises. Ühendkuningriigi politsei ja kuritegevuse voliniku büroo tegevjuht Fraser Sampson (2017, p. 56) on välja toonud, et blogidest, sisukogukondadest (nt. YouTube) ja sotsiaalmeediast saadav teave on väga oluline nii info kogumiseks kui ka võimalikeks tõenditeks kriminaalmenetluses. Võttes arvesse, et juba praegu mängivad olulist rolli erinevad sisukaevandamise (ingl k *text mining)* tarkvarad, mille eesmärgiks on kategoriseerida uudiste artikleid, e-kirju, filtreerida rämpsposti või analüüsida erinevat sisu ning seda on võimalik integreerida masinõppega (Kotze, *et al.,* 2020, p. 1). Kui nüüd integreerida sotsiaalmeedia sisu läbivaatust sisukaevandamise ja masinõppe tarkvaraga, siis on võimalik saadud andmetest koostada kasutajate psühholoogilisi profiile, millest saadud teavet on võimalik kasutada ohtude ja rünnakute ennetamiseks (Panagiotou, *et al.,* 2019, p. 3). Rumeenia riiklikust luureakadeemiast on Urgenau (2021, p. 199) välja toonud, et see kuidas jõustruktuurid kohanduvad avalike andmete kogumise tehnoloogilise protsessiga, on oluline edutegur, seda eelkõige olukorras, kus on võimalik kasutada tehisintellekti konkreetsetes andmete kogumise faasides ning kasutatavates tarkvaraplatvormides. Tehisintellektiga on võimalik kasutada tõhusaid automatiseeritud lahendusi andmete töötlemise etapis ning samuti hilisemas analüüsietapis, lisaks on võimalik luua stsenaariumianalüüs, prognoosiv analüüs nii korduvate kui ka tulevaste mustrite põhjal (The Economist Ingelligence Unit, 2019, p. 3).

Kriminaalmenetluse puhul on oluline näidata tõendite kujunemist ning seda eriti just avalike andmete kasutamisel. Siinkohal saab samuti välja tuua erinevad tarkvaralised lahendused, mis aitavad talletada (ekraanil tegevuste salvestamine videona või

kuvatõmmistena) kogu andmete kogumise protsessi, et oleks üheselt arusaadav, kust ning läbi milliste päringute, otsisõnade või tegevuste millistele tulemusteni jõuti (Baror, *et al.,* 2021, p. 582). See on oluline, et tõend oleks usaldusväärne ja autentne ning samuti tõendamaks, et tõendi saamisel ei ole rikutud õiguslike norme (Gregory, 2022, p. 710).

Käesolevas peatükis käsitletu põhjal saab öelda, et avalike andmete kasutamine aitab kaasa uurimisasutuste tööle sh. tõhustab võitlust kuritegevuse vastu (eriti raske peitkuritegevuse, samuti aitab kaasa kuritegude kiiremale avastamisele ning kriminaaltulu tuvastamisele). Kriminaalmenetlustes on oluline jälgida, et avalikest allikatest andmete kogumisel jälgitaks KrMS-s sätestatut. Eriti oluline on olla ettevaatlik õiguslikult „hallis alas" või selgelt reguleerimata olukordades, kuna ebaseaduslikult kogutud tõendid võivad kaasa tuua süüdistuse äralangemise kohtus. Seega on oluline kahtluse korral, et tegemist võib olla jälitustegevusega, pigem eelnevalt taotleda vajalik jälitustoimingu luba. Lisaks võivad olla avalikest allikatest kogutud andmed mahukad ning nende andmemahtude analüüsimiseks (ja kogumiseks) võib olla vajalik kasutada erinevaid tehnoloogilisi ja tarkvaralisi lahendusi, mis omakorda suurendavad nõudeid ametniku infotehnoloogilistele pädevustele. Siinkohal on oluline, et viidaks läbi kvaliteetseid koolitusi, mis aitavad ametnikel ajaga kaasas käia kasutamaks kaasaegseid tehnoloogilisi võimalusi ning omaksid teadmisi andmekogumise võimaluste kohta (Kim, *et al.,* 2017, p. 11; Peters & Ojedokun, 2019, p. 169; Rahwan, 2022, p. 17). Lisaks aitab koolituste läbiviimine ametnikel mõista avalike andmete kogumise, analüüsimise ja nende kasutamise potentsiaali kriminaalmenetlustes, ilma et ületataks võimalikke õiguslikke piiranguid.

2. AVALIKE ANDMETE RAKENDUSVÕIMALUSTE UURING

Magistritöös kasutatakse kvalitatiivset uurimisviisi, kuna see võimaldab läbi viia intervjuusid, vaatlusi ning dokumentide tõlgendusi, mis omakorda võimaldab leida mustreid ja teemasid käitumiste selgitamistel (Patton, 2015, p. 48). Kvalitatiivse uurimuse raames viiakse läbi empiiriline uuring, mis tähendab, et kogutakse andmeid tegelike tähtsuste ja fenomenide kohta. Empiirilise uuringu eesmärgiks on välja selgitada, kuidas kasutatakse avalikke andmeid kriminaalmenetluses. Uuringu eesmärgiks on aru saada, kas avalikke andmeid kasutatakse politseitöös piisavalt, millised on senised kitsaskohad avalike andmete kasutamisel ning kuidas oleks võimalik saadud andmeid paremini koguda ja kasutada.

Esimeses alapeatükis kirjeldab magistritöö autor läbiviidud empiirilise uuringu metoodikat ja uuringu valimit. Teises alapeatükis tuuakse välja läbiviidud uuringu tulemused.

2.1. Uurimismetoodika ja uurimuse käik

Magistritöö puhul on tegemist rakendust loova arendusuuringuga, mis tegeleb mingi eluvaldkonna praktiliste probleemide lahendamisega konkreetsete kasutajate vajadusi arvestades ning lähtub vastuoludest, vajakajäämistest või uuest ideest ja vajadusest midagi muuta või parandada (Tallinna Ülikool, 2015, lk. 18). Uurimismeetodiks on valitud individuaalne kvalitatiivintervjuu, mis sobib delikaatsete või keerukamate teemade uurimiseks ja parendamiseks ning võimaldab aru saada intervjueeritava kogemustest, mille eesmärgiks on arendada uuritavat nähtust (toimimise loogikat või kasutust) (Kidron, 2007, lk 123; Kval & Brinkmann, 2009, p. 10).

Uuringu valim on eesmärgistatud valimi (ingl k *purposive sampling)* meetod, mis tähendab, et valitakse kindel sihtrühm inimesi. Käesolevas magistritöös oli valimi sihtrühmaks PPA ja MTA ametnikud, kelle igapäevatöö üheks osaks on avalike andmete kogumine ja analüüsimine, nendest taustteabe ja tõendite eristamine ning saadud tõendite vormistamine. Riigiprokuröride valimi puhul olid olulised nende poolt juhitud

kriminaalmenetlused, kus on kogutud tõendeid avalikest allikatest ning saadud tõendeid on kasutatud kohtus. Eesmärgistatud valimi puhul on vastajad valitud olulise informatsiooni saamiseks, mida nad on kõige sobivamad andma. (Teddlie & Yu, 2007, p. 77)

Andmekogumise meetodina viidi läbi poolstruktureeritud ekspertintervjuud (Flick, 2009, pp. 156–169). Laherand (2008, lk 181) on välja toonud, et poolstruktureeritud intervjuud on kvalitatiivsetes uuringutes levinum andmekogumisviis. Intervjuu puhul saab olulise asjana välja tuua, et see annab võimaluse koguda andmeid vastavalt tekkinud olukorrale ning saadud vastuste tõlgendamiseks on erinevaid võimalusi (Hirsjärvi, *et al*., 2005, lk 192). Poolstruktureeritud intervjuude kasuks räägib asjaolu, et see võimaldab esitada täpsustavaid küsimusi. Lisaks aitavad intervjuud leida vastuseid uurimisküsimustele, kui neid analüüsitakse koos teoreetiliste allikatega.

Intervjuude eesmärgiks oli välja selgitada ekspertide tegevused ja kogemused uuritud valdkonnas ning selleks viidi läbi ekspertintervjuud isikutega, kes puutuvad kokku kriminaalmenetlustega ning omavad teadmisi ja kogemusi avalike andmetega töötamisel (vt tabel 2). Lähtuvalt PPA peadirektori 30. juuli 2010 käskkirjale nr 337 küsiti PPA uurimistööde kooskõlastamise komisjonist luba uuringu läbiviimiseks PPA-s ning saadi selleks komisjoni kooskõlastus 24.01.2023 nr. 1.1-14/12-2. Kõik intervjueeritavad osalesid uuringus vabatahtlikult. Arvestades, et politsei ja piirivalve seaduse § 4 lg 5 järgi on PPA kriminaalpolitsei isikkooseis asutusesiseseks kasutamiseks mõeldud teave avaliku teabe seaduse tähenduses ning asjaoluga, et enamik intervjueeritatavaid soovis jääda anonüümseks, ei tooda töös välja intervjuu andnud isikute nimesid (Politsei ja piirivalve seadus[1], 2009) .

Tabel 2. Intervjuus osalenud eksperdid (autori koostatud)

	Intervjueeritava tunnus	**Asutus**	**Intervjuu toimumise aeg ja kestvus**
1.	ST	PPA	17.02.2023; 46 minutit
2.	ST2	PPA	19.02.2023; 58 minutit

3.	ST3	PPA	22.02.2023; 45 minutit
4.	ST4	PPA	01.03.2023; 50 minutit
5.	ST5	MTA	02.03.2023; 55 minutit
6.	ST6	PPA	03.03.2023; 52 minutit
7.	ST7	PPA	08.03.2023; 48 minutit
8.	ST8	Riigiprokuratuur	10.03.2023; 1 tund 1 minut
9.	ST9	Riigiprokuratuur	13.03.2023; 51 minutit
10.	ST10	Riigiprokuratuur	23.03.2023; 52 minutit

Intervjuu küsimused koostati lähtuvalt magistritöö uurimisküsimustest ning tugineti esimese peatükis ilmnenud teoreetilistele lähtekohtadele.

Enne intervjuu läbiviimist tutvustati intervjueeritavale magistritöö eesmärki, metoodikat ja valimit ning seejärel küsiti intervjueeritavatelt luba selle salvestamiseks. Füüsilistel kohtumistel intervjueeritavatega kasutati salvestamiseks iPhone SE (A2296) aplikatsiooni „*Voice Memos"*. Distantsilt läbiviidud intervjuud teostati IPhone SE (A2296) *FaceTime* funktsionaalsust kasutades ning salvestati läbi Windows 11 kaasas oleva tarkvaraga „Helisalvesti" või kasutati „*Skype for Business*" rakendust.

Intervjuude transkribeerimiseks kasutati TTÜ kõnetuvastus teenuse lahendust (Olev & Alumäe, 2022). Arvestades asjaoluga, et intervjuudes kajastatu sisaldab asutusesiseseks kasutamiseks mõeldud teavet, siis selleks sai kasutatud eelpool toodud vabavaralist lahendust, mille käivitamiseks kasutati „*VirtualBox 7.0.6*" tarkvara läbi „*Linux Ubuntu 22.04.2"* operatsioonisüsteemi. Kõnetuvastuse teenuse poolt transkribeeritud tulemused korrigeeris autor käsitsi.

Transkribeeritud intervjuusid analüüsiti tarkvaraga NVivo 1.7, kuhu sisestati kõigi läbiviidud intervjuude transkriptsioonid. Transkribeeritud failides tehti sisuanalüüs, mis

teostati läbi avatud kodeerimise (Flick, 2009, p. 309). Avatud kodeerimine tähendab, et sisust otsitakse kriitilisi termineid, võtmesündmusi või -teemasid, märgistamist ja esialgsete koodide määramist, mille tulemusena andmestik koondatakse kategooriatesse (Neuman, 2014, pp. 481–482). Transkribeeritud intervjuude kodeerimise tulemusena tehti kodeerimistabel (vt tabel 3) koos kategooriatega, alamkoodidega ning tuuakse välja koodide esinemise sagedus.

