TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Kätriin Kangur

DIGITAALSETE TÕENDITE USALDUSVÄÄRSUS

MAGISTRITÖÖ

Juhendaja: *prof* Jaan Ginter

Tartu
2022

Sissejuhatus

Aina suurema osa tänapäevasest ühiskonnast moodustab digitaalsus koos kõigi oma omadustega. Inimkond on oma arengult jõudnud punkti, kus enamik tavapärastest tegevustest omab mingisugust digitaalset mõõdet. Sportides kasutame nutikella, tuttavatega suhtlemiseks nutitelefoni ning ka töö tegemisel on peamiseks abivahendiks arvuti. Võib spekuleerida, et ilmselt 40 aastat tagasi ei osanud keegi oodata, millise hüppelise arengu teeb digitaalmaailm ning kui sõltuvaks me oma igapäevases elus sellest muutume. Nutikad kodumasinad ja arenenud programmid on temaatika, mis võis aastaid tagasi kõlada keskmise inimese jaoks utoopiliselt, kuid tänapäeval on tegemist reaalsusega, mis ootab, et inimesed sellega sammu jõuaksid pidada.

Sir Arthur Conan Doyle on oma teoses tabavalt öelnud: „Mida üks inimene saab leiutada, seda teine inimene võib avastada."[1] Eelnev tsitaat iseloomustab autori hinnangul ka digitaalmaailma. Nimelt on ohtrate digitaalsete seadmete leiutamisega kaasnenud ka võimalus avastada informatsiooni või teavet, mida sellised seadmed on salvestatud. Taoline salvestatud informatsioon võib aga suurel määral aidata kaasa erinevates menetlustes, kuna see võimaldab anda digitaalsete tõendite näol informatsiooni juhtumi erinevate asjaolude kohta.

Eelnevale asjaolule viitab ka statistika. Nimelt on Euroopa Komisjon hinnanud, et umbes 85%-s kriminaalmenetlustes on märgatav digitaalsete tõendite kasutamise vajadus.[2] Kuid digitaalsed tõendid ei ole seotud ainult kriminaalmenetlusega. Eelneval on oluline koht ka eraõiguslikes suhetes, näiteks on digitaalsete tõendite kasutamine võrdlemisi levinud töövaidluste lahendamisel.[3] Samuti on digitaalsete tõendite abil võimalik tuvastada ärispionaaži juhtumeid. [4] Lisaks eelnevatele, võib digitaalsete tõendite kasutamist ette tulla ka intellektuaalse omandi varguse kahtluse tuvastamisel.

---

[1] Doyle, A.C „The Return of Sherlock Holmes" George Newnes Ltd., 1905, lk 75.
[2] European Commission „Frequently Asked Questions: New EU rules to obtain electronic evidence." Külastatud 04.03.2022. Arvutivõrgus kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
[3] Vacca, John R. Computer Forensics: Computer Crime Scene Investigation. Charles River Media Inc. Massachusetts, 2002. lk 4-5.
[4] Dokko, J. Shin, M. „A Digital Forensic Investigation and Verification Model for Industrial Espionage" Digital Forensics and Cyber Crime, 2019, lk 2.

Seega võib eelnevast järeldada, et digitaalsete tõendite kasutusala on võrdlemisi lai ning ei ole seotud ühe kindla õigusharuga. Võttes aga arvesse digitaalsete tõendite vajadust erinevates menetlustes ning tehnoloogia kiiret arengut, tekib paratamatult küsimus digitaalsete tõendite usaldusväärsuse kohta. Erialakirjanduses on viidatud asjaolule, et juriidika kogukonnas peetakse digitaalseid tõendeid usaldusväärseks.[5] Autori hinnangul võib taolise hinnangu põhjuseks olla veendumus, et arvutid ei ole suutelised tegema samu moraalseid vigu, mis inimesed. Kuid autori hinnangul on oluline siiski analüüsida, kas on olemas asjaolusid, mis viitavad arutelule, et ka digitaalsete tõendite osas on alust kahelda nende usaldusväärsuses.

Tegemist on vägagi aktuaalse probleemiga, kuna tehnoloogia osakaalu kasv inimeludes tähendab ka digitaalsete tõendite kasvu erinevates menetlustes. Õiglase korra tagamiseks on aga oluline, et tõend on usaldusväärne ja sobilik alus otsuste tegemiseks, kuna ebaõiget informatsiooni edastav tõend võib kaasa tuua võrdlemisi drastilisi olukordi, näiteks alusetuid süüdimõistmisi või muid tegelikkuses ebavajalikke tagajärgi. Ühiskondlik huvi on tagada, et karistada saaksid õiged inimesed ning sanktsioonidest puutumata jääksid süütud. Sestap on töö eesmärgiks analüüsida, kas digitaalsete tõendite osas esineb murekohti ning kuidas võivad taolised probleemkohad mõjutada sellise tõendi usaldusväärsust.

Et töö eesmärki täita, analüüsib autor väliskirjandust, mis toob välja erinevate ekspertide seisukohti antud temaatika osas. Tegemist on teoreetilise uurimusega, mis koondab digitaalsete tõendite erinevaid probleemkohti väliskirjanduse ning eriala ekspertide hinnangu näitel ning annab soovitusi, kuidas on antud kitsaskohti võimalik parandada. Samuti on autor läbi viinud intervjuusid erinevate inimestega, kelle töös võib kohata digitaalsete tõendite kasutamist. Intervjuude eesmärgiks oli analüüsida, kas intervjueeritavatel on ette tulnud probleeme digitaalsete tõendite kasutamise ning usaldusväärsusega. Lisaks soovis käesoleva töö autor intervjuude abil lugejatele anda võimaluse tutvuda erinevate inimeste kogemustega digitaalsete tõendite kasutamise osas.

Tegemist on aktuaalse problemaatikaga, kuna erinevaid digitaalseid seadmeid tuleb aina juurde ning eelnevast võib järeldada, et sellega koos kasvab ka potentsiaalsete digitaalsete tõendite hulk. Näiteks on väliskirjanduses viidatud juba juhtumile, kus nutikat koduabilist

[5] Van Buskirk, E. Liu, V.T „Digital evidence: challenging the presumption of reliability" Journal of Digital Forensic Practice, 2006, lk 1.

nimega *Alexa* on kasutatud kohtus digitaalse asitõendina. [6] On oluline, et ollakse suutelised taolise uue informatsiooni probleemkohti adekvaatselt hindama, et garanteerida erinevates menetlustes õiglane lahend.

Töö autor on jaotanud käesoleva magistritöö kolmeks erinevaks peatükiks, mis omakorda jagunevad alapeatükkideks. Esimese peatüki eesmärk on tutvustada lugejale digitaalsete tõendite olemust. Lugejale antakse informatsiooni selle kohta, mis on digitaalsed tõendid ning mis on digitaalne ekspertiis. Samuti selgitatakse, milline on digitaalsete tõendite ja digitaalse ekspertiisi ajalugu ja tekkelugu ning milline on digitaalse ekspertiisi positsioon tänapäevases maailmas. Lisaks eelnevale, antakse lugejale ülevaade sellest, mis on *chain of custody* ning kuidas see suhestub digitaalsete tõendite kogumisega.

Teise peatüki eesmärk on välismaailma erialakirjanduse ning välisekspertide hinnangute abil analüüsida erinevaid kitsaskohti, mis võivad ette tulla digitaalsete tõendite analüüsimise ning kasutamise korral. Teine peatükk on jaotatud neljaks alapeatükiks. Esimese alapeatüki juures analüüsitakse digitaalsete tõendite üldist usaldusväärsust. Tegemist on peatükiga, kus vaadeldakse erinevaid tehnilisi probleeme, mis võivad digitaalsete tõendite analüüsimisel ja kogumisel ette tulla. Sellele järgnevas alapeatükis tutvustatakse lugejale, mis on *anti-forensic* tarkvarad ning millisel eesmärgil neid kasutatakse. Samuti antakse ülevaade digitaalsete tõendite võltsimisest. Kolmandas alapeatükis analüüsib käesoleva magistritöö autor inimlikke vigu, mis esinevad digitaalsete tõendite kogumise ja digitaalse ekspertiisi protsessis. Järgnevas alapeatükis antakse lugejale ülevaade eelarvamuste kohta, mis võivad esineda digitaalsete tõendite analüüsis.

Viimane peatükk keskendub erinevatele intervjuudele, mis käesoleva magistritöö autor on läbi viinud inimestega, kes puutuvad oma professionaalses elus kokku digitaalsete tõendite kasutamisega. Intervjuud annavad võimaluse lugejal mõista, millised kokkupuuted on intervjueeritavatel digitaalsete tõenditega ning kas nende hinnangul esineb digitaalsete tõendite erinevate aspektide osas kitsaskohti. Viimases alapeatükis toob magistritöö autor välja intervjuude järeldused ning oma soovitused digitaalsete tõendite usaldusväärsuse parandamiseks.

[6] Browning, J.G. Angelo, L. „New sources of evidence from the internet of things." Texas Bar Journal. Vol 82, 2019, lk 2.

Käesolev magistritöö on kirjutatud eesti keeles ning resümee inglise keeles. Magistritöö kirjutamisel on kasutatud erinevat erialakirjandust, mida on avaldatud mitmetes kriminalistika ning õigusteaduse väljaannetes. Samuti on erialakirjanduses toetutud antud temaatika ekspertide teostele, sh Eoghan Casey ning Stephen Mason.

Digitaalsete tõendite kohta on Tartu Ülikoolis magistritöö kirjutanud veel Gerd Raudsepp, kelle töö pealkirjaks on „Digitaalsete tõendite kogumise ja kasutamise perspektiivikus kriminaalmenetluses" ning Mari Luuk, kelle töö pealkirjaks on „Digitaalsete tõendite kasutamise erisused". Sisekaitseakadeemias tehtud lõputöödest on Kerly Palm kirjutanud töö nimega „Digitaalsed tõendid ja nende talletamine Põhja Prefektuuri näitel". Käesoleva magistritöö autori hinnangul ei ole digitaalsete tõendite usaldusväärsuse ja problemaatika murekohti eelnevalt nimetatud töödes detailsemalt analüüsitud. Gerd Raudsepp on oma magistritöös küll põgusalt arutlenud digitaalsete tõendite võltsimise üle, kuid ülejäänud osas on tegemist muu temaatikaga.

Käesolevat magistritööd enim iseloomustavad märksõnad on: digitaalsed tõendid, digitaalinformatsioon, tõendid, küberkriminalistika.

1. Digitaalsed tõendid

1.1 Mis on digitaalsed tõendid?

Maailm on konstantses ja kiireloomulises muutuses. Koos sellega muutuvad ka inimeste asjaajamised ning vajadused. Võib spekuleerida, et tänapäevases arenenud riigis ei ole mõeldav, et ühiskonnas toimuks elu nii nagu see toimus sajand tagasi. Täpselt nagu ei ole mõeldav, et võimalik on täielik elektroonikavaba elu. Suur osa tänapäevasest asjaajamisest on autori hinnangul kolinud digitaalsesse maailma, kus raviandmete vaatamiseks, arvete maksmiseks ja muudeks toiminguteks on vaja internetti ja nutiseadet. Ka tänapäevane kohtumenetlus ja tõendite kogumine on sarnase sammu teinud - suure osa tõenditest ja menetlusest moodustavad digitaalsed tõendid.[7] Kahjuks peab sama tõdema ka kuritegevuse kohta. Kiire ühiskondlik areng tähendab, et ka kuritegevus võidutseb aina enam just kübermaailmas. Justiitsministeerium on viidanud asjaolule, et kui võrrelda hetkelist seisukorda 10 aasta taguse ajaga, on arvutikuritegude arv tõusnud kolmekordselt.[8]

Virtuaalne maailm annab pahatahtlikele inimestele palju uusi võimalusi oma tegude toime panemiseks ning sestap on oluline, et ka riiklik korrakaitse ja kohtuvõim on suutelised taolise maailmaga kaasas käima. Ka statistilised andmed viitavad küberkuritegevuse kiirele kasvule ja levikule. Üksnes 2021. aastal oli kokku 1596 arvutikuritegu.[9]

Rahvusvahelise Kriminaalpolitsei Organisatsiooni Interpoli kohaselt on küberkuritegevus kõige kiiremini arenev kuriteotüüp. Taolist kuritegu on tihti võrdlemisi keeruline uurida, kuna tegu pannakse toime kiiresti, tihti on see rahvusvaheline ja seega ka õiguslikult keeruline situatsioon, mis nõuab rahvusvahelist koostööd.[10] Ei ole haruldane situatsioon, kus ohver elab ühes riigis ja kurjategija teises riigis. Eelneva asjaolu tõttu võivad ka erinevad digitaalsed tõendid olla n-ö üle maailma laiali ning neid on seetõttu raske tuvastada. Interneti kõikehõlmavus muudab selle mittetundjate ekspluateerimise eriliselt tõhusaks ja lihtsaks.