Tabel 3. Uurimisküsimustele vastamiseks kasutatud andmekogumismeetodid ja andmeanalüüsi kategooriad (autori koostatud)

Uurimisküsimus	**Andmekogumismeetod**	**Moodustatud kategooriad**
Uurimisküsimus 1: Millised andmed on avalikud andmed?	Poolstruktureeritud intervjuud (küsimus nr. 2)	Avalike andmete määratlemine.
Uurimisküsimus 2: Milline on praegune praktika avalike andmete kogumisel, analüüsimisel ja vormistamisel kriminaalmenetlustes?	Poolstruktureeritud intervjuud (küsimused nr 3, 4, 5, 10, 11, 12)	Avalike andmete kogumine, analüüsimine ja vormistamine kriminaalmenetluses.
Uurimisküsimus 3: Millised õiguslikud piirangud on avalike andmete kasutamisel kriminaalmenetlustes?	Poolstruktureeritud intervjuud (küsimus nr 7)	Õiguslikud piirangud avalike andmete kasutamisel kriminaalmenetluses.
Uurimisküsimus 4: Kuidas on võimalik avalikke andmeid kasutada kriminaalmenetluses ning millist lisaväärtust annab nende kasutamine kriminaalmenetlusele?	Poolstruktureeritud intervjuud (küsimused nr 6, 8, 9)	Avalike andmete kasutamise võimalused kriminaalmenetluses ja nende lisaväärtus.

Intervjuude sisu kodeerimine teostati manuaalselt NVivo võimalusi kasutades – automaatse kodeerimise funktsiooni ei kasutatud. Kodeerimiseks loodi uurimisküsimuste põhjal kategooriad, mille alla loodi omakorda koodid ning vajadusel alamkoodid, mille alla vastavad tekstilõigud liigitati (vt tabel 4). Eeltoodu võimaldab esitada uurimistulemusi analüütilise kirjatekstina, lähtudes püstitatud uurimisküsimustest. Analüütilist teksti ilmestati intervjuueritavate asjakohaste tsitaatidega.

Tabel 4. NVivo andmeanalüüsi kategooriad ja koodid (NVivo faili alusel autori koostatud)

Kategooria/kood/alamkood	Koodi esinemine intervjuudes	Koodi esinemissagedus
Avalike andmete määratlemine		
Avalikud andmed	10	37
Avalike andmete kogumine, analüüsimine ja vormistamine kriminaalmenetluses		
Kogumine	7	26
Otsimootorid	3	5
Sotsiaalmeedia	5	12
Analüüsimine	8	18
Vormistamine	10	37
Ametnike oskused	9	19
Õppekava ja koolitused	5	11
Tarkvara	4	14
Õiguslikud piirangud avalike andmete kasutamisel kriminaalmenetluses		
Selge regulatsiooni puudus	10	49
Libakontod	10	39
Sihistatud andmete kogumine isiku suhtes	8	28
Andmelekked	10	62
Avalike andmete kasutamise võimalused kriminaalmenetluses ja nende lisaväärtus		
Isikute kohta taustinfo kogumine	10	21
Tõendi saamine	10	24
Isikute tuvastamine	3	6
Kriminaaltulu	8	16
Kasutamine kriminaalmenetluses	9	25
Eeltöö	5	12
Info suunatud päringuteks	4	5

2.2. Ekspertintervjuude analüüs

Käesolevas alapeatükis tuuakse välja ekspertintervjuude tulemused. Ekspertintervjuud viidi läbi eesmärgiga saada vastuseid uurimisküsimustele. Selleks viis autor läbi 10 poolstruktureeritud ekspertintervjuud ekspertidega kolmest riigiasutusest, milleks olid Politsei- ja Piirivalveamet, Maksu- ja Tolliamet ning Riigiprokuratuur. Ekspertintervjuude analüüsimiseks koostas autor neli kategooriat: Avalike andmete määratlemine; Avalike andmete kogumine, analüüsimine ja vormistamine kriminaalmenetluses; Õiguslikud piirangud avalike andmete kasutamisel kriminaalmenetluses; Avalike andmete kasutamise võimalused kriminaalmenetluses ja nende lisaväärtus.

Esimesele uurimisküsimuse vastuse leidmiseks loodi kategooria **„Avalike andmete määratlemine“**, mis koosneb ühes koodist **„Avalikud andmed“**, mille eesmärgiks on kindlaks teha, kuidas eksperdid mõistavad avalike andmete olemust ning mida nemad peavad silmas selle mõiste all. Selle mõiste olemuse lahti mõtestamine on käesoleva magistritöö üks fundamentaalseid osi, sest kõik teised uurimisküsimused tuginevad sellel, mida mõistetakse avalike andmete all.

Ekspertintervjuudest selgub, et termini „avalikud andmed“ all mõistetakse eelkõige andmeid, mis on avalikult kätte saadavad ning milledele on kõigil inimestel võimalik ligi pääseda. Eksperdid toovad välja, et avalikke andmeid saab koguda erinevatest registritest (nii riiklikest, kui ka erasektori omadest), ajakirjanduslikest väljaannetest, erinevatest sotsiaalmeediaplatvormidest, foorumitest jpm. Enamus ekspertidest ei näe probleemi selles, kui mõnda keskkonda on vaja teha konto või maksta andmetele ligipääsemiseks tingimusel, et seda saab teha iga inimene. Samuti ei näe enamik ekspertidest probleemina, kui andmete saamiseks on vajalik kasutada eritarkvara, kui see tarkvara on kõigile vabalt kättesaadav – nt. tumeveebi sisenemiseks on vajalik kasutada TOR brauserit. Ekspertide arvamus ühtib teoreetilise käsitlusega, kus mõistetakse avalike andmete all informatsiooni, mida on kõigil inimestel võimalik internetist koguda, andmed võivad olla tasulised ning pärineda era- ja avaliku sektori käest (käesolev töö, lk 13–14).

„Kõigile kättesaadavad, aga see ei tähenda seda, et teinekord kõigile kättesaadavad andmed on ka sellised, mis ei tule otseselt vahetu guugeldamisega nagu seal esimese TOP10 vastuse hulka. Et aga kui ta on ikkagi nii-öelda avalikult ilma ühtegi sellist digitaalset barjääri ületamata, kaitsebarjääridest rääkimises KarS-i mõistes kättesaadavad, siis need on avalikud andmed /…/ Karistusseadustiku 217 alusel, mis räägib sellesse nendest takistuste ületamisest. Et ma kuskile ei lähe paroolist mööda ega väldi seda ukse lukku /.../ kui ta on ikkagi ligipääsetav, siis otse brauseri kaudu on mulle, siis on ta kõigile ligipääsetav./.../ Mina pean seda ikka avalikuks, sest ajakirjanduse eesmärk on seda avalikustada ja nii paljudele inimestele kui võimalik“ (ST3, 2023).

„/.../ nad on ju avalikud andmed, lihtsalt darkweebi ülesehitus natuke erineb tavalisest interneti ülesehitusest aga see on samuti suunatav ja see on samuti avalikkusele suunatud, /.../ Nii kaua kui paari klikiga saab sinna ligi, nii on nad küll avalikud, lihtsalt see darkneti ligipääs on tehtud natuke keerulisemaks ja darkneti kasutamine ei ole niivõrd mugav kui tavalise interneti kasutamine“ (ST2, 2023).

„Minu jaoks on avalikud andmed, esiteks selline teave, mis on kättesaadav avalike kanalite kaudu, nagu meediakanalid, internetiotsingud, avalikud veebilehеküljed, aga tegelikult minu jaoks on ka avalikud registrid ja selline kättesaadav avalik teave siis riiklikest registritest. /.../ Õige, sotsiaalmeediat pean ma ka avalikeks andmeteks, et kui see info ei ole mingite privaatsus piirangutega seal piiratud“ (ST10, 2023).

Mõned eksperdid seavad siiski kahtluse alla, kas avalike andmete alla kuuluvad ka tasulised ajakirjanduslikud andmed ja keskkonnad, kus on andmete kättesaamiseks vajalik luua konto. Need eksperdid põhjendavad oma arvamust sellega, et andmete kättesaamiseks on vaja teha lisategevusi ehk ületada keskkonna valdaja poolt seatud barjäär. Saab öelda, et nende ekspertide arvamus ei ühti teoreetilise käsitlusega. Lähtudes teoreetilisest käsitlusest, liigituvad ka ajakirjanduslikud andmed avalike andmete alla (käesolev töö, lk 14).

„Maksumüüri taga olevad andmed iseenesest on avalikud, lihtsalt nende andmete autor soovib saada siis teatavat tasu nende andmete kasutamise eest. Ehk ma ütleks, et see pigem on hall ala, puht juriidiliselt võiks öelda, et tegemist ei ole avalike andmete, sest ma pean tegema mingeid liigutusi neile ligipääsuks“ (ST7, 2023).

„Millest ei pea tegema siis vastavalt keskkonnatingimustele kasutajalt omale või tasu maksma selle eest“ (ST6, 2023).

Üldjoontes saab välja tuua, et ekspertide arusaam avalikest andmetest ühtib käesoleva töö teooriaosa peatükiga 1.1. Teooriapeatükis analüüsitud teaduskirjandusele tuginedes mõistetakse avalike andmete all teavet, mis on internetti avalikkusele üles pandud ning kõigil kasutajatel on sellele juurdepääs olemas. Juurdepääs võib küll olla piiratud maksumüüri või vajaliku konto olemasoluga, kuid seni kuni kõigil on võimalik luua vajalik kontod või maksta nõutud summa teabe eest, siis on tegemist avalike andmetega. Ekspertide eriarvamust mõningatest avalike andmete osadest võib seletada sellega, et puudub ühtne rahvusvaheliselt tunnustatud definitsioon, mida täpsemalt saab nimetada avalikeks andmeteks.

„Avalik teave see on nagunii lai mõiste. Ta on esiteks defineerimata mõiste, see nagu sinna alla on võimalik absoluutselt kõike mahutada“ (ST8, 2023).

Parema selguse huvides, eriti kui kasutada avalikke andmeid kriminaalmenetluses, oleks parem kui mõiste oleks defineeritud või piiritletud kas mõnes õigusaktis või kohtulahendis. Autor näeb eelkõige probleemse kohana olukorda, kui andmeid kogutakse keskkondadest, mis vajavad kasutajakontot. Arvestades asjaoluga, et juba 10 eksperdi seas polnud selles ühtset seisukohta, siis menetlusliku poole pealt võivad tekkida probleemid kohtus, sest nii kaitsjad kui ka kohtunikud ei puurgi nõustuda, et vastav teave on avalikult kõigile kättesaadav teave. Sellest tulenevalt võib kohus jõuda järeldusele, et tõenduslik teave (olulised andmed) on kogutud valedel alustel.

Järgnevalt selgitab magistritöö autor välja vastuse teisele uurimisküsimusele „**Milline on praegune praktika avalike andmete kogumisel, analüüsimisel ja vormistamisel kriminaalmenetlustes?**“. Vastuse saamiseks loodi kategooria **„Avalike andmete kogumine, analüüsimine ja vormistamine kriminaalmenetluses“**, antud kategoorias on 6 koodi: kogumine, tarkvara, analüüsimine, usaldusväärsus, vormistamine, ametnike oskused.

Lõigud eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1].