---

[7] European Commission „Frequently Asked Questions: New EU rules to obtain electronic evidence." Külastatud 04.03.2022. Arvutivõrgus kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345

[8] Justiitsministeerium „Kuritegevus Eestis 2021". Külastatud 04.03.2022 Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevus2021/arvutikuriteod_page.html

[9] Justiitsministeerium „Küberkuritegude statistika". Külastatud 04.03.2022 Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/kuberkuriteod.html

[10] Interpol „Cybercrime". Külastatud 04.03.2022 Arvutivõrgus kättesaadav: https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Küberkuriteod jagunevad kaheks - arvutisüsteemide vastased küberkuriteod ning ka kuriteod, kus arvutid ja tehnoloogia on vahend, millega pannakse kuritegu toime. [11]

Loomulikult jätab ka küberkuritegevus ja muu virtuaalne tegevus maha jälje, mida võib tihti käsitleda tõendina. Kui mõelda tõendite olemuse peale, tulevad ilmselt meelde erinevad klassikalised füüsilised või bioloogilised tõendid nagu sõrmejäljed, riidekiud või inimese DNA. Kuid tänapäevases maailmas võib klassikaliste tõendite kõrval tõendiks pidada ka tegevust internetis, erinevaid logifaile, meta-andmeid või isegi *e-maile*. Erinevad seadmed tekitavad võimaluse endas hoiustada digitaalses vormis andmeid, mida saab hiljem menetluse käigus kasutada digitaalse tõendina, mis annavad informatsiooni käitumise kohta virtuaalmaailmas. Eelnev aga ei viita sellele, et saadav informatsioon annaks infot ainult käitumise kohta. Nimelt võib digitaalselt hoiustatud informatsioon anda palju informatsiooni ka süütegude kohta, mis on toime pandud füüsilises maailmas.

Digitaalseid tõendeid on võrdlemisi raske defineerida, kuna ei ole ühist definitsiooni selle kohta, mis täpselt on digitaalne tõend. Ka kiirelt arenev tehnoloogia ning uuenduslikud uurimismeetodid raskendavad ühise definitsiooni leidmist, kuna digitaalsete tõendite loetelu võib ajas veelgi suureneda. Liiga kitsas definitsioon ei pruugi olla tuleviku mõttes aga perspektiivikas. Ei ole välistatud, et tulevikus võib digitaalseid tõendeid koguda juba nutikate kodumasinate abil või mingi muu seadmega. Digitaalkriminalistika professor ja autor Eoghan Casey on aga digitaalseid tõendeid defineerinud kui igasugust teavet, mida on talletanud arvuti ning mis toetab või lükkab ümber teooriaid selle kohta, kuidas süütegu toimus, milline oli tahtlus ja *alibi*. [12]

Londoni Ülikooli poolt välja antud õpik viitab aga asjaolule, et Casey definitsioon on liigselt keskendunud kriminaalmenetlusele. Londoni Ülikooli õpikus on digitaalsed tõendid defineeritud kui andmed, mida töötleb, salvestab või edastab mis tahes tootja poolt loodud seade, arvuti või arvutisüsteem või mida edastatakse sidevõrgu kaudu. Need on andmed mis võivad muuta kummagi osapoole poolt esitatud asjaolusid rohkem või vähem tõenäolisemaks. [13]

---

[11] Justiitsministeerium. Kuritegevus Eestis, 2019. Külastatud 04.03.2022. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/

[12] Casey, E. „Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet" 2012 Elsevier Inc, lk 7.

[13] Mason, S. Seng, D. „Electronic Evidence" University of London Press, 2017, lk 19.

Siiski eksisteerib konsensus digitaalsete tõendite omaduste osas. Digitaalsete tõendite puhul võib väita, et need on varjatud ehk latentsed, digitaalseid tõendeid on võimalik võrdlemisi lihtsalt nihutada mitmete jurisdiktsioonide vahel, eelnevaid on lihtne muuta, kahjustada ning hävitada (see võib toimuda ka tavapärase kogumise protsessi käigus) ja tihti on ka märksõnaks aegkriitilisus. [14]

Ka Eesti Vabariigis ei ole digitaalsete tõendite definitsiooni osas veel ühist kehtivat määratlust. Kriminaalmenetluse (KrMs) seadustiku § 63 selgitab, mis on tõend. KrMs defineerib tõendit kui ,,kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või videosalvestis, samuti muu dokument ning foto või film või muu teabetalletus.” Sama sätte lõige 2 lisab veel, et kriminaalmenetluse asjaolude tõendamiseks võib kasutada ka esimeses paragrahvis loetlemata tõendeid, välja arvatud juhul, kui on tegemist kuriteo või põhiõiguse rikkumise teel saadud tõendiga.[15] Seega kehtivas kriminaalmenetluse seadustikus ei ole täpselt antud temaatikat defineeritud, kuigi digitaalsed tõendid on juba mitmete erinevate menetluste jaoks hindamatu osa. Digitaalsed tõendid on üritatud on mahutada ,,füüsiliste tõendite” regulatsiooni alla. [16]

Kriminaalmenetluse seadustik läbis ka revisjoni, mille eesmärgiks oli süsteemne KrMS analüüs kohtueelse menetluse perspektiivist. Revisjoni ajakava järgi kestis revisjon aastast 2015 kuni 2020 aasta jaanuarini ning üheks probleemkohaks olid ka digitaalsed tõendid ning üleminek täisdigitaliseeritud kriminaalmenetlusele. Ka justiitsministeerium nentis, et digitõendeid kasutatakse kriminaalmenetlustes üha enam, kuid kehtiv õigus ei sätesta eraldi menetluskorda ja digitõendite kogumise põhimõtteid. Just eelnevast asjaolust tingituna on seni lähtutud tavapäraste tõendite kogumise ja uurimise seadusandlusest. Tuleb aga tunnistada, et n-ö klassikalised füüsilised tõendid ja digitõendid on erinevad ja seetõttu võib selline olukord tekitada segadust. [17]

---

[14] Laurits, E. ,,Mõned probleemid arvutisüsteemi läbiotsimisel” Kohtute aastaraamat, Riigikohus, 2015, lk 135-136.
[15] Kriminaalmenetluse seadustik - RT I, 22.12.2021, 45
[16] Laurits, E. ,,Mõned probleemid arvutisüsteemi läbiotsimisel” Kohtute aastaraamat, Riigikohus, 2015, lk 136.
[17] Justiitsministeerium ,,Kriminaalmenetlusõiguse revisjoni lähteülesanne”. Tallinn, 2015, lk 9. Külastatud 05.03.2022 Arvutivõrgus kättesaadav: https://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf

Ka Õiguskantsler on antud temaatika osas selgitanud, et: „Arvestades elektroonilise suhtluse laia kasutusala ning elektroonilistes andmekandjates sisalduva info teatavaks saamisega kaasnevat põhiõiguste riive ulatust, oleks siiski asjakohane kaaluda, kas täpsem regulatsioon aitaks kaasa põhiõiguste ja –vabaduste paremale tagamisele.” [18]

Oluline on aga märkida, et kuigi digitõendeid kiputakse seostama just küberkuritegude, muude süütegude ja kriminaalmenetlusega, on digitaalsed tõendid laialdaselt kasutuses ka eraõiguses. Ka kokkulepped ja erinevad ostu-müügitehingud ning kahju tekitamise asjaolud vajavad tõendamist. Näiteks on Ameerika Ühendriikides digitõendid eriti populaarsed töövaidlustes. Tsiviilkohtumenetluse (TsMS) seadustikus on defineeritud dokumentaalseid tõendeid, kuid sarnaselt KrMs-ile on tegu loeteluga, mis otseselt ei defineeri, mis on digitaalne tõend ja selle eesmärk. Nimelt on TsMS-i kohaselt dokumentaalne tõend „igasugune kirjalikult, pildistamisega või video-, heli- või elektroonilise salvestusega või muu andmesalvestusega jäädvustatud dokument või muu sellesarnane andmekandja, mis sisaldab andmeid asja lahendamiseks tähtsate asjaolude kohta ja mida on võimalik kohtuistungil esitada tajutaval kujul.” [19]

Digitaalsetest tõenditest on mitmetes menetlustes suur abi. Nimelt inimese käitumine digitaalmaailmas annab uurimisasutustele tihti rohkem informatsiooni inimese kohta kui tema pere või sõbrad. Inimese personaalne arvuti ja tegevus võrgus viitab erinevatele käitumismustritele, harjumistele ja huvidele. Tänu erinevatele digitaalsetele näitajatele on võimalik uurida, kas inimene oli süüteo toimepanemise ajal nutiseadmes, kas tema nutiseadmes on informatsiooni, mis kinnitab süüteo toimepanemist (nt lapspornograafia omamine) või on inimene avaldanud virtuaalses vestluses tahet süütegu toime panna.

Näitena võib välja tuua Tartumaal toimunud juhtumi, kus grupp noormehi peksid surnuks oma eakaaslase ning seejärel süütasid tema surnukeha. Antud juhtumis oli olulisel kohal suhtlusrakendus *Facebook Messenger* (nüüd tuntud kui *Messenger by Meta*), mille abil lõid kurjategijad ohvriga kontakti. Selleks, et ohvrit enda juurde meelitada, kirjutas üks ründe

[18] Õiguskantsleri arvamus eelnõule: kriminaalmenetluse seadustiku jt seaduste muutmise eelnõu (295 SE), 2012, lk 7. Külastatud 31.01.2022. Arvutivõrgus kättesaadav: https://www.oiguskantsler.ee/et/seisukohad/seisukoht/arvamus-eeln%C3%B5ule-kriminaalmenetluse-seadustiku-jt-seaduste-muutmise-eeln%C3%B5u-295
[19] Tsiviilkohtumenetluse seadustik - RT I, 22.12.2021, 23

osalistest kannatanule *Facebook Messengeri*, paludes temaga kokku saada. Tartu Maakohtu otsusest selgub, et suhtlusportaali *Facebook Messengeri* vestluste väljavõte tõendas kannatanu välja kutsumise aega ja ka selle eesmärki. Ka asitõendite hulgas on välja toodud *Facebook Messengeri* arhiivifail. [20]

Eelnev juhtum illustreerib ideaalselt seda, kui oluliseks võivad osutada erinevad digitaalsed tõendid nii juhtlõngade leidmisel kui ka süü tõendamisel ja asjaolude väljaselgitamisel. Ka välismeediast leiame erinevaid suurt tähelepanu tõmmanud juhtumeid, kus digitaalsed tõendid aitavad kaasa juurdluse edasisele käigule, kuid samas annavad ka palju informatsiooni ohvri või süüteo toimepanija iseloomu, käitumise, psühholoogia ja huvide kohta.

Üks selline juhtum on Sharon Lopatka mõrv. Tegemist on 1996. aasta juhtumiga, kuid märgiliseks muudab juhtumi see, et tegemist oli esimese kaasusega, kus politsei arreteeris kahtlusaluse peamiselt e-kirjade vahetusest kogutud tõendite alusel. Sharon Lopatka informeeris oma abikaasat, et ta sõidab linnast ära selleks, et sõpradega kokku saada, kuid ta jättis oma abikaasale kirja, mille ebatavaline sisu pani mehe muretsema ja ta otsustas korrakaitseasutusega ühendust võtta. Politsei uuris Sharoni e-kirju ning nad avastasid sadu e-kirju Sharoni ja Robert Glassi nimelise mehe vahel. E-kirjade sisu paljastas Sharoni ja Roberti tegelikud huvid, milleks olid seksuaalfantaasiad piinamise ja surma kohta. E-kirjad ebatavalise sisu tõttu otsustasid politseinikud uurida Robert Glassi kodu. Tegemist oli tulemuslikud otsinguga, kuna Robert Glassi kodu juurest leiti ka Sharon Lopatka surnukeha. Ohvri käed ja jalad olid kinni seotud ning ta oli surnud asfüksia tagajärjel. Robert oli pärast ohvri tapmist matnud ta oma kodu juurde. Robert Glass tunnistas ennast süüdi. [21]

Tegemist on juhtumiga, mis illustreerib digitaalsete tõendite võimekust avaldada vajalikku informatsiooni nii kannatanu kui ka süüteo toimepanija kohta. Kui antud juhtumi puhul ei oleks politsei uurinud ohvri e-kirju, siis on võimalik, et kuriteo lahendamine oleks palju keerulisem, kuna ohvril ei olnud toimepanejaga muud nähtavat seost. Nende suhe oli eelnevalt olnud puhtalt virtuaalne.

[20] Tartu Maakohtu kohtuotsus nr 1-20-4575, 21.04.2021
[21] Casey, E ,,Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet" 2012 Elsevier Inc, lk 6.

Lähitulevikus on oodata ka Eestis digitaalsete tõendite kiiret kasvu. Nimelt allkirjastasid justiitsminister Maris Lauri ja siseminister Kristian Jaani kokkuleppe, mille eesmärgiks on aastaks 2025 digitaliseerida suurem osa süüteomenetlusi. Digitaalne menetlus annab võimaluse kasutada kaasaegsemaid lahendusi, muudab lihtsamaks piiriüleste juhtumite lahendamist ja samas arvestab rohkem ohvrite vajadustega. Samuti väheneks bürokraatia. Tänu digitaalsele menetlusele on tulevikus võimalik kasutada rohkem videosalvestusi ning tulevikus ka virtuaal- ja liitreaalsuse tehnoloogiaid. [22]

Seega võib järeldada, et digitaalsed tõendid annavad tihti erinevates juhtumites väärtuslikku informatsiooni, kuid Eestis puudub antud temaatika osas eriregulatsioon. Samuti võib järeldada, et digitaalsetel tõenditel on võrreldes ,,füüsiliste tõenditega" mõned eriomadused.

1.2 Digitaalsete tõendite ja digitaalse ekspertiisi ajalugu

Teatavasti ei ole arvutid ja muu modernne tehnoloogia alati olnud osa inimeste elust. Mitmeid aastakümneid tagasi ei olnud tavapärane, et inimestel on kodus arvuti, nutiseadmeid ei olnud isegi veel olemas ja kontseptsioon arvutiga toime pandud kuriteost tundus utoopilisena.

Esimene arvuti nägi ilmavalgust alles 19. sajandi alguses ning selle loojaks peetakse mehaanikainseneri Charles Babbage'it.[23] Arvuti ja selle võimekus arenes jõudsalt edasi, kuid tegemist oli siiski pigem industriaalseadmega, mida kasutasid suurkorporatsioonid, ülikoolid või riigiasutused. Arvuti muutus populaarseks ja tavapäraseks nähtuseks inimeste kodudes alles 80-ndatel.

1976. aastal kirjutas infoturbe ekspert Donn Parker raamatu ,,*Crime by Computer*". Tegemist on esimese teosega, mis kirjeldab, kuidas on võimalik digitaalsel kujul informatsiooni kasutada kuritegude uurimisel ja kuidas on võimalik süütegusid toime panna arvuti abil. Parkeri kirjutatud teos pälvis ka mitme õiguskaitseorgani tähelepanu. Nimelt Ameerika Ühendriikide Föderaalne Juurdlusbüroo (FBI), Ameerika Ühendriikide kaitseministeerium ja

[22] Justiitsministeerium. ,,Süüteomenetlus muutub digitaalseks ning asjatut bürokraatiat vältivaks". 2021. Külastatud 30.03.2022. Arvutivõrgus kättesaadav: https://www.just.ee/uudised/suuteomenetlus-muutub-digitaalseks-ning-asjatut-burokraatiat-valtivaks
[23] Skulrattanakulchai, A. ,,Charles Babbage, A Man before His Time" 2017, lk 1.

muud asutused otsustasid teose tõttu komplekteerida esimesed töörühmad, mis olid pühendatud just arvutitele ja sellega seonduvale kuritegevusele. Tegemist ei olnud tol momendil veel tavapärase probleemiga, kuid õiguskaitseorganid teadsid, et tulevikus võib *status quo* muutuda. [24]

Arvutite laialdane populariseerimine tõi omakorda kaasa suure hulga inimesi, kelle jaoks arvuti muutus huvitegevuseks. Taoliste hobidega inimeste hulgas olid ka erinevate õiguskaitseorganite töötajad üle maailma. Hobikorras arvutitega tegelemine tähendas aga, et tegemist on inimestega, kellel on tavapärasest paremad teadmised informaatika osas. Just tänu eelnevale mõistsid nad, et arvutid võivad olla tõendite allikad ja ilmselt hakkavad need tulevikus mängima olulist rolli erinevates kriminaalmenetlustes. Ennatlikult lõid nad esimese organisatsiooni, mis oli täielikult pühendatud digitaalsele ekspertiisile - *the International Assosciation of Computer Investigative Specialists* ehk IACIS. [25]

Digitaalse ekspertiisi [26] näol on tegemist kriminalistika ühe haruga, mille eesmärgiks on elektrooniliselt salvestatud andmete tuvastamine, hankimine, töötlemine ning analüüsimine. Taolise ekspertiisi sihiks on hankida elektroonikaseadmetest andmeid, mida saab töödelda arusaadavaks informatsiooniks, mida saab omakorda kasutada süüdistuse esitamiseks. [27]

Kuigi digitaalne ekspertiis on laialdaselt kasutusel kriminaalasjades, ei ole see kindlasti ainus kasutusala. Digitaalset ekspertiisi esineb tihti ka eraõiguslikes suhetes, näiteks on digitaalse ekspertiisi kasutamine võrdlemisi levinud töövaidluste lahendamisel.[28] Samuti ärispionaaži juhtumite tuvastamisel [29] ning ka intellektuaalse omandi varguse tuvastamisel. Digitaalsete tõendite kasutusala mitmekesisust kinnitab ka WIPO (World Intellectual Property Organization) poolt loodud programm nimega „WIPO Proof", mille abil oli võimalik faili eksistentsi ajaliselt kontrollida. [30]

---

[24] Pollitt, M. „A History of Digital Forensics". International Conference on Digital Forensics, 2010, lk 5.
[25] Samas, lk 6.
[26] Tihti tuntud kui ka arvutikriminalistika, digitaalkriminalistika või küberkriminalistika.
[27] Interpol. „Digital Forensics" Külastatud 02.04.2022. Arvutivõrgus kättesaadav: https://www.interpol.int/How-we-work/Innovation/Digital-forensics
[28] Vacca, John R.,, Computer Forensics: Computer Crime Scene Investigation. Charles River Media Inc. 2002, Massachusetts lk 4-5
[29] Dokko, J. Shin, M. „A Digital Forensic Investigation and Verification Model for Industrial Espionage" Digital Forensics and Cyber Crime, 2019, lk 2.
[30] World Intellectual Property Organization. WIPO Proof. Külastatud 02.04.2022. Arvutivõrgus kättesaadav: https://www.wipo.int/wipoproof/en/

1993. aastal toimus FBI Akadeemias Quanticos konverents nimega *First International Conference on Computer Evidence*. Konverentsil osalesid 26 riigi esindajad ning jõuti järeldusele, et efektiivsuse eesmärgil on erinevatel õiguskaitseorganitel vaja teha rahvusvaheliselt koostööd. Mõistagi olid esimesed uuritavad juhtumid tänapäeva mõistes võrdlemisi algelised ja tihti oli peamine eesmärk ühest arvutist andmete kättesaamine ja kasutamine. Kuid siiski mõisteti, kui laialdaseks võib taoline probleem tulevikus kujuneda.

Õiguskaitseorganid mõistsid aga kiiresti kui oluline ja vajalik on digitaalse kriminalistika teadus ning seetõttu arenes kiirelt ka ekspertide väljakoolitamine. Eelnevat asjaolu tingisid mitmed faktorid - elektroonikaseadmete arvu kiire kasv inimeste seas, lapspornograafia hoogne levimine internetis, muud küberkuriteod jne. Oli selge, et korrakaitse peab kaasas käima tehnoloogia levikuga. Enam ei piisanud politseitöö tavateadmistest ning mõelda oli vaja ekspertide peale, kes oskaks käsitleda juhtumi n-ö digitaalseid aspekte ja kes on võimelised sündmuskohalt leidma digitaalsete tõendite allikaid. Kaasajal on mitmed ametnikud üle maailma juba vastavad koolitused saanud.

Alates 2005. aastast on digitaalse ekspertiisi valdkond arenenud väga kiiresti nii meetodite kui ka võimaluste poolest. Digitaalse ekspertiisi ekspertide vajadus kasvas ning tekkisid esimesed akadeemilised programmid, mis taolisi oskuseid ka õpetasid. [31] Tänapäeval on tegemist juba erialaga, millest on saanud võrdlemisi populaarne karjäärivalik. Pädevad digitaalkriminalistika eksperdid tagavad, et kõikidest süüteoga seonduvatest seadmetest oleks võimalik leida digitaalsed tõendid, mis kindlustavad menetluse efektiivsuse ja aitavad paremini lahendada toime pandud kuritegusid.

Seega on digitaalse ekspertiisi ajalugu võrdlemisi lühike, kuid see on olnud kiires muutuses. 40 aasta jooksul on olnud mitmeid muutusi nii ekspertide vajaduse osas kui ka üleüldise võimekuse osas. Möödas on ajad, kus ekspertide ainsaks mureks oli ühest arvutist andmete kättesaamine - arenenud on nii digitaalkriminalistika valdkond kui ka kuriteod, mida pannakse toime arvutit kasutades.

Nüüdisajal peetakse digitaalkriminalistikat üheks kohtuekspertiisi haruks. Eelnevat on kohtuekspertiisi haruna tunnustanud mitmed organisatsioonid, s.h Austraalia Riiklik

[31] Pollitt, M. „A History of Digital Forensics". International Conference on Digital Forensics, 2010, Hong Kong, Hiina, lk 11-13

Kohtueksperti Instituut (Australian National Institute of Forensic Science), Ameerika Ühendriikide Riiklik Standardite ning Tehnoloogia Instituut (United States National Institute of Standards and Technology) ning Euroopa Kohtueksperti Instituutide Võrgustik (European Network of Forensic Science Institutes).[32]

On selge, et digitaalkriminalistika ja digitaalsed tõendid muutuvad aina suuremaks osaks korrakaitsest ja õiguskultuurist ning seega on oluline, et on olemas eksperdid, kes suudavad taolise muutusega efektiivselt kaasas käia. Eelnevale asjaolule viitavad erinevad statistilised näitajad. Näiteks on Interpol hinnanud, et digitaalkriminalistika turg kasvab igal aastal umbes 15,9%. 2017. aastal hinnati digitaalkriminalistika turu suuruseks umbes 4,62 miljardit dollarit. 2022. aastaks hinnatakse, et turu suuruseks on juba 9,68 miljardit dollarit.[33] Lisaks eelnevale on Euroopa Komisjon hinnanud, et umbes 85% juhtumitest kriminaalmenetlustes omavad digitaalsete tõendite kasutamise vajadust. [34]

1.3 *Chain of Custody*

Teatavasti on erinevate tõendite kasutamine kriminaalmenetluses koordineeritud rohkete reeglitega, et kindlustada tõendite efektiivsus ja lubatavus. Erinevad riigid on tõendite kogumise ja kasutamise protsessi reguleerinud erinevalt, mõned karmimalt ning mõned leebemalt. Näitena võib siin välja tuua Vene Föderatsiooni, kus on asitõendite kogumisel üldjuhul nõutud, et kogumise protsessi vaatleks vähemalt kaks tunnistajat, kes saavad hiljem tunnistada asitõendite kogumise protsessi legaalsuse ja tulemuste osas.[35] Nigeerias on aga tõendite kogumisest täiesti erinev arusaam. Nimelt on tõendite puhul kõige olulisemaks asjaoluks just see, et tõend oleks menetluse suhtes relevantne. Küsimus selle kohta, kas tõend on soetatud legaalselt või illegaalselt Nigeerias erilist rolli ei mängi, kuna põhirõhk on siiski

[32] Sunde, N, Dror, I.E. „Cognitive and human factors in digital forensics: Problems, challenges, and the way forward" Digital Investigation Volume 29, 2019, lk 1.
[33] Reedy, P. „Interpol review of digital evidence 2016 - 2019" Forensic Science International: Synergy Vo 2, 2020, lk 608.
[34] European Commission „Frequently Asked Questions: New EU rules to obtain electronic evidence." Külastatud 02.04.2022. Arvutivõrgus kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
[35] Уголовно-процессуальный кодекс Российской Федерации от 18.12.2001 N 174-ФЗ (ред. от 25.03.2022). Külastatud 04.04.2022. Arvutivõrgus kättesaadav: http://www.consultant.ru/document/cons_doc_LAW_34481/4160be26d48139e507d797da966e407b4662acfe/

suunatud tõendi olulisusele menetluses. Nimelt kirjeldab Nigeeria Asitõendite Akti (*Nigerian Evidence Act*) 14. artikkel järgnevat:

Evidence obtained-
(a) improperly or in contravention of a law; or
(b) in consequence of an impropriety or of a contravention of a law

shall he admissible unless the court is of the opinion that the desirability of admitting the evidence is out-weighed by the undesirability of admitting evidence that has been obtained in the manner in which the evidence was obtained.

Seega on illegaalsel teel saadud tõendeid teoorias siiski võimalik kasutada, kui Nigeeria kohus seda lubab. [36]

Nigeeria vaatepunkt läheb aga otseselt vastuollu mitmete teiste riikide põhimõtetega, mis nõuavad, et asitõendeid kogutakse legaalsel viisil. Üheks selliseks riigiks on näiteks Ameerika Ühendriigid.[37] KrMS-i 3. peatükk loetleb erinevaid põhimõtteid, mida tuleb arvestada tõendite (sh digitaalsete tõendite) kogumisel, samuti tuleb tõendite kogumisel arvestada Riigikohtu praktikaga. KrMS-i § 126^1 lg 4^{38} viitab küll, et Eestis tuleb jälitustegevusega saadavaid tõendeid koguda rangelt seaduse järgi, kuid kõigi teiste kriminaalmenetluses kogutavate tõendite puhul ei ole seaduse rikkumine küll eetiline, kuid siiski kehtib reegel, et tõend on siiski lubatav, kui selle kasutamine ei tee menetlust tervikuna ebaõiglaseks.[39] Täielikult ei keela seda ka Euroopa Inimõiguste Kohus.[40] Digitaalsete tõendite kogumisel tuleb Eestis seega lähtuda KrMS-i 3. peatükis välja toodud põhimõtetest ja reeglitest.