Koodi **tarkvara** juures nähtub, et uurimisasutuste eksperdid ei kasuta andmete kogumisel kommertstarkvaralisi lahendusi ning andmete kogumine on suuresti käsitöö. Mõni ekspert kasutab siiski vabavaralisi Pythoni skripte või brauserite laiendusi, mis lihtsustavad andmete kogumist. See näitab, et tasuta tarkvaraliste lahenduste kasutamine võimaldab teostada efektiivselt avalike andmete kogumist, mis ühtib teooriaosa alapeatükis 1.6 välja toodud Inglismaal Kenti ülikoolis läbi viidud uuringuga, milles selgus, et tasuta saadaolevate tarkvaradega on võimalik saada sama tulemus kui tasuliste tarkvaradega (käesolev töö, lk 42). Üldiselt väljendavad eksperdid seisukohta, et kommertstarkvaraliste vahendite kasutamine on küll võimalik, kuid enamik võimekaid tarkvaralisi lahendusi on äärmiselt kulukad. Samuti toovad eksperdid välja, et puudub üks kindel universaalne lahendus, mistõttu oleks vaja kasutada mitmeid erinevaid lahendusi. Mitme erineva kommertslahenduse kasutamine on uurimisasutusele ja seeläbi riigile kulukas, kuna nende kasutamiseks on igal aastal vaja maksta litsentsitasusid. Lisaks seavad litsentsi kasutamistingimused enamasti piiranguid kasutajate arvule, mis

võimaldaks tarkvara kasutada vähestel töötajatel. Tasuta saadaolevate tarkvaraliste lahenduste kasutajate arv ei ole piiratud ning igaüks saab nendest kombineerida endale vajalikud tööriistad. Enamasti kasutatakse andmete kogumiseks brauserite laiendusi ning Pythoni koodijuppe, mis lihtsustavad andmete kogumist. Erinevate tööriistade kasutamine sõltub siiski konkreetselt sellest, milliseid andmeid on vaja koguda.

„/.../ eks see kogumine ongi ikkagi täna ju suuresti käsitöö. Ongi peamised tööriistad brauser, selle erinevad lisavidinad. /.../ iseenesest, ega siis need lahendused on kõigile kättesaadavad. /.../ Githubis on päris palju valmis kirjutatud, Pythoni skripte, mis lihtsustavad nende andmete kokku kogumist. Ja ka Chrome'i ja Firefoxi enda niiöelda veebipoodides hästi palju igasuguseid lisasid, mida sa võid lihtsalt juurde installida.“ (ST7, 2023).

Lõigud eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1].

Koodis **usaldusväärsus** selgub, et andmete usaldusväärsus on üks olulisemaid aspekte, mis mõjutavad andmete kasutamist ja tõlgendamist. Läbiviidud ekspertintervjuudest selgub, et erinevate andmete puhul võib olla keeruline veenduda nende usaldusväärsuses, eriti juhul, kui need on kogutud erinevatest keskkondadest. Seda kinnitab ka teooriaosas väljatoodu, et andmete rohkus internetis ja sotsiaalmeedias võib tähendada, et suur osa andmetest ei pruugi omada mittemingisugust tähtsust ning osad andmed ei pruugi olla tõesed (käesolev töö, lk 27). Kahetsusväärselt tuleb välja, et liiga palju rõhku andmete usaldusväärsuse kontrollimiseks ei rakendata, kui just tegemist ei ole ilmselgelt kahtlase teabega. See tähendab, et sageli piirdutakse lihtsalt andmete esitamisega, nii nagu nad kogutud on. Kuigi kriminaalmenetluse eesmärgiks on kuriteo fakti tuvastamine ja tõendite kogumine eesmärgiga tuvastada kahtlustatav ja talle süüdistuse esitamine, siis andmete usaldusväärsusel on suur roll (käesolev töö, lk 25). Tehes valedel alustel kriminaalmenetluslike toiminguid, võib see lõppeda kohtus nö süüdistuse kokkukukkumisega. Eksperdid rõhutavad, et avalikud andmed saavad olla pigem toetavad andmed ning muud menetluslikud toimingud peaksid kinnitama andmete õigsust ja kvaliteeti, et suur pilt oleks selge ja üheselt arusaadav. Oluline on rõhutada, et kuigi avalikest andmetest kogutud teabel on tõendiväärtus ning ka muud menetluslikud toimingud kinnitavad teabe õigsust, siis lõpliku seisukoha andmete usaldusväärsuses saab

ikkagi anda kohus, kui on ära kuulanud ka teise poole seisukohad. Seetõttu on oluline tagada andmete õigsus ja usaldusväärsus nii palju kui võimalik, et nende kasutamine otsuste tegemisel oleks võimalikult usaldusväärne ja täpne ning kui on kahtlust saadud teabe õigsuses, siis seda teavet mitte kasutada.

„Lõppastmes ikka see, et kohus kontrollib seda, teab, siis kui nad nii-öelda tõendina juba see teave kuskil, et nii nagu teisi tõendeid, kas, kas seal see teave on see nii-öelda eluliselt usutav, kas ta haakub teiste tõenditega ja, ja seeläbi nagu selle usaldusväärsus tõuseb /.../ Et see on see milline see sisu tal on, aga ütleme just see, et et selle usaldusväärsusega ongi see, et kuidagigi haakub seal teiste tõenditega, siis kohus peab selle hinnangu andma, on see usaldusväärne või mitte.“ (ST9, 2023).

„/.../ lõppkokkuvõttes otsustab, kas on tõene või mitte, kohtunik. Ühelgi tõendil ei ole ette määratud jõudu. Ja seda otsust ei tohiks vastu võtta ka politseinik /.../ politseinik peab aru saama, et kui mul on võimalik, siis ma pean nagu veenduma selles autentsuses, vaidlusi elimineerida eos. Aga kui see on nagu oluline asi ja fifty-fifty siis mina seda vormistamata ei jäta, ma ei üritaks seda mitte kuidagi muidugi ilustada /.../“ (ST3, 2023).

„/.../et see on see vana tõde, et kas sul on lubatud nii-öelda teadustööd tehes viidata Wikipeediale või mitte, arvestades seda, et wikipeedias võib igaüks ükskõik millist pläusti kirjutada, pigem mitte eks, ta peaks olema niiöelda respektaabel allikas. Avaliku teabega täpselt samamoodi, et igaüks võib ükskõik millist pläusti internetti üles, noh avalikkusele üles panna, et see, et see avalikult on välja hõigatud, ei muuda seda automaatselt tõeseks või usaldusväärseks /.../“ (ST8, 2023).

Koodis **vormistamine** selgub, et enamikel juhtudel on vajalik menetluses kasutatavate andmete kohta teostada vaatlusprotokoll, mille nõuded on sätestatud KrMS § 87 lg 1, kuid olenevalt olukorrast ja teabest võib piisav olla teabe välja printimine. Ekspertide seas läbiviidud intervjuudest selgub, et puudub selge nägemus kuidas on vaja avalikke andmeid vaatlusprotokollis esitada. Enamik eksperte, nii uurimisasutustest kui ka riigiprokuratuurist, leidsid, et oluline on kirjeldada kust, millal ning milliseid andmeid leiti ning vajadusel lisada ekraanitõmmised, mis peaksid tagama piisava usaldusväärsuse vaatlusprotokollile. Samas oli riigiprokuratuurist arvamusi, et vajalik on kogu vaadeldava veebilehe talletamine, et kogu selle sisu oleks hilisemalt taasesitatav. Kogu veebilehe

talletamine, koos sinna kuuluva funktsionaalsusega, on oma olemuselt keeruline protsess, mis nõuab ametnikelt eriteadmisi ja oskusi ning võib olla vastuolus seadusandlusega (nt. andmekaitsega või intellektuaalse omandiõigusega). Kogu veebilehe talletamine koos funktsionaalsusega võib olla ka ebamõistlik, eelkõige mahu tõttu ja see ei ole kooskõlas menetlusökonoomika põhimõtetega. Eksperdid nõustusid ka võimalusega, kus kasutatakse ekraanil tegevuse salvestamist, kus kogu protsess on videona jälgitav. Ekraanil kogu tegevuse salvestamine ei ole oma olemuselt keeruline protsess, kui on olemas vastav tarkvaraline lahendus. Eriti rõhutasid eksperdid, et avalikest andmetest tõendi saamine peab olema loogiliselt jälgitav. See on vajalik tuvastamaks, kuidas jõuti andmeteni, mida esitatakse, eriti kui kasutati eritarkvara. Oluline on, et kogu protsess peab olema korratav, et nii kohtunikul kui ka kaitsjal on samu samme tehes võimalik jõuda samale järeldusele. Mõningatel juhtudel võib see osutuda võimatuks, kui andmeid on veebist kustutatud või muudetud ning sellisteks olukordades ongi oluline menetleja poolt talletada ja fikseerida oma tegevus selliselt, et ei tekiks hilisemalt kahtlusi saadud tõendi usaldusväärus es. *Sisu eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1]*.

Üks ekspert tõi välja, et Eestis, mis kuulub kontinentaalsesse õigussüsteemi, on kriminaalmenetlus oluliselt formaliseeritum, kui näiteks Ameerika Ühendriikides, mis kuulub angloameerika õigussüsteemi. See tähendab, et Eestis kasutatakse liiga kantseliitlikku teksti ja on palju kohustuslikke blankette (protokolle), samas kui Ameerika Ühendriikides kirjutatakse eksperdi kogemuse järgi kõik väga lihtsalt lahti ning lisatakse väga palju näitlikke elemente. Siinkohal on oluline rõhutada, et Eesti ja Ameerika Ühendriikide õigussüsteemid on oma olemuselt väga erinevad. Ameerika Ühendriikides on vajalik lisaks kohtunikule teha kogu tõendite protsess selgeks ka vandekohtunikele, kes kutsutakse kokku kodanikest juhuvalimi teel ning nende haridus ja eluvaldkond võib olla vägagi erinev. Sellegipoolest arvab ekspert, et näitlike vahendite kasutamine Eestis võib aidata hilisemas kohtuvaidluses teha kohtunikule tõend arusaadavamaks, kuna kõik kohtunikud ei pruugi mõista kõiki tehnilisi nüansse, mida esitada soovitakse. See tähendab, et tõend on vaja teha nii arusaadavaks, et ilma eriteadmisteta inimene mõistaks konkreetse tõendi väärtust ning olemust.

„/.../ ma ise imetlesin kunagi oli see Ameeriklaste see Ghost Clicki asi, mida siis tegime siin Eesti ja Ameerika ühistöös, aga see, kuidas ameeriklaste süüdistus oli kokku kirjutatud, et meie süüdistused on nagu selline võib-olla mingi kantseliitlik ja mingisuguseid kohustuslikke blanketsete normidega. Aga Ameerika süüdistus, lugesin inglisekeelset süüdistust, see süüdistus oli nii lihtsas keeles, et ma sain IT osast aru, aga seda oli nii palju näitlikustatud siis piltidega, kus oli juurde julgetud, teha näiteks mingisuguseid punaseid ringe, et vaadake seda kohta, kui seal punase ringi kohale vajutatakse, siis avaneb selline hüpikaken ja kõik muu, et et, et just igasugused näitlikustamise viisid oleksid abiks. /.../ meie peame ju ka kohtu ära veenma lõpuks selles, et selline teave tõesti oli lihtsasti kättesaadav ja igaühele kättesaadav oleks selline asi, et seda ei ole raske koguda, siin ei ole vaja mingeid eriteadmised, mingi eri, väga erilised teadmised, süvateadmised. Et ma arvan see võiks olla, et et mingisugune digitaalne talletus nende juurde, kes seal siis mingi salvestis sellest kuidas on arvutiga töötatud või

näiteks selle veebilehe koopia, et sellest oleks abi, aga ma arvan, et need võiks need põhinõuded olla /.../“ (ST10, 2023)

Koodis **ametnike oskused** juhtisid peaaegu kõik eksperdid tähelepanu olulisele probleemile, milleks on ametnike oskused ja teadmised avalike andmetega tegelemisel. Eriti rõhutati, et uurimisasutuste ametnikud ei mõista tihilugu avalike allikate olulisust ning neid ei taheta või ei osata kasutada piisvalt. Veel toodi ekspertide poolt välja, et kõik ametnikud ei pruugi osata avalikest allikatest saadud tõendeid õigesti talletada. Rõhutati asjaolu, et mõnikord võivad tõendamisväärtust omavad avalikud andmed muutuda või kaduda ning seetõttu on oluline, et iga ametnik oskaks vajadusel tõendit talletada. Avalikud andmed, mis võivad muutuda võivad olla näiteks sotsiaalmeediapostitused, kus postituse tegija hilisemalt muudab sisu või kustutab postituse. Lisaks võivad erinevad õngitsusleheküljed eksisteerida ainult loetud tunnid, mistõttu ajaline faktor selliste lehekülgede talletamiseks on väga oluline. Iga ametniku oskus selliseid lehekülgi õigesti talletada on oluline veel sellepärast, et ametnikud võivad ise juhuslikult sattuda mõnele õngitsusleheküljele ning enne, kui eksperdid sellisest leheküljest teada saavad, võib lehekülg juba kadunud või muudetud sisuga olla.