Digitaalsete tõendite eriregulatsiooni kui sellist antud ajamomendil Eesti seadusandluses veel ei ole. Autori hinnangul võib see olla aga problemaatiline, kuna tõendite kogumine peab oleme üleriigiliselt ühtne ja selge. Seaduse sõnastus on võrdlemisi üldsõnaline ning see võib

[36] The Nigerian Evidence Act, section 14, 2011. Külastatud 04.04.2022. Arvutivõrgus kättesaadav: https://www.refworld.org/pdfid/54f86b844.pdf
[37] Ameerika Ühendriikides tuntakse seda põhimõtet kui „*Fruits of the poisonous tree*" doktriinina, mida esmalt käsitleti lahendis *Silverthorne Lumber Co. v. United States*, 1920.
[38] Kriminaalmenetluse seadustik - RT I, 22.12.2021, 45
[39] Riigikohtu lahend 1-09-4486 p 40, 22.05.2020
[40] EIKo 12.07.1988, 10862/84, Schenk vs Šveits

praktikas tekitada probleeme. Samuti võib eelnev tekitada murekohti ka juhtumite puhul, kus tekib piiriülese koostöö vajadus, kuna taoline tõend võib olla lubatud ühes jurisdiktsioonis, kuid samas võib see olla automaatselt välistatud mõnes teises jurisdiktsioonis. [41]

Just reeglitel ja põhimõtetel on tõendite kogumisel oluline rõhk. Selleks, et tõendit oleks võimalik kasutada kohtumenetluses, on oluline, et järgitud oleks ka *digital chain of custody* põhimõtet. Eelneva põhimõtte kohaselt dokumenteeritakse kogu digitaalsete tõendite kogumis- ja säilitamisprotsess. Taolise printsiibi peamine eesmärk on tagada digitaalsete tõendite autentsus, originaalsus ja usaldusväärsus. Kui tõendeid on kogutud viisil, mis vastab nõuetele, on suurem võimalus, et tõendid on kohtus kasutatavad, tõesed ja ei teki vaidlust nende usaldusväärsuse üle. [42]

Eesti digitaalkriminalistika ekspert Pavel Laptev on oma esitluses välja toonud mõned põhimõtted ja metodoloogia, mida tuleks järgida digitaalsete tõendite kogumisel. Need on järgnevad:

1) Esmalt tuleb digitaalne teave hankida oma originaalvormis;
2) kasutatakse heakskiidetud kohtuekspertiisi metoodikat ja tehnoloogiat;
3) kogu tegevus dokumenteeritakse kronoloogilises järjekorras;
4) toiminguid viivad läbi ja tulemusi tõlgendavad kvalifitseeritud eksperdid. [43]

Erialakirjanduses viidatakse aga asjaolule, et mitmete riikide seadused on vastu võetud enne digitaalsete tõendite laialdast levikut ja seadusandlust ei ole vastavalt muudetud.[44] See aga omakorda tähendab, et seadusandlus on digitaalsete tõendite regulatsiooni osas puudulik. Samas rõhutatakse asjaolule, et selleks, et hoida efektiivset *digital chain of custody*'t, on oluline, et tõenditega tegelevad eksperdid omaksid vastavat kvalifikatsiooni. Erialakirjanduses on viidatud asjaolule, et kui puudub range reeglistik *chain of custody* hoidmiseks ja järgimiseks, on võimalik, et digitaalsete tõendite uurimisel ja kogumisel ei

[41] Kasper, A. Laurits, E. „Challenges in Collecting Digital Evidence: A Legal Perspective", Springer, 2016, lk 201
[42] M.N.O Sadiku, A.E. Shadare, S.M. Musa „Digital Chain of Custody"International Journals of Advanced Research in Computer Science and Software Engineering. Volume 7, 2017, lk 1.
[43] Laptev, P. „Digital Forensics view from the Estonian Forensic Science Institute" Estonian Forensic Science Institute. Cybercrime forensics & digital evidence, 2014.
[44] M.N.O Sadiku, A.E. Shadare, S.M. Musa „Digital Chain of Custody" International Journals of Advanced Research in Computer Science and Software Engineering. Volume 7, 2017, lk 1.

rakendata piisaval määral hoolsust.[45] Viidatakse ka elementidele, mida digitaalse *chain of custody* hoidmise puhul tuleks järgida ja dokumenteerida:

1) Omadused - ehk digitaalsete tõendite allikad.
2) Dünaamika - ehk inimesed, kes on digitaalsete tõenditega seotud (sh kahtlusalune, ohver, ametnikud, kriminalistid jne).
3) Faktorid - ehk erinevad küsimused digitaalsete tõendite kohta. Näiteks küsimused tõendi iseloomu kohta, küsimused tõendi kasutaja kohta, tõendi kasutamise kohta jne. Eelnevatele küsimustele saab üldjuhul vastuse leida teiste tõendite abil - sh sõrmejäljed, biomeetria, ajamärgistused, GPS jne.
4) Institutsioonid - ehk institutsioonid, millel oli kokkupuude digitaalse tõendiga (nt politsei, kohtuekspertiisi instituut jne).
5) Terviklikkus - ehk tehnikad, mis garanteerivad digitaalse tõendi terviklikkuse. [46]

Seega võib järeldada, et selleks, et muuta digitaalsete tõendite kogumist ühtsemaks ja efektiivsemaks, on oluline, et paigas oleks kindel reeglistik, mis reguleeriks digitaalsete tõendite kogumise ja uurimise protsessi. Siiani ei ole ühtseid reegleid ka Euroopa Liidus.[47] Eelnevalt on aga konstateeritud asjaolu, et digitaalsed tõendid mängivad suurt rolli paljudes menetlustes, millel on olemas ka rahvusvaheline element. Kasutades aga võõrriigist saadud digitaalseid tõendeid, tuleb kaalutleda asjaolu, et puudub ühtne reeglistik, mis määraks taoliste tõendite kogumisprotsessi legitiimsuse ja kvaliteedi. Just eelnevad näited ilmestavad, kui erinev võib olla tõendite kogumine maailma eri paikades.

Seega võib järeldada, et *chain of custody* on digitaalsete tõendite kasutamisel äärmiselt olulise tähtsusega põhimõte. Eelnev aitab hinnata digitaalse tõendi valiidsust, legitiimsust ja meetodeid, mida on kasutatud tõendi hankimiseks. *Chain of custody* järgimata jätmine võib kaasa tuua situatsiooni, kus väidetakse, et asitõendeid on muudetud, asendatud või neid on mõjutatud. Eoghan Casey hindab, et *chain of custody* järgimata jätmine võib kaasa tuua digitaalse tõendi kasutuskõlbmatuse kriminaalmenetluses, kuna tekkida võib vaidlus asitõendi autentsuse üle. [48]

---

[45] Samas, lk 1
[46] Samas, lk 1.
[47] Stoykova, R. „Digital evidence: Unaddressed threats to fairness and the presumption of innocence" Computer Law & Security Review, Volume 42, 2021, lk 1.
[48] Casey, E. „Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet". 2012 Elsevier Inc, lk 22.

Ühtsed reeglid *chain of custody* osas aitaks autori hinnangul tasakaalustada erinevaid menetlusi üle maailma ning parandada digitaalse tõendi kvaliteeti ja usaldusväärsust.

1.4 Digitaalsete tõendite ja digitaalse ekspertiisi tulevik

On selge, et mitmed aspektid inimeste igapäevaelust on muutunud järjest digitaalsemaks ning infotehnoloogia mängib autori hinnangul aina suuremat rolli inimeste eludes. Eelnevat toetab ka statistika, mis viitab asjaolule, et käesolevaks aastaks on prognoositud, et infotehnoloogilised kulutused küündivad ligi 4,45 triljoni USA dollarini.[49]

Infotehnoloogiline kasv on seega võrdlemisi kiireloomuline ning just eelnevast võib järeldada, et erinevaid muutusi võib kohata ka digitaalse ekspertiisi ning digitaalsete tõendite maastikul. Aina enam on tehnoloogiaturul võimalik näha uudseid seadmeid – nutikad kodumasinad, isesõitvad autod ning muud erinevad nutiseadmed. Eelnevate näol on tegemist uuendusmeelsete seadmetega, mis nõuavad, et ka digitaalne ekspertiis ning vastav seadusandlus jõuaks selle temaatikaga kaasas käia.

Uued ja huvitavad tehnoloogilised lahendused võivad olla positiivseks aspektiks tavakasutaja vaatepunktist, kuid digitaalse ekspertiisi osas võib tehnoloogia kiire kasv tähendada aina keerulisemalt tulevikku. Erialakirjanduses on viidatud asjaolule, et kuigi digitaalse ekspertiisi kasv on olnud võrdlemisi kiire, on siiski uute edusammude saavutamine suhteliselt keeruline. Nimelt on digitaalsele ekspertiisi arengut takistamas mitmed tehnoloogia arenguga seotud asjaolud – näiteks väga erinevad failiformaadid takistavad ühtsete digitaalse ekspertiisi tööriistade loomist ning krüptograafia laialdane levik muudab digitaalsete tõendite kogumise ning lahti mõtestamise äärmiselt keeruliseks. Samuti on problemaatiline digitaalsete tõendite rohkus, tihtipeale on ühel inimesel nutitelefon, arvuti, muud välised andmekandjad ning ka pilveteenus. Eelnev muudab andmete kogumise aga vägagi ajakulukaks.[50]

[49] Sava, J. A. „Information technology (IT) worldwide spending from 2005 to 2023" Statista, 2022. Külastatud 02.04.2022. Arvutivõrgus kättesaadav: https://www.statista.com/statistics/203935/overall-it-spending-worldwide/

[50] Caviglione, L. Mazurczyk, W. Wendzel, S. „The Future of Digital Forensics: Challenges and the Road Ahead" IEEE Security and Privacy Magazine, 2017, lk 1.

Taolised väljakutsed ei tähenda aga, et digitaalse ekspertiisi ning digitaalsete tõendite maastikul puuduksid igasugused uuendused ning realiseerimist ootavad ideed. Nimelt leidub erinevaid eksperte, kes on mõistnud, milles seisnevad kaasaegse digitaalse ekspertiisi vajadused. Taoliste vajaduste alusel on eksperdid välja pakkunud mõtteid erinevateks uuteks kontseptsioonideks, mis muudaksid tõendite kogumise efektiivsemaks.

Ühe näitena võib välja tuua artikli, kus mitmed eksperdid on viidanud asjaolule, et nutitelefonide käitlemine sündmuskohal on protseduur, mida saaks efektiivsemaks muuta n-ö kohapealse triaaži abil. Teatavasti on nutitelefonides suur hulk informatsiooni, mis võib uurimise seisukohalt olla äärmiselt tähtis. Tänapäeval on aga nutitelefonide hulk muutunud nii suureks, et praktiliselt igalt sündmuskohalt on võimalik leida nutitelefon. Iga telefoni saatmine ekspertiisi ning ekspertiisi tulemuste ootamine on aga vägagi ajakulukas, kuid telefonides peituv informatsioon võib olla ajatundlik. Autorite hinnangul mõjutab aga taoline pikk järjekord menetlust ning õigussüsteemi negatiivselt. [51]

Et kiiremini tuvastada informatsioon, mis peitub nutitelefonides, on autorid välja pakkunud idee, mille kohaselt oleks sündmuskohal olemas nutitelefonidele spetsialiseerunud tehnikud, kes on teadlikud digitaalsete tõendite kogumisprotsessi reeglitest ning vajadustest ja kelle kasutuses on vastavad tööriistad analüüsi teostamiseks. Eelneva idee teostamine tähendaks asja lahendamiseks oluliste andmete kiiremat avastamist ning lühemaid järjekordi ekspertiisis. Siiski on idee teostamiseks eelkõige vaja tehnikutele luua tööriistad, mis taolist kohapealset analüüsi teoorias võimaldaksid.[52]

Teatavasti ei ole nutitelefonid ainukesed digitaalsete tõendite allikad ja sestap on vaja ka tööriistu, mis on valmis analüüsima teisi seadmeid. Tuleviku ennustamine on keeruline, kuid erialakirjanduses leidub viiteid asjaolule, et tulevikus võib digitaalsete tõendite analüüsi koormat kergendada tehisintellekt.

Kuigi tehisintellekt on juba digitaalses ekspertiisis kasutusel, ei ole see veel saavutanud oma täielikku potentsiaali. Üldiselt saab tehisintellekti kasutamist digitaalse ekspertiisi valdkonnas jagada kaheks. Esiteks juhtumid, kus tehisintellekti aitab automatiseerida mingit

[51] Mislan, R.P, Casey, E. Kessler, G.C. „The growing need for on-scene triage of mobile devices" Digital Investigation 6, 2010, lk 112
[52] Samas, lk 115

individuaalset osas ekspertiisist. Teiseks aga juhtumid, kus tehisintellekt aitab ekspertiisi teostavat inimest juhendada. Kuigi tehisintellekt ei ole veel digitaalses kriminalistikas väga laialdaselt kasutusel, on autori hinnangul vägagi võimalik asjaolu, et tulevikus suureneb tehisintellekti osakaal digitaalses kriminalistikas märkimisväärselt.[53] Autori hinnangul on tehisintellekt just see tööriist, mis suudaks suurel määral aidata vähendada ekspertide pidevalt suurenevat töökoormat.

Samuti on oluline tähelepanu pöörata asjaolule, et tänapäeval on mitmeid võimalusi informatsiooni hoiustada ka oma seadme väliselt. Eksisteerib mitmeid erinevaid pilveplatvorme, mis annavad võimaluse hoiustada suures koguses informatsiooni „pilves". Oluline on aga märkida, et taolisi andmeid on samuti vaja digitaalse kriminalistika ekspertidel analüüsida ning see võib olla võrdlemisi keeruline ettevõtmine. Esmalt on probleemkohaks jurisdiktsioon, kuna ühest riigist pärit isik võib oma informatsiooni ning andmeid hoiustada teise riigi serverites. Samuti on keeruline luua ühtset ekspertiisi tööriista, kuna puuduvad standardsed liidesed.[54]

Autori hinnangul on pilveteenuste ekspertiis just see digitaalse ekspertiisi valdkond, mis võib tulevikus jõudsalt edasi areneda. Taolist arengut on ka kindlasti vaja, kuna juba üle 3 miljardi inimese kasutab pilveteenuseid.[55] Kuna inimeste seadmete ja informatsiooni rohkus on aina suurem, siis autori hinnangul on oodata ka nende inimeste arvu kasvu, kes otsustavad tulevikus pilveteenuse kasuks. Pilveteenuste digitaalse ekspertiis kasvule ning tulevikule on viidatud ka erialakirjanduses, kus jaatatakse pilveteenuse ekspertiisi kasvavat vajalikkust ning loodetakse näha antud temaatika arengut.[56]

Kuigi digitaalse ekspertiisi valdkonnas võib tulevikus näha mitmeid uuendusi, ei ole see ainukene arenguvaldkond. Ka digitaalsete tõendite seadusandlus võib tulevikus sattuda erinevate muudatuste osaliseks. Ühe olulise arenguna võib välja tuua Budapesti

[53] Mitchell, F „The Use of Artificial Intelligence in Digital Forensics: an Introduction" Digital Evidence and Electronic Signature Law Review, 2010, lk 40-41.
[54] Caviglione, L. Wendzel, S. Mazurczyk, W „The Future of Digital Forensics: Challenges and the Road Ahead" IEEE Security & Privacy, 2017, lk 14.
[55] Statista „Number of consumer cloud-based service users worldwide in 2013 and 2018", 2014. Külastatud 20.04.2022. Arvutivõrgus kättesaadav: .https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/
[56] Caviglione, L. Wendzel, S. Mazurczyk, W „The Future of Digital Forensics: Challenges and the Road Ahead" IEEE Security & Privacy, 2017, lk 14.

konventsioonile [57] teise lisaprotokolli lisamise plaani. Tegemist on vägagi olulise täiendusega, kuna lisaprotokolli üheks peamiseks ülesandeks on parandada kiiret juurdepääsu digitaalsetele tõenditele erinevates piiriülestes kriminaalmenetlustes. Samuti loodetakse lisaprotokolli abil lihtsustada koostööd erinevate Euroopa Liidu liikmesriikide vahel ning edendada võitlust küberkuritegevuse vastu.[58]

Budapesti konventsiooni teise lisaprotokolli allkirjastamistseremoonia toimub 12. mail 2022. aastal.[59] Samuti võib tulevikus näha ka suuremat koostööd Ameerika Ühendriikide ning Euroopa Liidu õigusorganite vahel, kuna 2019. aastal algasid omavahelised läbirääkimised digitaalsete tõendite kättesaadavuse hõlbustamiseks piiriülestes kriminaalmenetlustes. Käesoleva magistritöö kirjutamise ajal eelnevalt viidatud kõnelused veel käivad.[60]

Seega võib digitaalse ekspertiisi ning digitaalsete tõendite maastikul oodata erinevaid muutusi, mis on suunatud koostöö parandamisele ning ka ekspertiisi efektiivsuse tõstmisele. Autori hinnangul on tegemist positiivsete muudatuste ning ideedega, mis võivad muuta võitlust küberkuritegevusega efektiivsemaks.

[57] Tegemist on rahvusvahelise lepinguga, mis reguleerib Interneti teel toime pandud kuritegusid. Konventsioon käsitleb eelkõige autoriõiguste rikkumisi, arvutipettusi, lapspornograafiat ja võrguturbe rikkumisi. Konventsioon on kättesaadav Euroopa Nõukogu kodulehel: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=185

[58] Council of the European Union ,,Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence,, Explanatory Report. Külastatud 20.04.2022. Arvutivõrgus kättesaadav: https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b

[59] Council of the European Union ,,Access to e-evidence: Council authorises member states to sign international agreement", 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/

[60] Council of the European Union ,,Better access to e-evidence to fight crime", 2022. https://www.consilium.europa.eu/en/policies/e-evidence/

2. Digitaalsete tõendite usaldusväärsust mõjutavad aspektid

Digitaalsete tõendite ja digitaalkriminalistika kiiret arengut ja laialdast kasutust erinevates menetlustes võib pidada pigem positiivseks asjaoluks. Digitaalsed tõendid ja digitaalkriminalistika loovad aina rohkem erinevaid võimalusi teabe avastamiseks, süütegude lahendamiseks ja menetluse efektiivsuse parandamiseks. Mitmete juhtumite puhul on digitaalsed tõendid just need, mis on aidanud lahendada kuriteo, mis oleks muidu suure tõenäosusega lahendamata jäänud.

Kuigi digitaalsetel tõenditel on suur hulk positiivseid aspekte, tekib siiski paratamatult küsimus, kas tegemist on täiesti kasutuskõlbuliku tõendiallikaga. Kas digitõendid on alati piisavalt usaldusväärsed ja objektiivsed ning kas nende autentsuses ning legitiimsuses ei pea kahtlema? Kohtuvaidluses üritab vastaspool sageli kahtluse alla seada tõendite autentsuse ja usaldusväärsuse ning seda on võimalik teha ka digitaalsete tõendite puhul. Järgnevas peatükis analüüsib autor erinevaid aspekte, mis võivad digitaalsete tõendite usaldusväärsust mõjutada. Samuti toob autor näiteid välismaa erialakirjandusest ning kohtulahenditest, mis aitavad lugejal paremini mõista digitaalsete tõendite potentsiaalseid kitsaskohti.

2.1 Üldine usaldusväärsus

Digitaalsete tõendite kogumine on vaid üks osa menetlusest. Omakorda väga oluline osa on ka digitaalsete tõendite hindamisel ja kasutamisel. Eelnevalt on konstateeritud, et üks oluline asjaolu, mis annavad infot digitaalse tõendi kogumise legitiimsuse kohta on digitaalse tõendi *chain of custody*. Samas eksisteerib ka teisi erinevaid faktoreid, mis annavad teavet tõendi terviklikkuse, kvaliteedi ja usaldusväärsuse osas.

Teatavasti on kaasajal arvutisüsteemid juba võrdlemisi keerulised ning kindlasti ei ole mõistlik kahelda selles, et süsteemide keerukus süveneb tulevikus veelgi. Eoghan Casey viitab asjaolule, et digitaalkriminalistika ekspert peab aga olema suuteline hindama oma järelduste tõenäosust, kuid digitaalkriminalistikas puudub üldiselt aktsepteeritud konkreetne matemaatiline meetod selle tegemiseks.[61] Seega puudub digitaalsete tõenditega tegeleva eksperdi järelduste tõenäosuse osas hindamise osas ühtsus. Eelnevat asjaolu tingib arvutite

[61] Casey, E. „Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet". Elsevier Inc, 2012, lk 68-72.

keerukas ülesehitus ja kiire areng. Arusaadavalt on raske järge pidada temaatika osas, mis on pidevas muutuses.

Arvutid on suutelised looma ja talletama informatsiooni mitmete erinevate aspektide kohta, kuid taolise informatsiooniga võivad kaasneda erinevaid ebatäpsuseid. Probleeme võib esineda muuhulgas seadme sisemise kella osas ja asukoha osas. Nimelt võib arvuti sisemine kell olla vale, s.t mittevastavuses tegeliku kellaajaga ja kuupäevaga. Samuti võib muudetud olla ka ajatsoon, milles arvuti paikneb. Eelnev asjaolu aga tähendab, et ajamärgistusi võib tõlgendada ebakorrektselt. Sama probleem võib tekkida ka infoga, mis puudutab asukohta. Allika IP-aadress võib olla suunatud proksiseadmesse.[62] Samuti ei pruugi mobiiltelefoni GPS-i koordinaadid tõeväärsed olla. Teatavasti on arvuti sisemist kella ja kuupäeva võimalik muuta ja seega tuleks ajamärgistusse alati suhtuda kriitiliselt.[63] Need on vaid mõned näited, mis viitavad erinevatele meetodile, kuidas on võimalik arvuti poolt salvestatava informatsiooniga manipuleerida.

Mõistagi kasutavad digitaalkriminalistika eksperdid erinevaid tehnikaid ja tööriistu. Täpselt nagu klassikaliste tõendite puhul on erinevad meetodid teabe kogumiseks, on loodud erinevaid tarkvarasid, mis aitavad ekspertidel analüüsida ning koguda just digitaalseid tõendeid. Erialakirjandus viitab aga asjaolule, et mitmetes välismaistes menetlustes on tekkinud küsimus just digitaalsete tõendite kogumise jaoks loodud tarkvara ja meetodite usaldusväärsuse kohta.

Nimelt on Eoghan Casey oma õpikus pööranud tähelepanu asjaolule, et Ameerika Ühendriikides on enamik osariikidel kriteeriumid selleks, et hinnata uudseid teaduslikke tõendeid. Eelnevad kriteeriumid tulenevad 1993. aasta lahendist *Daubert v. Merrell Dow Pharmaceuticals, Inc* ning need on järgnevad:

1) Esmalt tuleb kaalutleda, kas seda tehnilist võtet või teooriat on võimalik katsetada või kas seda on juba katsetatud.
2) Järgnevalt tuleb analüüsida, kas esineb kõrge teadaolev/potentsiaalne veamäär ning kas on olemas antud tehnilise võtte või teooria toimimist kontrollivad standardid.

[62] Võrguliikluse lähte-IP-aadress võib olla suunatud proksiserverile, mitte tegelikule arvutile, mida kasutati teo toime panemiseks.
[63] Casey, E. „Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet". 2012 Elsevier Inc, lk 68-69

3) Kas tehniline võte või teooria on läbinud vastastiku eksperthindamise ja publitseerimise.
4) Viimasena tuleb kaalutleda, kas tehniline võte või teooria on pälvinud kõnealuse eriala ekspertide heakskiidu.[64]

Kitsaskohaks kujuneb seega arvutite ja seadmete kiire areng. Nimelt limiteerib kiire areng ja üldine keerukus uurimismeetodite katsetamise ning hindamise ajalist pikkust ja efektiivsust. Ehk uued meetodid ei pruugi piisavalt kaua aega viita testimisfaasis. See, aga omakorda tähendab, et uurimismeetod ei pruugi olla piisavalt usaldusväärne ning tähelepanuta võivad jääda vead, mis võivad esineda programmis. See võib seada aga seada digitaalsete tõendite usaldusväärsuse kohtumenetluses küsimärgi alla, kuna tõend annab teavet, mis ei ole tegelikkuses õige.

Kuigi Eesti õiguskorras ei ole tõenditele taolisi kriteeriumeid loodud, on siiski oluline märkida, et antud temaatika võib tulevikus ka Eestit tabada. Nimelt rõhutab Casey veel, et mitmetes digitaalsete tõendite töötlemise tarkvarades ja tööriistades on avastatud erinevaid veateateid, mis võivad omakorda kaasa tuua asitõendite koha pealt ebakorrektseid järeldusi. Tegemist on autori hinnangul võrdlemisi suure probleemiga, kuna erinevad tarkvarad on laialdaselt kasutatud üle maailma ning tähelepanuta jäetud veateated võivad viia valede järeldusteni. Valed järeldused võivad aga kriminaalmenetluses viia katastroofiliste tulemusteni.

Lisaks on autor viidanud asjaolule, et arvutite keerulise ehituse ja pideva arengu tõttu ei ole välistatud, et digitaalseid tõendeid analüüsiv isik satub vastamisi olukorraga, mida ei ole veel digitaalkriminalistika valdkonnas ette tulnud. Eelnev asjaolu aga tähendab, et taolise situatsiooni lahendamiseks ei ole veel koostatud mingisugust dokumenteeritud käitumissoovitust. Kõik eelnev kogumina viitab aga omakorda asjaolule, et ekspert võib ennenägematut olukorda tõlgendades jõuda järelduseni, mis ei ole korrektne ja ei peegelda tegelikku olukorda. [65]

Seega peab alati hindama kui usaldusväärsed on tööriistad, mida me kasutame digitaalsete tõendite kogumiseks ja kui täpne on esialgne informatsioon, millele digitaalsed tõendid

[64] Casey, E. „Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet." Elsevier Inc, 2012, lk 73-75.
[65] Samas, lk 73-75

viitavad. Ainult nii saab tagada, et tõendid peegeldavad tegelikkust ja karistatud saab õige isik. Ameerika Ühendriikide kohtupraktikast võib juba leida olukordi, kus digitaalkriminalistikas kasutatava tarkvara legitiimsuse osas on tõstatatud põhjendatud küsimusi. Eelnevat näitlikustab järgnev näide.

Ameerika Ühendriikides on lapspornograafia tabamiseks laialdaselt kasutatav tarkvara nimega Child Protection System (CPS), mis suudab lapspornograafiat kujutava sisuga failide edastamist seostada arvuti IP-aadressiga. Tarkvara suutis tuvastada, et sellise sisuga faile on edastanud ka T. Tolworthy ning mehele esitati süüdistus. Kui uurijad hakkasid aga Tolworthy arvutit täpsemalt uurima, ei suutnud nad taolise sisuga faile tuvastada. Juhtum pälvis ka nimeka inimõigusi kaitsva organisatsiooni tähelepanu ning organisatsioon tegi antud juhtumi osas Ameerika Ühendriikide justiitsministeeriumile (U.S Department of Justice) arupärimise. Muuhulgas soovis organisatsioon justiitsministeeriumilt ka vastuseid selle kohta, kas antud tarkvara on üldse varem läbinud katsetusfaasi ning millised on tarkvara veamarginaalid. Samuti viitas organisatsioon asjaolule, et taolise programmi kasutamine politsei poolt võib riivata põhiõigusi, kuna programmi efektiivsust ei ole täielikult tuvastatud. [66]

Taolised situatsioonid võivad autori hinnangul potentsiaalselt tekitada samas ka olukorra, kus inimene on reaalselt süüdi, kuid kohtumenetluses seatakse kahtluse alla digitaalkriminalistiliste ,,vigaste" tarkvarade abil analüüsitud tõendite usaldusväärsuse. Kriminaalmenetluses kõrvaldamata kahtlused tuleb aga tõlgendada süüdistatava kasuks ning süüdlane võibki puhtalt pääseda. Autor näitlikustab oma väidet näitega Ameerika Ühendriikide kohtupraktikast.