„/.../ punkt üks, neid alati ei kasutata, punkt kaks on see, et ka ei osata. Et kui ikkagi minu poole pöördub, uurija, kes nagu ei oska põhimõtteliselt infot guugeldada, et kui ma nii-öelda a la kasvõi seda inimese nime Google'isse sisend sisestades juba saan kogu info kätte, aga ta ei ole seda esimest liigutust teinud, siis ma ütlen, et kuskil on probleem.“ (ST4, 2023)

“Mu hinnang on see, et mitte väga palju, ma arvan, et see kinni konkreetsetes isikutes /.../ laiema, nii-öelda lähenemise või vaatega, et nemad võib olla kasutavad seda aktiivsemalt ja rohkem. Ja kindlasti on inimesi, kes pole sellest kuulnudki ja ei oskagi nagu selles kategoorias mõelda.(ST9, 2023).

Mitmed PPA eksperdid rõhutasid, et ametnike oskused ja teadmised avalike andmete kasutamisel on tõsine probleem, mis vajab lahendamist juba rohujuure tasandil. Ekspertide hinnangul on vaja politsei- ja piirivalvekolledži õppekava täiendada avalike andmete otsimise, kogumise ja talletamise osas. See on oluline kuna lisaks kriminaalmenetlusele on võimalik avalikke andmeid kasutada nii korrakaitseliste

eesmärkide saavutamiseks kui ka haldusmenetluse raames. Kui kooli lõpetanud politseiametnikud oskavad õigesti avalikke andmeid otsida ja neid koguda, siis on neil võimalus tuua uut lähenemist ja kompetentsi üksustesse, kuhu nad tööle suunduvad. Lisaks toovad eksperdid välja, et ka juba töötavatele ametnikele on vaja teadvustada avalike andmete olulisust. Seda eelkõige sellepärast, et on tulnud ette juhuseid, kus ametnikud eksivad andmete vaatamisel ka tööalaseks kasutamiseks mõeldud andmebaasides, kuigi need andmed, mida vaadati, on kättesaadavad avalikult. Selleks, et tuvastada probleemi põhjus ja ulatus, on vajalik selgeks teha, kui paljud ametnikud on üldse kursis digitaalajastu võimalustega ning seejärel praegustele ametnikele korraldada asjakohaseid koolitusi, mille sisu peaks vastama nende ametikohale. Probleemi, miks avalikke andmeid kasutatakse ebapiisavalt, põhjus võib olla seotud ametnike puudulike arvutikasutamise oskuste ja kehva digitaalmaailma võimaluste tundmisega. Oskuste ja võimaluste puudumine võib olla tingitud politseiametnike keskmise vanusega, aga ka asjaoluga, et lähtuvalt töökoormusest ei jätku ametnikel aega iseseisvalt uute oskuste ja võimaluste tundmaõppimiseks (2021 aastal oli PPA keskmine politseiniku vanus 40 eluaastat; käesolev töö, lk 32). Eksperdid ei too eraldi välja, et probleem peitub vananevates ametnikes, vaid nende hinnangul on probleem pigem üleüldises elementaarses arvutikasutamise oskuses.

„/…/ mitte ainult avalikud allikad, me siin räägime ka digitõenditest on ju nagu selles mõttes, seadmetest ja asjadest, et samamoodi see analüüsi teema, et, et see, et inimesed ei oska Excelis Pivotit teha, võtame endalt päevi, tööpäevi võtab ära nagu. Et see nagu nagu väga hirmus vaadata.“ (ST3, 2023).

„/../kui sa pead andma sisekontrollile aru, et miks sa oma autot oled kolm korda läbi löönud, põhjendus on see, et ma tahtsin kontrollida kas mu kindlustus on kehtiv. Ja see tuleb nagu minust noorema kolleegi käest. Mina olen eks 30 pluss ja see tuleb noorema, kui kolmkümmend aastat vana kolleegi käest. Siis tekkis see küsimus, et kuule noh, avalikud andmed, et sa ei pea selleks kasutama politsei andmebaasi, mida sa ei tohi selleks kasutada, sul on kõriauguni avalikke andmebaase, kust sa saad selle kätte, ilma et sa peaksid selleks siis seadust rikkuma /…/ alustada tasub rohujuurest ehk siis alustada kadettidest. Seda saaks õpetada koolis ka kadettidele elementaarsel tasandile. Esimene mõte võiks olla see kas ma saan need andmed avalikest allikatest kätte, kui mul on vajalik

kellegi kohta mingit infot saada. Esimene mõte võiks olla Google*, siis võiks tulla see* Kairi*. Tsitaadi edasine sisu eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1].*

(ST7, 2023).

Lõigud eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1].

Koodis **kasutamine kriminaalmenetluses** selgus ekspertide intervjuudest avalike andmete kasutamise praegune praktika. Enamik eksperte oli seisukohal, et avalikest andmetest saadud teavet ei kasutata kriminaalmenetluste erinevates etappides piisavalt. Ainult üks ekspert arvas, et avalikke andmeid kasutatakse piisavalt. Erinevus võib tekkida sellest, kui palju ekspert väljaspool oma üksust teiste menetlevate üksuste ja nende tegevusega kokku puutub. Siinpuhul saab positiivsena välja tuua, et uurimisasutustes on üksusi, mis kasutavad kriminaalmenetlustes avalikke andmeid piisavalt, kuid üldiselt ning eelkõige arvestades enamiku küsitletud ekspertide seisukohti, on avalike andmete mitte kasutamine suur probleem. Suuremalt jaolt nähti probleemse kohana asjaolu, et uurimisasutuste ametnikud ei oska piisavalt tähtsustada avalikest andmetest tulenevaid võimalusi või ei osata nendega midagi peale hakata. Siinkohal võib uuesti välja tuua asjaolu, et ametnikel puuduvad piisavad teadmised avalikest andmetest, nende kasutamise võimalustest ning nende andmete kogumisest, analüüsimisest ja talletamisest. Nagu eelmise uurimisküsimuse vastusest selgus, siis ekspertide hinnangul jääb avalike andmete kasutamine enamasti ametnike teadmiste ja oskuste taha ning see on üleüldine probleem uurimisasutustes.

„/…/ Mu hinnang on see, et mitte väga palju, ma arvan, et see kinni konkreetsetes isikutes, et kes on võib-olla nagu kas siis uuendusmeelsemad või, nii-öelda laiema, nii-öelda lähenemise või vaatega, et nemad võib olla kasutavad seda aktiivsemalt ja rohkem.“ (ST9, 2023).

„/…/ma mõtlen, et väga palju andmeid tegelikult avalikult ei kasuta ja täna minu meelest tingimused loodud, et neid kasutada. Kas seda kõige mugavamad või mitte, selles on nagu teine küsimus.“ (ST6, 2023).

Järgnevalt selgitab magistritöö autor välja neljanda uurimisküsimuse „**Millised õiguslikud piirangud on avalike andmete kasutamisel kriminaalmenetlustes?**“ vastuse. Vastuse saamiseks loodi kategooria **„Õiguslikud piirangud avalike andmete kasutamisel kriminaalmenetluses“**, antud kategoorias on 4 koodi: sihistatud andmete kogumine isiku suhtes, selge regulatsiooni puudus, libakontod, andmelekked.

Arvestades kriminaalmenetlusega ning sellest tulenevate mõjudega menetluses puudutatud isikutele, siis on oluline järgida kehtivaid õiguslikke norme. Kuna internet on globaalne ning selles on palju erinevaid keskkondi, siis võib tekkida olukord, kus mingi teabe saamine võib olla reguleeritud erinevate õigusaktidega. Seega on magistritöö autori arvamusel oluline teada saada, kuidas eksperdid mõistavad avalike andmete kasutamise õiguslikku poolt.

Lõigud eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1].

Teoreetilise osa peatüki 1.5 ja ekspertide arvamuse analüüsist nähtub, et avalike andmete kasutamisel puudub selge regulatsioon (kood: **selge regulatsiooni puudus**) ning eksisteerib nö „hall ala“, eriti kui tegemist on sotsiaalmeediast andmete kogumisega või andmeleketega. KrMS sätestab, kuidas kriminaalmenetluses on vaja tõendeid koguda, samuti on sätestatud jälitustoimingute tegemise tingimused, nende liigid ning millistel

alustel võib toiminguid teha. Lisaks KrMS-le on tõendite kogumise ning jälitustoimingute kohta erinevaid kohtulahendeid, kus on analüüsitud nii tõendite kogumist kui ka jälitustoimingute lubatavusi. Siiski saab öelda, et avalike andmete kogumisel ja kasutamisel kriminaalmenetluses on ebaselgeid kohti. Siinkohal on eksperdid toonud välja, et on vaja selgemaid juhiseid või regulatsioone, kuidas avalikke andmeid kasutada võib – ka andmelekkeid. Samas kardavad eksperdid, et kui hakatakse avalike andmete kasutamist reguleerima, siis võidakse kogu tegevus üle reguleerida, mis pärsib lõpuks avalikest allikatest saadud teabe kasutamise lisaväärtust. Eriti rõhutatakse asjaolu, et uurimisasutuste tegevus sotisaalmeediast teabe kogumisel on selgelt ja üheselt reguleerimata, sealhulgas tingimused „libakontode" kasutamiseks. Kuna iga kuritegu ei luba teostada jälitustoiminguid, eriti politseiagendi kasutamist ning alati ei ole see ka otstarbekas, siis just see valdkond vajab kõige rohkem reguleerimist.

„Põhiline kitsaskoht täna, ma arvan, et ongi selle ala nii öelda ja avalike andmete asumine kohati hallis alas ehk siis ei ole seadusega reguleeritud, samas kui me hakkame seda seadusega reguleerima, võib see asi minna jaburaks ja absurdseks on, oli see vist Belgia või Hollandi näide, kus politseinik võib kellegi kontot vaadata ühe korra ja kui ta teist korda vaatab see on juba jälitamine, sellest peaks teavitama, me õnneks täna veel ei ole selles punktis." (ST7, 2023).

„Ma, mulle meeldiks, kui see oleks selgemini reguleeritud kasvõi kohtupraktika tasandil. Jällegi noh avalik teave ja avalik teave, seal on suur vahe eks ju, aga kui me, kuivõrd me jõudsime selle vestluse lõpuks ka nii-öelda nende Wikileaksi ja Panama paberiteni siis see on niuke nagu sogane vesi, kus mul oleks lihtsam kui ma teaksin õiget vastust või noh oleks selgemad juhtnöörid. Et näiteks Belgias on selline sellised teabe kasutamine tõendina keelatud. Et häkkimise ehk siis kuriteo toimepanemisel saadud tõendi kasutamine on kuritegu, Belgia regulatsiooni kohaselt. Eestis ta otsesõnu keelatud ei ole. Jah, ta ei lähe sul süüteona saadud asjana." (ST8, 2023).

Eksperdid nõustusid autori poolt välja pakutuga, et kui on tarvis kasutada andmelekkeid, siis kriminaalmenetluslikus mõttes on õigem ja seaduspärasem, kui need andmed saadakse mõne menetlustoimingu raames, näiteks kui lekkinud andmed on saadud kahtlustatava juures teostatud läbiotsimise käigus leitud arvuti läbivaatusest. Sellisel

juhul on võimalik saadud andmeid menetlustes kasutada, kuna tõendite ristkasutamine on kriminaalmenetluses lubatud tegevus.