Nimelt sai eelnevalt viidatud asjaolule, et Ameerika Ühendriikides on asitõenditele loodud kriteeriumid, mis tagavad asitõendi teaduslikku väärtuse. Kui aga kriteeriumeid ignoreeritud, siis on võrdlemisi kerge kahtluse alla seada tõendi legitiimsust. Taoline situatsioon tekkis Todd Hartmani kaasuses. Hartmani vastu oli kogutud tõendeid samuti CPS tarkvara abil. Nimelt aitas CPS tuvastada, et Hartmani IP-aadress on seotud lapspornograafiaga. Hartman vahistati ja tema arvutist tuvastati vastavasisulist materjali. Seega antud juhul tarkvara töötas korrektselt ja andis vajalikku informatsiooni, mis aitas kinni pidada pedofiilia kalduvustega

[66] Human Rights Watch ,,Letter to US Department of Justice About Child Protection System Software", 2019. Arvutivõrgus kättesaadav: https://www.hrw.org/news/2019/04/03/letter-us-department-justice-about-child-protection-system-software

kurjategija. Probleemkohaks muutus aga kohtuprotsess, kuna taoliste juhtumite puhul tekib kaitsjatel ideaalne võimalus kahtluse alla seada digitaalsete tõendite usaldusväärsuse. Nii juhtus ka Hartmani kaasuses ning tänu eelnevale Hartman karistada ei saanud. [67]

Taoliste kaitsestrateegiate levikule viitab ka Tami Loehrs, kes töötab digitaalkriminalistika eksperdina. Nimelt loetleb ta üle 60-ne juhtumi, kus kaitsjate peamiseks strateegiaks on digitaalsete tõendite kahtluse alla seadmine.[68] Selleks, et tagada, et kurjategijad ei pääseks karistusest üksnes digitaalsete tõendite ja digitaalkriminalistiliste tarkvarade kahtluse alla seadmise pärast, on vaja garanteerida, et nii tõendite kogumine kui ka tööriistad selle tegemiseks, on usaldusväärsed, läbipaistvad ja läbinud vastava kontrolli.

Tihti on arvutite, digitaalsete tõendite ja digitaalkriminalistika osas justkui uskumus, et tegemist on täiesti usaldusväärsete meetoditega ja arvutid, erinevalt inimestest, ei ole võimelised eksima. Tegelikkus taolist illusiooni ei peegelda. Kui niinimetatud klassikaliste tõendite osas rakendatakse ranget kontrolli ja pidevalt käib arutelu nende tõesuse üle, siis digitaalsete tõendite ja digitaalkriminalistika osas puudub praegusel ajamomendil tagatis kvaliteedi ja vastavuse osas. Samuti puuduvad digitaalkriminalistika ja digitaalsete tõendite teadusliku valideerimise osas Euroopa Liidus ühtsed standardid. [69] Kui n-ö klassikalised tõendid läbivad pidevalt rahvusvahelisi eksperthinnanguid, siis digitaalkriminalistika puhul veel taoline ühtsus hindamise ja akrediteerimise osas puudub. Ka Ühendkuningriikide digitaalkriminalistika strateegiast joonistub välja sama problemaatika. Nimelt on eksperdid viidanud asjaolule, et digitaalkriminalistika osas puudub igasugune teaduslik kontroll, mis tuvastaks, kas kasutatav tarkvara ja meetodid on üldsegi usaldusväärsed. [70] Taoline puudujääk kontrolli osas võib aga viia tulemuseni, kus kasutatakse meetodit, mis ei anna legitiimseid tulemusi.

---

[67] Kui Hartmani kaitsja seadis kahtluse alla ning soovis uurida tarkvara, mille abil tema klient tabati, siis leidis prokuratuur, et nad ei saa avalikustada kõnealuse tarkvara omadusi ja võimekust. Taoline avalikustamine võib vähendada tarkvara efektiivsust järgnevates menetlustes, kuna avalikuks tuleb see, kuidas tarkvara töötab. Eelnev aga omakorda tingib, et kurjategijad võivad leida erinevaid mooduseid, kuidas ennast tarkvara eest varjata. Prokuratuur loobus juhtumiga tegelemisest, kuigi Hartmanile kuuluvast arvutist leiti lapspornograafiat.

[68] Gillum, J. Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned. ProPublica, 2019. Arvutivõrgus kättesaadav: https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned

[69] Stoykova, R. ,,Digital evidence: Unaddressed threats to fairness and the presumption of innocence" Computer Law & Security Review, Volume 42, 2021, lk 1.

[70] National Police Chiefs' Council ,,Digital Forensic Science Strategy" 2020.Arvutivõrgus kättesaadav: https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf

Antud problemaatikat on analüüsinud ka digitaalkriminalistika ekspert Eoghan Casey, kes on viidanud asjaolule, et kuna digitaalsete tõendite ja digitaalkriminalistika osas puudub ühine hindamine, on keeruline hinnata tõendite usaldusväärsust. Ta on loetlenud ka erinevaid probleeme, mis võivad tekkida. Muuhulgas on kirjeldatud, et digitaalsete tõendite osas võib probleeme tekkida andmekaoga, üksikisikute poolt tõendite varjamise või võltsimisega, vigadega andmete analüüsimisel ning ajalise ebakindlusega sündmustiku osas. Et taolist kitsaskohta leevendada, pakub Casey välja lihtsa süsteemi. Nimelt ekspert peab hindama kui kõrge on tema leitud digitaalse tõendi usaldusväärsus. Eelnev aitab menetluses otsustajal hinnata tõendi relevantsust ja usaldusväärsust ning seeläbi muudab otsustamisprotsessi kergemaks ja ausamaks. [71]

Seega võib väita, et digitaalkriminalistikas ja seeläbi ka digitaalsetes tõendites võib esineda erinevaid ebatäpsuseid või vigu. Vead, mis võivad esineda, saab jaotada kahte suuremasse kategooriasse: tehnilised vead ja mitte-tehnilised vead. Tehnilised vead on pigem seotud digitaalkriminalistika meetodite ja tööriistadega. Mitte-tehnilised vead aga pigem inimliku eksimuse aspektiga. Mitte-tehniliste vigade kohta annab autor ülevaate järgnevas peatükis.

Tehnilisi vigasid saab omakorda jaotada kolmeks - tehniline viga, rakenduslik viga ning tööriista ebaõige kasutamise ja tõlgendamisega seotud viga. Tehniliste vigade all peetakse peamiselt silmas vigu, mis on seotud algortimidega. Tegemist on raskesti mõõdetava ja tuvastatava veaga ning pigem üksikjuhtumitega. Rakenduslikeks vigadeks võib lugeda ebatäielikkust, ebatäpsust ning väära tõlgendust. Ebatäielikkuse all mõeldakse eelkõige seda, et tööriist ei töötle kogu informatsiooni, mis on selle jaoks kättesaadav. Näiteks jätab tööriist tähelepanuta olulised failid või logiandmed. Ebatäpsust võib tõlgendada kui olukorda, kus tööriist annab infot aspektide kohta, kuid muudab informatsiooni selliselt, et muutub ka informatsiooni tähendus. Tõlgendamisega seotud veaks võib pidada olukorda, kus tööriist küll töötab korrektselt, kuid saadud tulemusi tõlgendatakse ebakorrektselt. Samuti olukorrad, kus kasutatakse tööriista valel eesmärgil. [72]

[71] Casey, E. „Error, Uncertainty and Loss in Digital Evidence.”International Journal of Digital Evidence, 2002, lk 41-42.
[72] Horsman, G. Sunde, N. „Part 1: The need for peer review in digital forensics”. Forensic Science International: Digital Investigation, Volume 35, 2020, lk 2-4.

Nagu igas teadusharus, on ka digitaalkriminalistikas võimalik eksida ja teha vigu. Siiski tuleb tõdeda, et ebaõige informatsiooni kasutamine võib viia äärmiselt negatiivsete tulemusteni. Euroopa Komisjoni hinnangul on digitaalseid tõendeid kasutada vaja umbes 85% kriminaalmenetluse juhtumitest.[73] Võttes arvesse, et tegemist on aina rohkem vajamineva tõendiliigiga, on potentsiaalsed probleemid usaldusväärsusega äärmiselt murettekitavad.

2.2 *Anti-forensics* ja digitaalsete tõendite võltsimine

Tõendite varjamine või hävitamine on temaatika, millest on kõik ilmselt kuulnud. Ka popkultuurist võib leida näiteid selle kohta, kuidas filmimaailmas üritatakse kuriteo toimepanemiseks kasutatud relvalt pühkida sõrmejälgi või kasutatakse kloori, et kaotada inkrimineerivaid vereplekke. Ka digitaalsete tõendite puhul on tegemist tõendiliigiga, mida üritatakse võltsida või kustutada, et varjata oma tegusid või suunata uurimisasutused hoopis valedele jälgedele. Võrreldes traditsiooniliste tõenditega, on digitaalseid tõendeid kergem muuta.[74]

Selleks, et digitaalkriminalistika eksperdid saaksid efektiivselt uurida digitaalseid tõendeid, on abiks mitmed kriminalistika tarkvarad ehk CFT-d (*computer forensic tools*). CFT-d aitavad ekspertidel koguda erinevat informatsiooni arvutisüsteemidest ning samuti aitavad need analüüsida teavet, et anda informatsiooni sellise teabe kohta, mis ei ole koheselt ilmne.[75] CFT-d on viimase kümnendi jooksul jõudsalt edasi arenenud ja nüüdisajal on neid juba väga palju. Tihti on iga spetsiifilise tõendi jaoks eraldi loodud tarkvara, mis keskendub just sellist tüüpi tõendi hindamisele ja analüüsimisele. Näiteks on loodud spetsiaalsed tarkvarad audio- ja videotõendite uurimise jaoks. [76]

Siiski tuleb tõdeda, et kiirelt ei arene mitte ainult CFT-d vaid ka erinevaid tarkvarad ja meetodid, mis on mõeldud just CFT-de vastu töötamiseks. Eelnevaid võib kokkuvõtlikult nimetada *anti-forensic* tööriistadeks. *Anti-forensic* tööriistade peamisteks eesmärkideks on

[73] European Commission. „FAQ: New EU rules to obtain electronic evidence" 2018. Arvutivõrgus kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
[74] Schneider, J. Wolf, J. Freiling, F. „Tampering with Digital Evidence is Hard: The Case of Main Memory Images" Forensic Science International: Digital Investigations, Volume 32, 2020, lk 51.
[75] Garfinkel, S.L. „Anti-forensics: Techniques, detection and countermeasures" 2015, lk 77.
[76] Mohammad, N. Fayyad-Kazan, H. Saab, M. „Anti-Forensics: The Tampering of Media" International Journal on Recent and Innovation Trends in Computing and Communication, 2020, lk 2-3.

eksitada eksperte, varjata mingi sündmuse juhtumist, segada informatsiooni kogumist ning ka seada kahtlusi tõendi usaldusväärsuse osas. Taolise tehnoloogia kiire areng on kaasa toonud igasuguse multimeedia manipulatsiooni võimalused. [77]

Anti-forensic tööriistasid on mitmeid ning nende profiil on võrdlemisi laiahaardeline. On spetsiaalsed tööriistad, mis on loodud just meta-andmete muutmiseks, samas ka tööriistasid, mille peamine eesmärk on rünnata CFT-des esinevaid vigu. Taoliste vigade ründamine võib aga kaasa tuua olukorra, kus CFT ei suuda korrektselt tuvastada informatsiooni. Samuti on olemas *anti-forensic* tööriistad, mis on suutelised muutma oma käitumist, kui tajuvad, et kasutatakse CFT-d.[78] Lisaks on tuvastatud juba erinevaid *anti-forensic* tarkvarasid, mis on võimelised ründama CFT tarkvarasid ning seeläbi halvama nende töö täielikult.

Mitmed CFT-d on läbinud kontrolli oma töökindluse ja usaldusväärsuse osas ning taoliste kontrollide tulemused avaldatakse avalikes teadusportaalides. Teadusportaalides avaldatu annab aga võimaluse tutvuda CFT-ga põhjalikumalt ning seega luua ka *anti-forensic* tööriista, mis oleks võimeline ründama just seda tüüpi CFT-d.[79] Kõik eelnev võib aga potentsiaalselt tekitada situatsiooni, kus ekspert saab *anti-forensic* tööriista poolt tugevalt manipuleeritud informatsiooni ning jõuab ka seetõttu ebaõigete järeldusteni. Samuti ei ole välistatud olukord, kus informatsioonist jäädakse täielikult ilma ning süüdlase vastu ei saa efektiivselt kasutada digitaalseid tõendeid, mis aitaks kaasa süüdimõistvale otsusele.

Mitmed *anti-forensic* tööriistad on loodud tarkvaraarendajate poolt, kelle eesmärk on olnud kontrollida just CFT-de usaldusväärsust. Üks taolistest arendajatest on Vincent Lui, kes on ka viidanud asjaolule, et digitaalsete tõendite täieliku usaldusväärsuse presumptsioon ei ole õigustatud. Tema hinnangul ei ole õigussüsteem piisavalt kriitiline selle osas, mida kasutatakse tõendina.[80] Seega saab järeldada, et *anti-forensic* tööriistade efektiivne kasutamine võib täielikult muuta tõendi väärtust, legitiimsust ning terviklikkust. Eelnev võib suunata CFT tarkvara valedele jälgedele ja luua vale kuvandi asjaoludest, mis omakorda mõjutavad ekspertide järeldusi.

[77] Samas, lk 2-3.
[78] Garfinkel, S.L. „Anti-forensics: Techniques, detection and countermeasures" 2015, lk 82.
[79] Mason, S. Seng, D. editors. *Electronic Evidence*. University of London Press, 2017, lk 334
[80] Samas, lk 333

Kuigi *anti-forensic* tööriistad on võrdlemisi levinud, ei tähenda see, et puuduksid ka lihtsamad meetodid eksitamiseks ja valedele jälgedele suunamiseks. Oluline on siiski märkida, et taolised lihtsamad meetodid ei pruugi teoorias nii efektiivsed olla.