Kokkuvõtvalt saab ekspertide seisukohalt välja tuua, et avalike andmete kasutamisel on oluline roll kriminaalmenetluste menetlemisel, kui osata andmeid õigesti koguda, analüüsida ning saadud tulemusi vormistada nii, et kogu tegevus on loogiliselt jälgitav ja võimalusel ka teiste osapoolte poolt kontrollitav. Avalike andmete puhul on oht, et need võivad ajas muutuda või kustuda ning alati ei pruugi saadud andmed olla usaldusväärsed. Seetõttu on oluline, et kui avalikke andmeid talletatakse tõendina, siis fikseeritakse täpselt millal ja kust on andmed saadud. Usaldusväärsuse kohalt rõhutavad eksperdid, et ainult avalike andmete põhjal ei tohiks kindlaid järeldusi teha, vaid need peaksid toetama teisi kogutud tõendeid. Avalike andmete kasutamise poolelt suurimaks probleemiks on uurimisasutuste töötajate kompetents, kes ei oska või ei tea kuidas avalikke andmeid tõhusalt kasutada.

2.3. Järeldused ja ettepanekud

Arvestades, millist lisaväärtust avalike andmete kasutamine võib kriminaalmenetluste menetlemisele juurde anda, on oluline, et uurimisasutuse töötajad teaksid neid võimalusi ja oskaksid neid efektiivselt kasutada. Nii teoreetilisest osast kui ka ekspertintervjuude analüüsist nähtub, et avalikke andmeid on võimalik koguda ja analüüsida erineval viisil ning saadud teavet on võimalik kasutada erinevate eesmärkide saavutamiseks. Ühe võimalusena, kuidas avalike andmete kasutamine võib muuta kriminaalmenetlusi efektiivsemaks, saab välja tuua taustteabe kogumise. Taustteabe järgi on võimalik määratleda keskkondi, kuhu teha suunatuid päringuid ning päringust saadud teavet on võimalik vormistada tõendina või planeerida järgmisi menetluslikke samme. Avalikest andemest võib saada olulisi tõendeid erinevate kuritegude lahendamiseks. Olulisteks tõenditeks võivad olla näiteks sotsiaalmeediakeskkondades levivad videod, kus on näha kuriteotoimepanemise fakt ja millest on võimalik tuvastada kahtlustatav ning leida täiendavaid tunnistajaid. Teise olulise tõendina saab välja tuua erinevad leheküljed, näiteks õngitsusleheküljed, mille eesmärgiks on saada kasutajatelt andmeid, mida saab kasutada kuritegude toimepanemiseks. Täiendavalt võib olla oluline tõend ka muu avalikest andmetest saadud teave, mis on oluline konkreetse kriminaalasja lahendamisel.

Siinjuures on oluline, et ei muututaks liialt sõltuvaks avalikest andmetest pärinevate tõendite kogumisest. Oluline on koguda tõendeid ka traditsioonilisel viisil. Parima tulemuse saab, kui kombineerida traditsioonilised võimalused digitaalmaailma võimalustega (s.o eelkõige avalike andmetega), nii täiendavad meetodid üksteist, muutes kriminaalmenetlused efektiivsemaks.

Lõigud eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1].

Veel võib probleemina välja tuua asjaolu, et puudub ühtne nägemus kuidas avalikest allikatest pärit tõendeid vormistada – eelkõige kuidas neid talletada, et säiliks tõendi usaldusväärsus.

Järgmise probleemse kohana toodi välja, et kahjuks ei kasutata avalikke andmeid kriminaalmenetlustes piisavalt ning seda eelkõige seetõttu, et ametnikel puuduvad vajalikud teadmised ja oskused. Samuti leiti, et ametnikel on puudulikud teadmised enda kaitsmisest võimalike ohtude eest, kui avalikke andmeid kogutakse sotsiaalmeediast.

Lähtudes teooriast ja empiirilisest uuringust toob magistritöö autor ettepanekuna välja, et uurimisasutuste ametnikele on vaja viia läbi ametialaseid koolitusi, millega näidatakse avalike andmete kasutamise võimalusi. Sealhulgas on oluline, et menetlejad oskaksid märgata avalike andmete seas tõendeid ning teaksid kuidas neid õigesti koguda,

analüüsida ja talletada. Lisaks on oluline, et menetlejad teaksid avalike andmete kogumise potentsiaalseid ohukohti, et ei seataks ohtu võimalikku käimasolevat kriminaalmenetlust.

Teise ettepanekuna toob magistritöö autor välja, et avalike andmete kasutamise teadlikkust on vaja hakata õpetama juba politseikoolis ehk rohujuure tasemelt. Kui avalike andmete kasutamise teadlikkus integreerida politseiametniku väljaõppe baaskursustesse, siis see avardaks tulevaste politseitöötajate silmaringi ning annaks oskusi tulevikus avalike andmete laiemaks kasutamiseks. Lisaväärtusena annab see võimaluse vältida olukordi, kus ametnik enda teadmatusest väärkasutab tööülesannete täitmiseks mõeldud andmebaase olukorras, kus soovitav teave on kõigile avalikult kättesaadav.

Kolmanda ettepanekuna toob magistritöö autor välja, et avalike andmete kasutamist nii kriminaalmenetlustes kui ka politseitöös tuleks õigusaktides paremini reguleerida. Hetkel puudub regulatsioon, millises ulatuses, millistel eesmärkidel ja kelle suhtes on uurimisasutustel õigus avalikest andmetest teavet koguda, saadud teavet talletada ning seda töödelda, et oleks tagatud inimeste põhiõiguste kaitse. Seejuures on oluline, et oleks tagatud andmekaitsealased nõuded. Oluline on reguleerida selgemini „libakontode“ ja andmeleketega saadud andmete kasutamise võimalused. Praegune regulatsioon, milleks on politseiagendi kasutamine, ei ole igas olukorras mõistlik. *Sisu eemaldatud tööst autori poolt, kuna sisaldavad juurdepääsupiirnanguga teavet. Alus AvTS § 35 lg 1 p 5[1]*.

Samuti on oluline reguleerida kuidas võib kasutada lekkinud andmeid, kuna selliste andmete kasutamisel võib olla oluline roll mõningate kriminaalasjade edukal menetlemisel. Magistritöö autor on seisukohal, et kuna tegemist on oluliste küsimustega, siis ei saa jätta avalike andmete kasutamise reguleerimist ainult kohtupraktika lahendada. Tegemist võib olla isiku põhiseaduslike õiguste riivega ning õigusselguse huvides tuleks seadusandjal sellistes olukordades avalike andmete kasutamise õiguspärasus selgemalt reguleerida.

Siiski on oluline, et avalike andmete kasutamisel ei unustataks ära traditsiooniliste meetodite kasutamist, vaid nad mõlemad peavad toetama üksteist menetluslike eesmärkide saavutamiseks. Seeläbi on võimalik kriminaalmenetlusi efektiivsemalt menetleda ning saadav kasu on suurim.

KOKKUVÕTE

Käesolevas magistritöös otsis autor vastust **uurimisprobleemile**, kuidas on võimalik kasutada avalikke andmeid kriminaalmenetlustes tõhusamalt ja rohkem. Lähtudes uurimisprobleemist oli magistritöö **eesmärgiks** leida lahendusi, mida saaks kasutusele võtta, kui avalike andmete kasutamine muudab kriminaalmenetlusi efektiivsemaks. Eesmärgini jõudmiseks uuris magistritöö autor teoreetilisi lähtekohti avalike andmete osas ning viis läbi empiirilise uuringu. Empiirilise uuringuga eesmärgi saavutamiseks kasutati kvalitatiivset uurimisviisi ning andmekogumise meetodina kasutati poolstruktureeritud ekspertintervjuud.

Magistritöö **aktuaalsus** seisneb selles, et kuritegevus, eriti organiseeritud- ja raske peitkuritegevus, on oma olemuselt muutumises ning digitaliseerunud ühiskonnas on vajalik leida uusi lähenemisviise kuritegude uurimisel ning tõendite kogumisel. Leida uusi lähenemisviise on oluline, kuna EIK ja ka Eesti Riigikohus on võtnud suuna piiramaks varasemalt kasutusel olnud andmete kogumise ja väljastamise viise. Üheks lähenemisviisiks saabki pidada avalike andmete kasutamist kriminaalmenetlustes. Käesoleva töö **uudsus** ja **originaalsus** seisneb selles, et varasemalt ei ole Eestis uuritud avalike andmete kasutamist kriminaalmenetluslikus võtmes.

Magistritöö koosneb kahest peatükist. **Esimeses peatükis** uuriti teoreetilise kirjanduse põhjal avalike andmete kasutamist. Peamine fookus oli suunatud teemadele: kuidas avalikud andmed kujunesid oluliseks teabe hankimise võimaluseks; avalike andmete kasutamine julgeoleku vaates; avalike andmete kogumine kriminaalmenetlustes; avalike andmete kasulikkus õiguskaitseasutustele; avalike andmete kogumise ja kasutamise õiguslik vaade kriminaalmenetlustes; tehnoloogilised vahendid avalike andmete kasutamisel kriminaalmenetlustes. Esimeses peatükis leiti vastus esimesele ja viimasele uurimisküsimusele. **Teises peatükis** on kirjeldatud uurimismetoodika ja uurimiskäik, teostatud ekspertintervjuude analüüs ning lähtuvalt uuringust tehtud järeldused ning ettepanekud. Teises peatükis leiti vastused teisele ja kolmandale uurimisküsimusele. Mõlema peatükiga täideti kõik püsitatud uurimisülesanded.

Esimene uurimisülesanne oli teada saada, mida käsitletakse avalike andmetena ning kuidas neid koguda. Teoreetilises osas anti ülevaade avalikest andmetest, nende

kujunemisest oluliseks teabe hankimise võimaluseks ning sellest, kuidas ning milliseid vahendeid on võimalik kasutada andmete kogumiseks ja analüüsimiseks.

Teise uurimisülesande eesmärgiks oli leida avalike andmete kasutamise õiguslikud piirangud kriminaalmenetluse raames. Selleks analüüsis magistritöö autor kriminaalmenetlusseadustiku vastavaid sätteid ning erinevaid kohtulahendeid, mille kaudu leidis võimalikud piirangud avalike andmete kasutamise suhtes. Kriminaalmenetluse raames on peamiseks piiranguks sotsisaalmeediast andmete kogumisel „libakontode" kasutamine, kuna tegemist on uurija identiteedi muutmisega, mis on oma olemuselt jälitustoiming ning vajab prokuratuuri poolt väljastatud luba. Samuti on oluline, et avalikke andmeid kogudes ei riivataks kolmandate isikute õiguseid ning järgitakse kehtivaid kriminaalmenetluse protseduure.

Kolmanda uurimisülesande eesmärgiks oli läbi viia uuring ekspertide seas, tuvastamaks avalike andmete kasutamise kitsaskohti kriminaalmenetlustes ning leida lahendusi nende paremaks kasutamiseks. Ekspertide seas viidi läbi poolstruktureeritud intervjuud, mille analüüsist leiti võimalikud kitsaskohad avalike andmete kasutamisel. Ekspertide arvamusele tuginedes järeldab magistritöö autor, et avalikke andmeid ei kasutata kriminaalmenetluste uurimistel piisavalt, arvestades kui palju täiendavat tõenduslikku teavet võib avalikest allikatest leida. Selle põhjuseks arvati olevat asjaolu, et paljudel ametnikel puuduvad piisavad IT-alased teadmised ning ametnikud ei teadvusta või ei tea avalike andmete kasutamises peituvat potentsiaali. Veel toodi kitsaskohana välja, et puudub selge ja ühtne nägemus, kuidas saadud tõendeid vaatlusprotokollides esitada.

Neljandaks uurimisülesandeks oli sünteesida empiirilise uuringu tulemusi kasutades teaduskirjandust, õigusakte ja kohtulahendeid ning esitada ettepanekuid avalike andmete kasutamise rakendamiseks kriminaalmenetluses. Peamisteks rakenduskohtadeks kriminaalmenetlustes, kus saab avalikke andmeid kasutada, on sihistatud päringute tegemine, subjektide profiilide koostamine, kriminaaltulu tuvastamine ning erinevate menetluslike tegevuste ja taktika planeerimine.

Peamiste ettepanekutena toob magistritöö autor välja, et avalikke andmeid on kriminaalmenetlustes vaja rohkem kasutada ning selleks on koolitustega vaja tõsta ametnike teadlikkust avalikest andmetest ning suurendada ka ametnike IT-alaseid

teadmisi. Lisaks on vaja selgeid juhiseid, kuidas avalikest andmetest saadud tõendeid vaatlusprotokollides esitada. Oluline on tuua välja, et täna piirab avalike andmete laiemat kasutamist õiguslike hallide alade olemasolu ehk õigusselgus, millisel viisil ja moel kogutud avalike andmete kasutamist kohtueelses kriminaalmenetluses on tõendina lubatav ka kohtus.

Võttes arvesse magistritöö eesmärgi saavutamiseks seatud uurimisülesandeid, uurimisküsimusi ning küsimustele saadud vastuseid, võib öelda, et magistritöö eesmärk sai täidetud.

Magistritöö autori hinnangul saaks antud teemat edasi uurida uurijate vaates laiemalt, et täpsemalt tuvastada uurijate teadmiste puudujäägid avalike andmete kasutamisel ning uurida, kuidas uurimisasutustes kasutusel olevaid tehnoloogilisi või tarkvaralisi vahendeid edasi arendada, et avalike andmete kogumine oleks lihtsam ning turvalisem. Käesolevas töös väljatoodud ettepanekuid on võimalik rakendada juba praegu, kui selgitada ametnikele avalike andmete kasutamise võimalusi kriminaalmenetlustes. Lisaks pakub magistritöö autor välja järgmised teemad, mida tulevikus edasi uurida: „Millised on efektiivsed ja usaldusväärsed *OSINT* tööriistad.“; „Kuidas tagada *OSINT* abil kogutud tõendite usaldusväärsus?“; „Kuidas mõjutavad *deep fake* ja *AI* avalike andmete usaldusväärsust?“; „Kuidas *AI* vahendeid kasutades on võimalik koguda avalikke andmeid?“

SUMMARY

The research problem of the thesis is: "How can open-source intelligence (OSINT) be used more widely and effectively during criminal proceedings?" The aim is to find available solutions that could be used in practice. In order to reach the set target, theoretical viewpoints on OSINT were studied and an empirical study was carried out. Qualitative method was used to conduct the research and reach a conclusion in the empirical study. Semi structured expert interviews were used to gather data.

Organized and serious latent crime are changing in their nature, which requires that digitalized societies adopt new approaches in criminal proceedings and evidence gathering. The importance of the topic is further emphasized by both the European Court of Human Rights and the Supreme Court of Estonia taking a more limiting approach towards previously used intelligence gathering methods. The use of OSINT in the context of criminal proceedings has not been researched previously in Estonia.

The first chapter focuses on theoretical background and literature regarding the use of OSINT and answers research questions 1 and 4. **The second chapter** describes the research method and process, analyses and proposes new approaches. The second chapter answers research questions 2 and 3.

The first research question is understanding what OSINT is and how to gather it. An overview is provided of the opportunities, as well as tools for both gathering and analyses.

The second research question looks for legal limitations of using OSINT during criminal proceedings. The main limitation is the use of fake social media accounts, which is considered changing the investigator's identity, which in turn must be sanctioned by a prosecutor.

The third research question looks for current limitations of using OSINT in criminal proceedings, considering how much evidential information is available.

The fourth and final research question synthesises the results of the empirical study and makes actionable recommendations. Situations when OSINT can have a significant

impact include making targeted requests, profiling of the subjects, detecting and pinpointing criminal income, and planning procedural activities and tactics.

Future studies are needed to more accurately pinpoint where investigators' knowledge should be improved most, as well as how technical or software-based solutions could be developed further, in order to simplify gathering and using open-source intelligence in a secure manner.

In conclusion, OSINT should be used more in criminal proceedings. Various trainings are needed to achieve both awareness and techniques of using it. Additionally, clear instructions are needed on how to properly document the findings.

VIIDATUD ALLIKATE LOETELU

A. K. & R.P kriminaalasi Karistusseadustiku § 184 järgi (2008) 3-1-1-63-08.

Aftergood, S., 2015. Open Source Center (OSC) Becomes Open Source Enterprise (OSE). *Federation of American Scientists,* 28. oktoober. [Võrgumaterjal] Leitav: https://fas.org/blogs/secrecy/2015/10/osc-ose/ [Kasutatud 02.01.2023].

Albert, M., & Buzan, B., 2011. Securitization, sectors and functional differentiation. *Security Dialogue,* 42(4–5), pp. 413–425.

Allen, T., Haggard, A., Higgins, E., Kivimaki, V.-P., Ostanin, I. & Toler, A., 2014. MH17: Source of the Separatists' Buk. *A Bellingcat Investigation.* [Võrgumaterjal] Leitav: https://www.bellingcat.com/app/uploads/2014/11/Origin-of-the-Separatists-Buk-A-Bellingcat-Investigation1.pdf [Kasutatud 11.09.2022].

Anderson, R. J., 2008. *Security Engineering: a guide to building dependable distributed systems, Second Edition*. Indianapolis: Wiley Publisinh, Inc.

Andmekaitse ja infoturbe leksikon, 2022. *OSINT*. [Võrgumaterjal] Leitav: https://akit.cyber.ee/term/1145 [Kasutatud 27.11.2022].

Aradau, C. & Blanke, T., 2017. Governing others: Anomaly and the algorithmic subject of security. *European Journal of International Security,* 3(1), pp. 1–21.

Balzacq, T., Basaran, T., Bigo, D., Guittet, E.-P. & Olsson, C., 2010. *Security Practices*. *The International Studies Encyclopedia Online.* [Võrgumaterjal] Leitav: http://www.open.ac.uk/researchprojects/iccm/files/iccm/olsson-christian-publication7.pdf [Kasutatud 21.11.2021].

Baror, S., Venter, H.S. & Adeyemi, R., 2021. A natural human language framework for digital forensic readiness in the public cloud. *Australian Journal of Forensics Scoemces,* 53(5), pp. 566–591.

Behera, N. C., Hinds, K., & Tickner, A. B., 2021. Making amends: Towards an antiracist critical security studies and international relations. *Security Dialogue*, 52(1), pp. 8–16.

Bellingcat, 2022. *About.* [Võrgumaterjal] Leitav: https://www.bellingcat.com/about/ 1 [Kasutatud 11.09.2022].

Bereziuk, B., 2016. *The Modus Operandi of Chinese Intelligence*. Ottawa: Carleton University.

Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P. & Sullivan, R., 2018. Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *Journal of Public Health*, 26, pp. 509–514.

Bhuiyan, S., 2023. The Pandora Papers Opens up Pandora's Box: Integrity in Crisis. *Public Integrity*, 25(2), pp. 245–256.

Bigo, D. & McCluskey, E., 2018. What Is a PARIS approach to (in)securitization? Political anthropological research for international sociology. Rmt: A. Gheciu & W.C. Wohlforth, toim-d. *The Oxford Handbook of International Security*. Croydon: CPI Group, pp. 116–130.

Bigo, D., 2000. When two become one: Internal and external securitisations in Europe. Rmt: M. Kelstrup & M. Williams, toim-d. *International Relations Theory and the Politics of European Integration: Power, Security and Community*. London: Routledge, pp. 320–360.

Bigo, D., 2002. Security and immigration: Toward a critique of the governmentality of unease. *Alternatives*, 27(1), pp. 63–92.

Bigo, D., 2008. Globalized (in)Security: the Field and the Ban-opticon. Rmt: D. Bigo & A. Tsoukala, toim-d. *Terror Insecurity and Liberty: Illiberal Practices of Liberal Regimes After 9/11*. 1st edition. London: Routledge, pp. 10–48.

Boateng, F. D. & Chenane, J., 2020. Policing and social meedia: A mixed-method investigation of social meedia use by a small-town police department. *International Journal of Police Science & Management,* 22(3), pp. 263–273.

Briggs, C.M., Matejova, M. & Weiss, R., 2022. Disaster intelligence: developing strategic warning for national security. *Intelligence and National Security*, 37(7), pp. 985–1002.

Browning, C. S., & McDonald, M., 2013. The future of critical security studies: Ethics and the politics of security. *European Journal of International Relations*, 19(2), pp. 235–255.

Buzan, B., Wæver, O. & de Wilde, J., 1998. *Security: A New Framework for.* London: Lynne Rinner Publishers.

C.A.S.E. Collective. 2006. Critical Approaches to Security in Europe: A Networked Manifesto. *Security Dialogue*, 37(4), pp. 443–487.

CEPOL, 2022a. *The agency*. [Võrgumaterjal] Leitav: https://www.cepol.europa.eu/about/the-agency [Kasutatud 04.12.2022].

CEPOL, 2022b. *OSINT*. [Võrgumaterjal] Leitav: https://www.cepol.europa.eu/tags/osint [Kasutatud 06.11.2022].

Central Intelligence Agency, 2016. *The Art of Intelligence.* Washington: Cia Museum and The Center For The Study Of Intelligence. [Võrgumaterjal] Leitav: https://www.cia.gov/static/83f5ee7757837b458163077d214a7c93/The-Art-of-Intelligence.pdf [Kasutatud 07.12.2022].

Černý, J. & Potančok, M., 2023. Information literacy in international masters students: A competitive and business intelligence course perspective. *Cogent Education*, 10(1), pp. 1–12.

Chainey, S. P. & Berbotto, A. A., 2021. A structured methodical process for populating a crime script of organized crime activity using OSINT. *Trends in Organized Crime*, 25, pp. 272–300.

Danewid, I., 2022. Policing the (migrant) crisis: Stuart Hall and the defence of whiteness. *Security Dialogue*, 53(1), pp. 21–37.

Dawson, M., Lieble, M. & Adeboje, A., 2017. Open Source Intelligence: Performing Data Mining and Link Analysis to Track Terrorist Activities. Rmt: L. Shahram, toim. *Information Technology - New Generations.* Berlin: Springer Nature, pp. 159–163.

Delehanty, W.K. & Steele, B.J., 2009. Engaging the narrative in ontological (in)security theory: insights from feminist IR, *Cambridge Review of International Affairs*, 22(3), pp. 523–540.

Demirkol, A., 2023. A Perspective on Critical Security Concept and International Migration Nexus through Copenhagen School: The Quest for Societal Security. *Lectio Socialis*, 7(1), pp. 23–32.

De Rechtspraak, 2022. *Summary of the day in court: 17 November 2022 – Judgment.* [Võrgumaterjal] Leitav: https://www.courtmh17.com/en/news/2022/summary-of-the-day-in-court-17-november-2022---judgment.html [Kasutatud 18.12.2022].

Dixon, S., 2022. *Social meedia – Statistics ja Facts.* [Võrgumaterjal] Leitav: https://www.statista.com/topics/1164/social-networks/#topicHeader__wrapper [Kasutatud 14.01.2023].

Dogruer, N., Eyyam, R. & Menevis, I., 2011. The use of the internet for educational purposes. *Procedia - Social and Behavioral Sciences*, 28, pp. 606–611.

Dover, R., 2020. SOCMINT: a shifting balance of opportunity. *Intelligence and National Security*, 35(2), pp. 216–232.

Duisembina, Y., Grishina, N. Y. & Boldyreva, E. L., 2018. Cambridge Analytica: Ethics And Online Manipulation With Decision-Making Process. Rmt: V. Chernyavskaya, & H. Kuße, toim-d. *Professional Culture of the Specialist of the Future*, 51. London: Future Academy, pp. 91–102.

Edwards, L. & Urquhart, L., 2015. Privacy in Public Spaces: What Expectations of Privacy do we have in Social Media Intelligence? *International Journal of Law and Information Technology*, 24(3), pp. 279–310.

Eesti Keele Instituut, 2022. *IMINT.* [Võrgumaterjal] Leitav: https://sonaveeb.ee/search/unif/dlall/dsall/IMINT/1 [Kasutatud 06.11.2022].