Üks lihtsamaid viise digitaalsete tõendite abil eksitamiseks on tõendite sisu muutmine. Tegemist on mitmetel juhtudel võrdlemisi lihtsa protsessiga, mis ei pruugi vajada mingisuguseid eriteadmisi. Erinevaid katsed esitada kohtule võltsitud tõendeid on küll haruldane, kuid erialakirjanduses on jõutud seisukohale, et selliste katsete arv on suurenemas.[81]

Võttes arvesse, kui kerge on digitaalsete tõendite sisu muutmine või nendest lahti saamine, võib oletada, et tulevikus sageneb taolise meetodi kasutamine. Ei ole välistatud ka see, et inimesed ise üritavad luua fiktiivseid asitõendeid, mida nad saavad kohtule esitada. Eelnev ei ole piiratud ainult kriminaalmenetlustega, taolist käitumist võib kohata ka töövaidlustes. Ühe näitena võib tuua lahendi *Public Prosecutor v Rudy Lim.* Antud kaasuses võltsis Rudy Lim oma palgateatist, muutes igakuise palga 25 000 dollari asemel hoopis 65 000 dollariks. Eelneva teostamiseks kasutas Lim *Microsoft Office Word* programmi ning *Adobe* arvutitarkvara programmi. Lim muutis *Microsoft Office Word* programmis oma palgateatise numbrilisi näitajaid, kopeeris sinna oma tööandja logo ja oma ülemuse allkirja ning konverteeris dokumendi seejärel pdf. failiformaati. Lim mõisteti süüdi võltsimises ning talle määrati 2 kuud vanglakaristust. [82]

Mitmetes riikides on lubatud kasutada ka e-kirjade vahetust tõendina ning püstitatud on küsimusi ka sellise tõendusmaterjali autentsuse osas. Nimelt on kõne alla tulnud küsimus selle kohta, et kuidas tõendada, kes e-kirja tegelikkuses saatis. Kaasuses *Tassone v Kirkham* tekkis just taoline küsimus. Nimelt oli Hr. Tassone'i töö *e-maili* pealt laekunud kolleegidele e-kiri, mille sisu oli Tassone'i suhtes alandava sisuga.[83] E-kiri saadeti Tassone'i kontolt, sellel oli tema digitaalne allkiri ning kirja said üle 2000 kolleegi avalikus sektoris.[84] Kui situatsiooni lähemalt uurima hakati, selgus, et e-kirja oli saatnud Tassone'i kolleeg Hr. Kirkham, kes märkas, et Tassone oli oma arvuti juurest eemal, kuid oli siiski sisse logitud.

[81] Samas, lk 330
[82] Samas, lk 332
[83] Kirja sisu oli järgnev: „hello people, just a note to say that i am homosexual and i am looking for like minded people to share time with."
[84] *Tassone v Kirkham* (2014) SADC 134

Situatsioon kulmineerus kohtuotsusega, kus kohus leidis, et Tassone'ile on tekitatud mittevaralist kahju suuruses 75 000 dollarit. [85]

Samas on potentsiaalselt võimalik digitaalsete tõendite võltsimisega ennast välja arvata kahtlusaluste ringist. Üheks selliseks võimaluseks on luua võltsitud digitaalne *alibi*. On mitmeid juhtumeid, kus digitaalne *alibi* on aidanud inimestel tõendada oma süütust. Selline juhus oli näiteks Rodney Bradfordiga, kes oli kahtlusalune relvastatud röövis. Bradford lasti vabaks, kui tuvastati, et röövi toimumise ajal oli tema *Facebook*i kontol tegevust. Leiti, et Brafordil oli digitaalne *alibi*, mis tõestas, et tema ei saanud röövi toime panna. [86]

Võltsitud digitaalne *alibi* annaks võimaluse inimesel eksitada uurijaid ja eksperte arvama, et inimene ei saanud süütegu toime panna, kuna ta viibis süüteo toimepanemise momendil mujal. Võltsitud digitaalse *alibi* loomiseks on erinevaid võimalusi ning mitmed neist on võrdlemisi kergesti kasutatavad. Näiteks pakub sellist võimalust skriptikeel *AutoIt*, mis suudab luua automatsiooni programmi. Näiteks on võimalik eelnevaga simuleerida erinevate veebilehtede külastamist või avamist, simuleerida klahvivajutusi, simuleerida hiire kasutamist jne. Täielikult automatiseeritud programmi loomiseks on vaja võrdlemisi elementaarseid teadmisi *AutoIt* skriptikeelest.[87] Ehk võltsitud digitaalse *alibi* loomine ei ole välistatud ka inimeste puhul, kellel puuduvad vastavad erialateadmised, kuna tegemist ei ole liigselt keeruka ülesandega. Mitmed käsklused on Internetis ka vabalt leitavad, sh:

1) *("sequence-of-keys")* - Simuleeritud klahvivajutused.
2) *("mouse_button")* - Simuleeritud hiire liigutus või hiireklahvi vajutus.
3) *("path/to/external/program")* - Välise programmi käivitamine. [88]

Seega võib kõigest eelnevast järeldada, et tihti ei ole digitaalsete tõendite võltsimise osas alati vaja erilisi oskusi ja teadmisi. Mõnikord piisab lihtsalt mingi programmi tundmisest või võimaluse nägemisest. Ei ole välistatud, et ka mitmed inimesed üritavad eksitada digitaalsete tõenditega tegelevaid isikuid kasutades lihtsamaid meetmeid, mis on üldjuhul kergesti

[85] Stephen, M. Seng, D. „Electronic Evidence" University of London Press, 2017, lk 243
[86] De Santis, A. Castiglione, A. Cattaneo, G. De Maio, G. Ianulardo, M. „Automated Construction of a False Digital Alibi" 2011, lk 2-3.
[87] Samas, lk 8-9.
[88] Samas, lk 10.

tuvastatavad. Näiteks kuupäevadega manipuleerides üritatakse edastada ebaõiget või eksitavat informatsiooni.

On oluline seega järeldada, et eksisteerib erinevaid viise digitaalsete tõendite muutmiseks ja ekspertide ning muude isikute eksitamiseks. Kuigi paljude juhtumite puhul suudavad eksperdid ilmselt pettused tuvastada, on oluline taolistele võimalustele ja nende lihtsale kättesaadavusele siiski tähelepanu pöörata. Tähelepanu juhtimine erinevatele pahatahtlikele meetoditele suurendab autori hinnangul võimekust taolisi meetodeid efektiivsemalt tõrjuda ja tulevikus potentsiaalselt ka ära hoida.

2.3 Kasutajaga seonduvad vead

Eelnevas peatükis andis autor ülevaate erinevatest tehnilistest vigadest, mis võivad digitaalse ekspertiisi osas ette tulla ning moodustest ekspertide eksitamiseks. Teatavasti ei ole digitaalne ekspertiis täielikult automatiseeritud ning suure osa tööst peab siiski tegema ka inimene, kes antud juhtumiga tegeleb. Inimeste puhul ei ole aga tegemist perfektsete organismidega, kes kunagi ei eksi. Sestap tuleb järgnevalt tuleb analüüsida mitte-tehnilisi ehk inimlikke vigu, mis võivad ette tulla digitaalses ekspertiisis.

On selge, et selleks, et saavutada efektiivseid tulemusi, on vaja vastavaid teadmisi. Peab aga tõdema, et mitmetel erialadel võivad töötada eksperdid, kelle teadmised on puudulikud. Taolisi eksperte võib leida ka digitaalse ekspertiisi valdkonnast. Eksperdi teadmised mõjutavad tugevalt menetluse tulemit ning võivad kujundada suurel määral ka tõendite põhjal tehtud järeldusi. Üha kiiremini arenev digitaalmaailm tingib aga asjaolu, et eksperdil võib tekkida puudujääk teadmiste osas. Nimelt võib taoline kiire areng luua olukorra, kus ekspert seisab vastamisi täiesti tundmatu informatsiooni liigiga. Eelnev aga tõstatab küsimuse eksperdi enesekriitilise mõtlemise kohta - kuidas tagada, et ekspert mõistaks oma oskuste piiratust ja ei ületaks oma teadmiste valdkonna piire? On oluline, et digitaalse ekspertiisiga tegelev inimene on valmis tunnistama, et mingi probleem on tema jaoks liiga keeruline ja vajab seega kogenenuma isiku analüüsi.

Olukorras, kus ekspert on võimeline objektiivselt hindama oma oskusi antud juhtumi valguses, on võimalik ära hoida potentsiaalseid probleeme tõendite usaldusväärsusega ja ka

süütu inimese süüdi mõistmist. Eelnevat näitlikustab juhtum, mis leidis aset Ameerika Ühendriikides. Kohtuasi *State of Connecticut v. Julie Amero* on juhtum, millest on digitaalkriminalistikas saanud kurikuulus kaasus. Tegemist on vägagi olulise kaasusega, kuna antud juhtum näitlikustas, milleni võib inimlik viga viia kriminaalmenetluses. [89]

Nimelt töötas Julie Amero asendusõpetajana, kes andis tundi 7. klassi õpilastele. Õppetöö ajal hakkas arvuti näitama pornograafilise sisuga *pop-up* reklaame, mida nägid ka õpilased. Amerole esitati süüdistus alaealiste ohtu panemise eest ning süüdimõistva otsuse puhul, oleks Amerot võimalik karistada olnud kuni 40 aastase vanglakaristusega. Peamiseks asitõendiks antud kaasuses oli koolis kasutatava arvuti kõvaketas, millest oli tehtud koopia. Kõvaketta koopiaga loodeti tõendada, et arvuti brauseriajalugu näitab pornograafia lehekülgede külastust, mis viitab asjaolule, et Amero külastas taolisi lehti tahtlikult ja teadlikult.[90] Oluline on aga märkida, et arvuti kõvaketta kopeerimise osas oli küsitavaid asjaolusid ning samuti esines probleeme ajamärgistustega. Mõlemad probleemkohad oleksid pidanud tõstatama küsimuse digitaalsete tõendite usaldusväärsuse kohta, kuid neid aspekte ei võetud kohtus arvesse. [91]

Lisaks oli kohtuasjas tunnistajaks mitu eksperti, kelle poolt antud ütlused ei olnud asjakohased. Näiteks oli tunnistajaks Bob Hartz, kooli IT juht, kes andis mitmele küsimusele eksitavaid vastuseid. Hartzi käest küsiti, kas arvutis olev nuhkvara suudab genereerida pornograafilise sisu näitamist. Hartz ei olnud kindel, kas nuhkvara suudaks seda teha. Kui aga uuriti, kas taoliste pornograafiliste *pop-upide* konstantne tahtmatu näitamine on võimalik, vastas Hartz, et kuna tema ei ole taolist asja varem näinud, siis ilmselt ei ole see ka võimalik. Tegemist oli spekulatiivsete vastustega, mis ei peegeldanud tõde. Samuti ei kaalutletud absoluutselt eksperdi kogemuste ulatust ja legitiimsust.

Lisaks oli küsitav politseiametnik Lounsbury tunnistus (tegemist oli ametnikuga, kes kopeeris kõnealuse kõvaketta). Nimelt viitas tema tunnistus asjaolule, et politseinik oli ekspertiisi käigus uurinud kõvaketast originaalkujul, mitte selle koopiat. See ei ole aga tavapraktika, kuna kõvaketta otsene uurimine (s.h failide avamine) muudab failide originaalseisundit ja

[89] Endicott-Popovsky, A. E . „Digital Evidence Education in Schools of Law," Journal of Digital Forensics, Security and Law: Vol. 7, 2012, lk 76-80.
[90] On oluline märkida, et hiljem tuvastati, et kooli arvuti viirusetõrje oli aegunud, arvutil puudus tulemüür ning ka arvuti sisu kontrolliv filter oli aegunud.
[91] Samas, lk 76-80.

seega muudab ka asitõendeid ja nendes peegelduvat informatsiooni. Samuti tunnistas Lounsbury, et ta ei olnud isegi kontrollinud, kas kõvakettal oli infot, mis oleks viidanud pahavara, nuhkvara või viiruste olemasolule.

Tegelikkuses tuvastas erapooletu ekspert Herb Horner (kes uuris kõvaketta koopiat), et kõvakettal leidus nuhkvara, mis tekitas pornograafilise sisuga *pop-upe*, kuid kohus ei olnud nõus tema seisukohti kuulama. Horner on hiljem ka öelnud, et tegemist oli frustreeriva juhtumiga, kuna tõendid viitasid Julie Amero süütusele, kuid neid lihtsalt ei võetud arvesse.

Tegemist on juhtumiga, mis illustreerib, kui traagilised tagajärjed võivad olla eksperdi teadmatusel. Valed meetodid ja oma võimete ülehindamine viisid antud juhtumi puhul süüdimõistva otsuseni. Kui kõnealuses kaasuses oleksid tunnistajad viidanud asjaolule, et neil puuduvad vastavad oskused ja teadmised, ei oleks süütut Julie Amerot süüdi mõistetud ning pädev ekspert oleks tuvastanud *pop-upide* tegeliku allika.[92]

Eelnev kaasus illustreerib kui olulised on eksperdi erialased teadmised digitaalkriminalistikas ning milliste tulemusteni võib viia oma võimete ebaadekvaatne hindamine. Eelnevalt on töös viidatud Eoghan Casey seisukohale, et digitaalkriminalistika ekspert peab olema suuteline hindama oma järelduste tõenäosust. Kui ekspert suudab anda teavet selle kohta, kui tõenäolised või ebatõenäolised on tema järeldused, on autori hinnangul võimalik adekvaatsemalt kaaluda tõendi usaldusväärsust.