Eesti Keele Instituut, 2023a. *Andmed.* [Võrgumaterjal] Leitav: https://sonaveeb.ee/search/unif/dlall/dsall/andmed/1 [Kasutatud 06.03.2023].

Eesti Keele Instituut, 2023b. *Õiguskaitseorgan.* [Võrgumaterjal] Leitav: https://xn--snaveeb-10a.ee/search/unif/dlall/dsall/%C3%B5iguskaitseorgan/1 [Kasutatud 12.03.2023].

Economic Commission for Latin America and the Caribbean, 2021. *Digital technologies for a new futuure*. Santiago: United Nations publication.

Eesti Vabariigi põhiseadus (1992) RT I, 15.05.2015, 2.

Euroopa Inimõiguste ja põhivabaduse kaitse konventsioon (1950) RT II 2010, 14, 54.

Euroopa Komisjon, 2022a. *Glossary: International Mobile Subscriber Identity (IMSI).* [Võrgumaterjal] Leitav: https://ec.europa.eu/eurostat/cros/content/Glossary%3AInternational_Mobile_Subscriber_Identity_%28IMSI%29_en [Kasutatud 08.12.2022].

Euroopa Komisjon, 2022b. *Open-source intelligence.* [Võrgumaterjal] Leitav: https://data.europa.eu/en/publications/datastories/open-source-intelligence [Kasutatud 08.01.2023].

Euroopa Parlamendi ja Nõukogu, 2016. *füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). Määrus. (EL) 2016/679.*

Euroopa Parlament, 2016. *Panama paberid: uurivad ajakirjanikud räägivad parlamendis oma tööst.* [Võrgumaterjal] Leitav:

https://www.europarl.europa.eu/news/et/headlines/economy/20160926STO44008/panama-paberid-uurivad-ajakirjanikud-raagivad-parlamendis-oma-toost [Kasutatud 12.03.2023].

European e-justice, 2023. *Süüdistatavad (kriminaalmenetlused).* [Võrgumaterjal] Leitav: https://e-justice.europa.eu/content_rights_of_defendants_in_criminal_proceedings_-169-EE-maximizeMS-en.do?clang=et&idSubpage=2 [Kasutatud 18.02.2023].

EUROPOL, 2021. *Cyber Intelligence.* [Võrgumaterjal] Leitav: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/intelligence-analysis/cyber-intelligence [Kasutatud 08.01.2023].

EUROPOL, 2022a. *Secure Information Exchange Network Application (SIENA)* [Võrgumaterjal] Leitav: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena [Kasutatud 06.11.2022].

EUROPOL, 2022b. *Stop Child Abuse – Trace an Object.* [Võrgumaterjal] Leitav: https://www.europol.europa.eu/stopchildabuse [Kasutatud 16.10.2022].

Fallik, S. W., Deuchar, R., Crichlow, V. J. & Hodges, H., 2020. Policing through social meida: a qualitative exploration. *International Journal of Police Science & Management*, 22(2), pp. 208–218.

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

French Republic Presidency, 2017. *Defence and National Security Strategic Review.* [Võrgumaterjal] Leitav: https://www.dsn.gob.es/sites/dsn/files/2017%20France%20Strategic%20Review.pdf [Kasutatud 25.09.2022].

Graham, R. & Pitman, B., 2020. Freedom in the wilderness: A study of a Darknet space. *Convergence*, 26(3), pp. 593–619.

Gregory, S., 2022. Deepfakes, misinformation and disinformation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism. *Journalism*, 23(3), pp. 708–729.

Hauter, J., 2021. Forensic conflict studies: Making sense of war in the social media age. *Media, War & Conflict.* 0(0), pp. 1–20.

Hirsjärvi, S., Remes, P. & Sajavaara P., 2005. *Uuri ja kirjuta*. Tallinn: Medicina.

H. K. kriminaalasi KarS § 199 lg 2 p-de 5, 8 ja 9, § 213 lg 2 p 1 ning § 323 lg 1 järgi (2021) 1-16-6179.

Huysman, J., 2006. *The Politics of Insecurity. Fear, migration and asylum in the EU.* Milton Park: Routledge.

Hwang, Y-W., Lee, I-Y., Kim, H., Lee, H. & Kim, D., 2022. Current Status and Security Trend of OSINT. *Wireless Communications and Mobile Computing*, 2022, pp. 1–14.

INTERPOL, 2022a. *Our 19 databases.* [Võrgumaterjal] Leitav: https://www.interpol.int/en/How-we-work/Databases/Our-19-databases [Kasutatud 06.11.2022].

INTERPOL, 2022b. *Project Trace.* [Võrgumaterjal] Leitav: https://www.interpol.int/en/Crimes/Terrorism/Counter-terrorism-projects/Project-Trace2 [Kasutatud 06.11.2022].

IRS, 2023. *Foreign Account Tax Compliance Act (FATCA).* [Võrgumaterjal] Leitav: https://www.irs.gov/businesses/corporations/foreign-account-tax-compliance-act-fatca [Kasutatud 26.02.2023].

Johnson, L. K., 2007. *Handbook of Intellignece Studies.* New York: Routledge.

Joyce, J., 2003. Bayes Theorem. *Stanford Encyclopedia of Philosophy Archive.* [Võrgumaterjal] Leitav: https://plato.stanford.edu/archives/spr2019/entries/bayes-theorem/ [Kasutatud 05.09.2022].

Karistusseadustik[1] (2001) RT I, 06.08.2022, 27.

Kassim, S. R. B. M., Li, S. & Arief, B., 2022. How national CSIRTs leverage public data, OSINT and free tools in operational practices: An empirical study. *Cyber Security: A Peer-Reviewed Journal,* 5(3), pp. 251–276.

Katz, B., 2020. *The Collection Edge: Harnessing Emerging Technologies for Intelligence Collection.* [Võrgumaterjal] Leitav: https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/20713_Katz_CollectionEdge_v4_WEB%20FINAL.pdf [Kasutatud 25.09.2022].

Kidron, A., 2007. *Uurija käsiraamat: mis ja milleks? Kuidas? Mis meetodil? Teadus- ja rakendusuuringuist psühholoogias.* Tallinn: Mondo.

Kim, K., Oblesby-Neal, A. & Mohr, E., 2017. *2016 Law Enforcement Use of Social Media Survey.* [Võrgumaterjal] Leitav: https://www.urban.org/sites/default/files/publication/88661/2016-law-enforcement-use-of-social-media-survey.pdf [Kasutatud 14.01.2023].

Koops, B.J., 2013. Police investigations in Internet open sources: Procedural-law issues. *Computer Law & Security Review*, 29(6), pp. 654–665.

Koovit, K., 2018. Saksamaa suurima panga kontorid otsiti Panama paberitest vallandunud rahapesusüüdistuste tõttu läbi. *Delfi Ärileht,* [Võrgumaterjal] Leitav: https://arileht.delfi.ee/artikkel/84603163/saksamaa-suurima-panga-kontorid-otsiti-panama-paberitest-vallandunud-rahapesusuudistuste-tottu-labi [Kasutatud 12.03.2023].

Kotsios, A., Magnani, M., Rossi, L., Shklovski, I. & Vega, D., 2019. *An Analysis of the Consequences of the General Data Protection Regulation (GDPR) on Social Network Research.* [Võrgumaterjal] Leitav: https://www.researchgate.net/publication/331645097_An_Analysis_of_the_Consequences_of_the_General_Data_Protection_Regulation_GDPR_on_Social_Network_Research [Kasutatud 19.02.2023].

Kotze, E., Senekal, B. A. & Daelemans, W., 2020. Automatic classification of social meedia reports on violent incidents in South Africa using machine learning. *South African Journal of Science*, 116(3/4), pp. 1–8.

Kozera, C. A., 2020. Fitness OSINT: Identifying and tracking military and security personnel with fitness applications for intelligence gathering purposes. *Security & Defence Quarterly*, 32(5), pp. 41–52.

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

Kvale S. & Brinkmann S., 2009. *Interviews: Learning the craft of qualitative research interviewing*. Thousand Oaks: Sage.

Laherand, M.-L., 2008. *Kvalitatiivne uurimisviis*. 2. trükk. Tallinn: OÜ Sulesepp.

Leavell, R., 2007. *The Evolution Of Regional Counterterrorism Centers Within A National Counterterrorism Network: Is It Time To Fuse More Than Information? Thesis.* California: Naval Postgraduate School.

Lutai, R. C., 2020. Open Source Intelligence: Opportunities and Challenges. *Strategic Impact No.* 1, pp. 95–109.

Madise, Ü., 2021. *Kriminaalmenetluse seadustiku § 215 lõike 1 vastavus põhiseadusele. [E-kiri]* (07.09.2021). [Võrgumaterjal] Leitav: https://www.oiguskantsler.ee/sites/default/files/field_document2/Kriminaalmenetluse%20seadustiku%20%C2%A7%20215%20l%C3%B5ike%201%20vastavus%20p%C3%B5hiseadusele.pdf [Kasutatud 18.02.2023].

Maksualase teabevahetuse seadus[1] (2014) RT I, 29.12.2022, 28.

Mayda, M., 2022. Digital Footprint Management in Digital Visual Culture. *Journal of Erciyes Communication*, 9(2), pp. 1031–1044.

Medewar, S., 2023. *Download Google Dorks Cheat Sheet PDF for Quick References*. [Võrgumaterjal] Leitav: https://hackr.io/blog/google-dorks-cheat-sheet [Kasutatud 12.03.2023].

Mesipuu, B., 2021. *Suur uuring – eestlaste interneti ja sotsiaalmeedia kasutus aastal 2021*. [Võrgumaterjal] Leitav: https://milos.ee/eestlaste-interneti-ja-sotsiaalmeedia-kasutus-aastal-2021/ [Kasutatud 12.03.2023].

Militerm, 2022a. *GEOINT*. [Võrgumaterjal] Leitav: https://sonaveeb.ee/search/unif/dlall/mil/GEOINT/1 [Kasutatud 18.09.2022].

Militerm, 2022b. *MASINT*. [Võrgumaterjal] Leitav: https://sonaveeb.ee/search/unif/dlall/mil/MASINT/1 [Kasutatud 18.09.2022].

Murray, R., 2018. *The Unrealized Value of Open Source Intelligence in Irregular Warfare.* [Võrgumaterjal] Leitav: https://thestrategybridge.org/the-bridge/2018/7/25/the-unrealized-value-of-open-source-intelligence-for-irregular-warfare [Kasutatud 08.01.2023].

NATO, 2001. *Nato Open Source Intelligence Handbook. Käsiraamat.* [Võrgumaterjal] Leitav: https://www.academia.edu/4037348/NATO_Open_Source_Intelligence_Handbook [Kasutatud 08.01.2023].

Ndubueze, P. N., 2021. *Security Agencies, Open Source Intelligence and Insurgency Control in North East Nigeria*. [Võrgumaterjal] https://www.researchgate.net/publication/356192087_Security_Agencies_Open_Source_Intelligence_and_Insurgency_Control_in_North_East_Nigeria [Kasutatud 14.01.2023].

Neuman, W. L., 2014. *Social research methods: Qualitative and Quantitative Approaches*. 7th ed. Essex: Pearson Education Limited.

OECD, 2014. *Standard for Automatic Exchange of Financial Account Information in Tax Matters.* [Võrgumaterjal] Leitav: https://read.oecd.org/10.1787/9789264216525-en?format=pdf [Kasutatud 26.02.2023].

Office of the Director of National Intelligence, 2022. *What is Intelligence?* [Võrgumaterjal] Leitav: https://www.dni.gov/index.php/what-we-do/what-is-intelligence [Kasutatud 18.09.2022].

Office of the Director of National Intelligence, 2023. *Home.* [Võrgumaterjal] Leitav: https://www.dni.gov/ [Kasutatud 07.04.2023].

Ooi, J., 2015. *IMSI Catchers and Mobile Security.* [Võrgumaterjal] Leitav: https://www.cis.upenn.edu/wp-content/uploads/2019/08/EAS499Honors-IMSICatchersandMobileSecurity-V18F.pdf [Kasutatud 08.12.2022].

OSINT Framework, 2022. *Notes.* [Võrgumaterjal] Leitav: https://osintframework.com/ [Kasutatud 12.09.2022].

Panagiotou, A., Ghitar, B., Shiaeles, S. & Bendiab, K., 2019. *Machine Learning in Detecting User"s Suspicious Behaviour through Facebook Wall. Ettekanne.* St. Petersburg, 26-28.08.2019 konverents: 19th International Conference, NEW2AN 2019, and 12th Conference, ruSMART 2019.

Pai, Y. & Prasad, K., 2021. Open Source Intelligence and its Applications in Next Generation Cyber Security - A Literature Review. *International Journal of Applied Engineering and Management Letters (IJAEML),* 5(2), pp. 1–25.

Pastor-Galindo, J., Nespoli, P., Marmol, F.G. & Perez, G.M., 2020. The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Transactions on Network and Service Management,* 17(4), pp. 2156–2170.

Patton, M. Q., 2015. *Qualitative research & evaluation methods: integrating theory and practice*. 3rd ed. Thousand Oaks, London, New Delhi: SAGE Publications.

Pattom, D. U., Brunton, D.-W., Dixon, A., Miller, R. J., Leonard, P. & Hackman, R., 2017. Stop and frisk online: Theorizing everyday racism in digital policing in the use of social media for identification of criminal conduct and association. *Social Media + Society,* 3(3), pp 1–10.

Peters, S. E. & Ojedokun, U. A., 2019. Social Media Utilization for Policing and Crime Prevention in Lagos, Nigeria. *Journal of Social, Behavioral, and Health Sciences,* 13(1), pp. 166–181.

Phantom Technologies, 2023. *What Is Imsi Catcher And What Is The Use Of It?* [Võrgumaterjal] Leitav: https://phantom-technologies.com/what-is-imsi-catcher/ [Kasutatud 02.01.2023].

Politsei ja Piirivalve seadus[1] (2009) RT I, 11.03.2023, 35.

Popel, J., 2022. OSINT: The New Big Thing In B2B Business. *Forbes.* [Võrgumaterjal] Leitav: https://www.forbes.com/sites/forbesbusinessdevelopmentcouncil/2022/01/26/osint-the-new-big-thing-in-b2b-business/?sh=21adfda07b7e [Kasutatud 14.01.2023].

Olev, A. & Alumäe, T., 2022. Estonian Speech Recognition and Transcription Editing Service. *Baltic J. Modern Computing*, 10(3), pp. 409–421.

Quick, D. & Choo, K. K. R., 2018. Digital forensic intelligence: Data subsets and Open Source Intelligence (DFINT+OSINT): A timely and cohesive mix. *Future Generation Computer Systems*, 78, pp. 558–567.

Rahapesu ja terrorismi rahastamise tõkestamise seadus[1] (2017) RT I, 10.02.2023, 29.

Rahvusvahelise sanktsiooni seadus (2019) RT I, 08.03.2022, 3.

Rahwan, A., 2022. *Artificial Intelligence And Interoperability For Solving Challenges Of Osint And Cross-Border Investigations.* [Võrgumaterjal] Leitav: https://www.researchgate.net/profile/Amr-El-Rahwan/publication/365710562_ARTIFICIAL_INTELLIGENCE_AND_INTEROPERABILITY_FOR_SOLVING_CHALLENGES_OF_OSINT_AND_CROSS-BORDER_INVESTIGATIONS/links/637f6cb4554def6193681292/ARTIFICIAL-INTELLIGENCE-AND-INTEROPERABILITY-FOR-SOLVING-CHALLENGES-OF-OSINT-AND-CROSS-BORDER-INVESTIGATIONS.pdf [Kasutatud 04.12.2022].

Riigi Infosüsteemide Amet, 2022. *Andmejälgija.* [Võrgumaterjal] Leitav: https://www.ria.ee/et/riigi-infosusteem/x-tee/andmejalgija.html [Kasutatud 25.09.2022].

Riigikogu, 2017. „*Eesti julgeolekupoliitika alused“ heakskiitmine. Otsus. Lisa.* RT III, 06.06.2017, 2.

Riigikogu, 2020. *Kriminaalpoliitika põhialuste aastani 2030 heakskiitmine. Otsus.* RT III, 13.11.2020, 6.

R. K. väärteoasi liiklusseaduse § 74[19] järgi (2005) 3-1-1-19-05.

Rohn, U., 2015. Social Media Business Models. Rmt: R. Mansell & P. H. Ang, toim-d. *The International Encyclopedia of Digital Communication and Society.* 1. ed. West Sussex: Wiley & Sons, pp. 1049–1050.

Rønn, K. V. & Søe, O., 2019. Is social media intelligence private? Privacy in public and the nature of social media intelligence. *Intelligence and National Security*, 34(3), pp. 362–378.

Rotaru v. Romania Euroopa Inimõiguse Kohus (2000) 28341/95.

Saks, H., 2020. Kuidas … võita kübervaenlast? Küberhügieen – riigi kaitsevõime alus. *Kaitse kodu*, 3, lk 46–47.

Samier, E. A., 2015. The globalization of higher education as a societal and cultural security problem. *Policy Futures in Education*, 13(5), pp. 683–702.

Sampson, F., 2017. Intelligent evidence: using open source intelligence (OSINT) in criminal proceedings. *Police Journal: Theory, Practice and Principles*, 90(1), pp. 55–69.

Schaurer, F. & Ströger, J., 2013. The Evolution of Open Source Intelligence (OSINT). *Journal of U.S. Intelligence Studies,* 19(3), pp 53–56.

Settanni, G., Skopik, F., Shovgenya, Y., Fiedler, R., Carolan, M., Conroy, D., Boettinger, K., Gall, M., Brost, G., Ponchel, C., Haustein, M., Kaufmann, H., Theuerkauf, K. & Olli, P., 2017. A collaborative cyber incident management system for European interconnected critical infrastructures. *Journal of Information Security and Applications*, 34, pp. 166–182.

Siseministeerium, 2021. *Politseinike ja päästjate tulevikuvajaduse ning töötasu analüüs.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/media/1427/download [Kasutatud 14.01.2023].

Siseministeerium, 2023a. *Sisejulgeoleku tagamine.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/tegevusvaldkonnad/kindel-sisejulgeolek/sisejulgeoleku-tagamine [Kasutatud 08.01.2023].

Siseministeerium, 2023b. *Valitsemisala asutused.* [Võrgumaterjal] Leitav: https://www.siseministeerium.ee/ministeerium-ja-kontaktid/valitsemisala-asutused [Kasutatud 08.01.2023].

Sootak, J. & Pikamäe, P., 2021. *Karistusseadustik. Kommenteeritud väljaanne. 5., täiendatud ja ümbertöötatud väljaanne.* Tallinn: Juura.

Southeton, C. & Taylor, E., 2020. Habitual disclosure: routine, affordance, and the ethics of young people‟s social media surveillance. *Social Media + Society,* 6(2), pp. 1–11. [Võrgumaterjal] Leitav: https://journals.sagepub.com/doi/pdf/10.1177/2056305120915612 [Kasutatud 15.02.2023].

Swift, 2023a. *What is KYC?* [Võrgumaterjal] Leitav: https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/meaning-kyc#:~:text=illicit%20criminal%20activities.-,Know%20Your%20Customer%20(KYC)%20standards%20are%20designed%20to%20protect%20financial,of%20funds%20is%20legitimate%3B%20and [Kasutatud 14.01.2023].

Swift, 2023b. *The KYC process explained.* [Võrgumaterjal] Leitav: https://www.swift.com/your-needs/financial-crime-cyber-security/know-your-customer-kyc/kyc-process [Kasutatud 26.02.2023].

Sõnaveeb, 2022. *Guugeldama.* [Võrgumaterjal] Leitav: https://sonaveeb.ee/search/unif/dlall/dsall/guugeldama/1 [Kasutatud 18.12.2022].

Tallinna Ülikool, 2015. *Tehnoloogia didaktika erialade kirjalike tööde koostamiseks ja vormistamiseks. Juhend.* Tallinn: Tallinna ülikool.

Teddlie, C. & Yu, F. 2007. Mixed Methods Sampling A Typology With Examples. Journal of Mixed Methods Research, 1(1), 77–100.

The Economist Intelligence Unit, 2019. *A whole new world: How technology is driving the evolution of intelligent Banking. Report.* [Võrgumaterjal] Leitav: https://impact.economist.com/perspectives/sites/default/files/intelligent_banking_temenos_2019_0.pdf [Kasutatud 25.09.2022].

Ungureanu, G.-T., 2021. Open Source Intelligence (Osint). The Way Ahead. *Journal of Defense Resources Management*, 12(1), pp. 177–200.

Venemaa president, 2015. *Russian National Security Strategy.* [Võrgumaterjal] Leitav: https://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Internacional/2016/Russian-National-Security-Strategy-31Dec2015.pdf [Kasutatud 25.09.2022].

Venemaa president, 2016. *Doctrine of Information Security of the Russian Federation*. [Võrgumaterjal] Leitav: http://www.scrf.gov.ru/security/information/DIB_engl/ [Kasutatud 25.09.2022].

Von Hannover v. Germany Euroopa Inimõiguste Kohus (2004) 59320/00.

V. R., T. S & A. P kriminaalasi Karistusseadustiku §-de § 293, 295 ja 297 lg 1 järgi (2010) 3-1-1-22-10.

V. S. kriminaalasi KarS § 300[1] lg 2 järgi (2021) 1-19-6293.

Walklate, S., McCulloch, J., Fitz-Gibbon, K., & Maher, J., 2019. Criminology, gender and security in the Australian context: Making women's lives matter. *Theoretical Criminology*, *23*(1), pp. 60–77.

Warkentin, N., Frank, R., Zhang, Y. & Zakimi, N., 2022. Potential cyber-threats against Canada's critical infrastructure: an investigation of online discussion forums. *Criminal Justice Studies*, 35(3), pp. 322–345.

Wæver, O., 2011. Politics, security, theory. *Security Dialogue,* 42(4-5), pp. 465–480.

Wells, D. & Gibson, H., 2017. OSINT from a UK perspective: considerations from the law enforcement and military domains. *Proceedings Estonian Academy of Security Sciences,* 16, pp. 83–113.

Williams, H. J. & Blum, I., 2018. *Defining Second Generation Open Source Intelligence (OSINT) for the Enterprise*. California: Rand Corporation.

Yeboah-Ofori, A. & Brimicombe, A., 2017. Cyber Intelligence & OSINT: Developing Mitigation Techniques Against Cybercrime Threats on Social Media. *International Journal of Cyber-Security and Digital Forensics,* 7(1), pp. 87–98.

Yimer, B. L., 2021. Social Media Usage, Psyhosocial Wellbeing and Academic Performance. *International Quarterly of Community Health Education,* 0(0), pp. 1–6.

LISA 1. EKSPERTINTERVJUUDE KÜSIMUSED

Kui sageli Te puutute kokku avalike andmetega?

Kuidas Te kirjeldate, mis on avalikud andmed Teie meelest?

Milliseid vahendeid Te kasutate avalikke andmete kogumiseks?

Kuidas või milliseid vahendeid Te kasutate kogutud andmete analüüsimiseks?

Kuidas toimub saadud andmete vormistamine tõendiks ning millised olulisi nüansse oskate Te välja tuua?

Kuidas ja millisel juhul olete avalike andmeid kasutanud kriminaalmenetlustes?

Millised on avalike andmete kasutamise kitsaskohad kriminaalmenetlustes?

Millistel juhtudel on Teie arvates kõige mõistlikum avalike andmeid kasutada? (näited)

Kuidas Teie arvates avalike andmete kogumine tõhustab kriminaalmenetlusi?

Kuidas veenduda saadud andmete usaldusväärsuses?

Kas avalikke andmeid kasutatakse piisavalt?

Mis võiks olla avalike andmete kasutamise tulevik?