Samas ei ole Euroopa Liidus otseselt määratletud, millise haridusliku taustaga peab olema digitaalse ekspertiisi ekspert. Üldine konsensus on see, et eksperdil võiks olla infotehnoloogia, matemaatika või inseneriteaduse kõrgharidus ning digitaalkriminalistika sertifikaat ja 2 aastat kogemust digitaalkriminalistikas. Kui kõrgharidus puudub, võiks eksperdil olla vähemalt 5 aastat kogemust digitaalkriminalistikas ning erinevad sertifikaadid tõendamaks digitaalkriminalistika oskusi.[93] Analoogne seis on ka Norras. Nimelt on Norra Politsei Direktoraat selgitanud, et kriminaalmenetluses peaks digitaalsete tõenditega tegelema

[92] Samas, lk 76-80.
[93] Laptev, P. „Digital Forensics view from the Estonian Forensic Science Institute" Estonian Forensic Science Institute. Cybercrime forensics & digital evidence, 11/2014.

vaid adekvaatse õppega ja vastava kompetentsiga inimesed, kuid ei ole selgitatud, mida need terminid praktikas tähendavad.[94]

Ühtsed reeglid ekspertide haridustaseme osas on olulised, et saavutada ekspertide seas ühtlaselt kõrge kvaliteet. Teatavasti on rohkem kui pooltes kriminaalmenetlustes ka välismaine element, mis eeldab koostööd piiriüleste uurimisasutustega.[95] Kui aga reguleerida ekspertide haridustaseme nõudeid Euroopa Liidu tasandil, võib autori hinnangul tugevalt parandada ekspertide oskusi ja omavahelist koostööd menetlustes, mis nõuavad rahvusvahelist suhtlust. Lisaks kõigele eelnevale, võiks ekspertide taset testida rutiinsete tasemetestidega. SIRIUS projekti [96] 2019. aasta raporti hinnangul on üheks probleemiks digitaalsete tõendite teenusepakkujatelt kättesaamise puhul just uurimisasutuste ebakompetentsus. Probleeme on mitmeid - uurimisasutuse töötajate tehnilised teadmised ei ole piisavalt head ning seetõttu ei suudeta oma nõudmisi piisavalt konkretiseerida. Samuti esineb takistusi keelebarjääriga.[97]

Digitaalsete tõenditega tegelevad eksperdid on, sarnaselt teiste elukutsete esindajatele, võimelised eksima. Erialakirjanduses tuuakse välja mõned murekohad, mis võivad tekitada vigu ekspertarvamuste osas. Esmalt suunatakse tähelepanu ekspertide teadmistele. Juba eelnevalt on töös konstateeritud asjaolu, et tehnoloogia kiire levik võib kaasa tuua situatsiooni, kus ekspert puutub kokku millegagi, mida ta varem näinud ei ole. Taolisele probleemile viitavad ka Graeme Horsman ja Nina Sunde. Ka nemad viitavad asjaolule, et on oluline, et ekspert teaks oma piire ning ei ületaks neid. Positiivse aspektina tuuakse aga välja asjaolu, et mitmete ekspertide laialdased kogemused aitavad neil tulevikus edukalt tuvastada potentsiaalseid vigu ja nendest hoiduda. [98]

Lisaks viitavad autorid protseduurilistele puudujääkidele. Nimelt on olemas suurel hulgal erinevaid põhimõtteid, mida tuleb järgida digitaalkriminalistikas - näiteks *digital chain of*

[94] Sunde, N. „Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation", 2017, lk 104.
[95] Europol „SIRIUS Project" Külastatud: 06.04.2022. Arvutivõrgus kättesaadav: https://www.europol.europa.eu/operations-services-innovation/sirius-project
[96] SIRIUS projekt on Europoli, Eurojusti ja Euroopa Õigusalase Võrgustiku koostoimes rakendatud projekt, mille eesmärgiks on teadmiste jagamine digitaalsete tõendite kohta.
[97] Europol. „SIRIUS: EU Digital Evidence Situation Report 2nd Annual Report". 2020. Külastatud: 06.04.2022. Arvutivõrgus kättesaadav: https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/SIRIUS_REPORT_20.pdf
[98] Horsman, G. Sunde, N. Part 1: The need for peer review in digital forensics, Forensic Science International: Digital Investigation, Volume 35, 2020, lk 4-5.

custody ja asitõendite originaalformaadi säilitamine. Kuigi printsiipe on mitmeid ja erinevaid, ei anna need erilist infot selle kohta, millised peaksid olema digitaalkriminalistikas rakendatavad protseduurilised reeglid. Puuduvad ettekirjutused selle kohta, et kuidas uurimisprotsessi kui sellist läbi viia. Protseduurilised reeglid võivad aga tugevalt kaasa aidata uurimise efektiivsusele ja kvaliteedile. Nimelt viitavad autorid asjaolule, et taoliste protseduuriliste reeglite ning kontrollnimekirjade olemasolu võiks olulisel määral aidata potentsiaalseid vigu vähendada. [99]

Eelnevat asjaolu kinnitavad ka uuringud, mis on lähedast temaatikat analüüsinud. Uuringud on tehtud küll meditsiinivaldkonnas, kuid siiski võib saadud tulemusi rakendada ka teiste valdkondade osas. Uuringu käigus tutvustati meditsiini valdkonna spetsialistidele kontrollnimekirja, milles olid välja toodud erinevad sammud, mis peaksid minimaliseerima infektsioonide teket (nt käte pesemine, naha desinfitseerimine jne). Taolise kontrollnimekirja kasutamine viis väga heade tulemusteni, kuna infektsioonide määr langes peaaegu olematu määrani. [100]

Taoliste ühtsete protseduuriliste reeglite ja kontrollnimekirjad lisamine digitaalekspertiisi maailma ei tähenda, et eksperdid ja muud selle temaatikaga tegelevad inimesed oleksid ebapädevad või vajaksid juhendeid tegutsemiseks. Kindel reeglistik ja kontrollnimekirjad aitaksid ekspertidel kõigest paremini meeles pidada pisemaid tööülesandeid, mille tegemise vajadusest on nad teadlikud, kuid mis võivad töö käigus tahtmatult ununeda. Meditsiini valdkonna spetsialistid on samuti teadlikud käte pesemise vajadusest ja naha desinfitseerimise nõudest, kuid taolise pisidetailid on altid töö käigus ununema.[101] Autori hinnangul aitaksid taolised kontrollnimekirjad ning reeglistikud unustamisi minimaliseerida ning seeläbi vähendada ka potentsiaalseid vigu, mis ekspertide töös võivad ette tulla.

Kuigi digitaalkriminalistikas ei ole loodud ühtset käitumiseeskirja, on olemas mitmete erinevate riikide eeskirju, mida tihti kasutatakse „hea tava" näitlikustamiseks. Neist üks enim tuntud on Inglismaa, Wales'i ja Põhja-Iirimaa koostöö tulemusena loodud Association of Chief Police Officers' *Good Practice Guides for Digital Evidence.*[102] Tegemist ühe enim viidatud juhisega digitaalkriminalistikas, mis sisaldab digitaalkriminalistika n-ö

[99] Samas, lk 3-4.
[100] Samas, lk 3-4.
[101] Samas, lk 3-4.
[102] Tuntud kui ka ACPO Guidelines või ACPO Principles.

põhiprintsiipe. Juhis koosneb erinevatest soovitustest digitaalkriminalistika valdkonnaga tegelevatele inimestele. Ka selle, laialdaselt tuntud, juhise suunas on erialakirjanduses väljendatud kriitikat, kuna juhist ei ole uuendatud aastast 2012. Tehnoloogia kiire arengu ja uute meetodite tõttu leitakse aga, et juhendi uuendamine oleks hea idee. [103]

Autori hinnangul aitaksid ühised eeskirjad ühtlustada menetlusi üle maailma ja seeläbi edendada rahvusvahelist koostööd erinevate õiguskaitseorganite vahel. Kui õiguskaitseorganitel oleks ühine praktika, suureneks tõenäosus, et ka piiriülene koostöö sujuks paremini, kuna arusaam erinevatest digitaalkriminalistilistest probleemidest on erinevate riikide õigusorganitel sama.

Käesolevas magistritöös on eelnevalt juhitud tähelepanu asjaolule, et rahvusvahelises koostöös võib esineda mitmeid probleeme. Digitaalse ekspertiisi ja digitaalsete tõendite kogumise efektiivsust aitaks aga parandada laialdane teadmiste jagamine erinevate riikide korrakaitseorganite vahel. Erialakirjanduses on rahvusvahelise teadmiste jagamise võimalust palju soovitatud. Ühe murekohana tuuakse välja asjaolu, et tehnoloogia ja erinevate tarkvarade kiire kasv tähendab, et leidub eksperte, kes ei ole kokku puutunud mitmete erinevate katsumustega, mis esinevad digitaalse ekspertiisi valdkonnas. [104]

Erinevate teadmiste ja meetodite jagamine võib endaga kaasa tuua erinevaid positiivseid asjaolusid. Esiteks suurendaks see erinevate digitaalkriminalistika ekspertide teadmisi ning oskusi. Teiseks võib välja tuua kvaliteedi paranemise. Kui omavahel jagada erinevaid meetodeid, siis suureneb ka inimeste hulk, kes selliseid meetodeid katsetavad. Nii on võimalik leida ning elimineerida erinevaid vigu, mis võivad esineda. Samuti saavad eksperdid praktikas kinnitada, kas valitud meetod on reaalselt efektiivne.[105] Digitaalkriminalistikas töötatakse ühise eesmärgi nimel ning tuleb tõdeda, et efektiivne koostöö aitab seda ühist eesmärki paremini saavutada.

Samuti tuleb potentsiaalse inimliku veana analüüsida ka eksperdi pädevust. Digitaalse ekspertiisi ekspertide, politseinike ja muude antud temaatikaga tegelevate inimeste pädevus

[103] Horsman, G „ACPO principles for digital evidence: Time for an update?" Forensic Science International: Reports. Volume 2, 2020, lk 2-3.
[104] Horsman, G „Part 2:- quality assurance mechanisms for digital forensic investigations: Knowledge sharing and the Capsule of Digital Evidence (CODE)" Forensic Science International: Reports. Volume 2, 2020, lk 1.
[105] Samas, lk 2.

on teatavasti oluline menetluse kvaliteedi seisukohast. Välismaailmast võib juba leida juhtumeid, kus menetlus on tõsiselt kannatada saanud just üldise ebapädevuse tõttu. Näiteks võib leida mitmeid juhtumeid, kus menetlus on jäänud pooleli ametnike ebapädevuse tõttu.[106] Samuti võib leida juhtumeid, kus menetluse hilises järgus avastatakse digitaalseid tõendeid, mis viitavad hoopis süüdistatava süütusele.

Ühendkuningriikides leidis aset juhtum, kus noort meest süüdistati naise vägistamises ning talle esitati vastav süüdistus. Nimelt oli naine väitnud, et mees vägistas ta, hoidis teda oma korteris kinni ning naine sai politseisse pöörduda alles siis kui mees magama jäi. Süüdistatav eitas pidevalt oma süüd ning väitis, et tegemist ei olnud vägistamisega. Politsei uuris mehe telefoni ning tuvastas, et peale sõnumite mehe ja naise vahel, ei olnud telefonis midagi, mis oleks menetluse seisukohalt oluline. Kui politsei mehele telefoni tagastas, saatis mehe advokaat telefoni edasi iseseisva digitaalse ekspertiisi eksperdi juurde, kes avastas, et telefonis olid mitmed pildid süüdistatavast ja naisest koos. Fotodelt oli näha süüdistatavat ja naist embamas. Fototõendid läksid aga vastuollu prokuratuuri versiooniga ning kohtuasi lõpetati.[107]

Digitaalsete tõendite ja digitaalkriminalistika valdkonnas töötavate isikute pädevust mõjutavad mitmed erinevad faktorid. Tihti võib olla probleem hariduses, väheses kogemuses või isegi alarahastuses. Ühe võrdlemisi suure probleemina võib välja tuua ka digitaalsete tõendite rohkuse. Erinevate seadmete hulk ja mälumaht on tõusuteel ning see tähendab, et läbi töötatava materjali hulk on juba suurenenud ning ilmselt suureneb tulevikus veelgi. Digitaalse luurega tegelev Iisraeli ettevõte Cellebrite on 2021. aastal läbi viinud uuringu, milles analüüsiti erinevaid digitaalkriminalistika probleeme. Uuringus osales üle 2000 inimese (sh politseinikud, riigitöötajad, militaartöötajad, agentuuride juhtivtöötajad) 117 erinevast riigist. Raporti tulemused viitavad mitmele erinevale probleemile. Nimelt nõustub suurem osa uurijatest väitega, et digitaalsete tõendite analüüs on liiga keeruline ning pooled

[106] The Guardian. Dodd, V. „MET to review all ongoing rape cases after second trial collapses" 19.12.2017. Arvutivõrgus kättesaadav: https://www.theguardian.com/uk-news/2017/dec/19/met-to-review-all-ongoing-cases-after-second-trial-collapses

[107] The Guardian. Bowcott, O. „London rape trial collapses after phone images undermine case" 15.01.2018. Arvutivõrgus kättesaadav: https://www.theguardian.com/law/2018/jan/15/london-rape-trial-collapses-after-phone-images-undermine-case

agentuuride juhtkonnast vastanutest leiavad, et nende töötajad ei ole piisavalt koolitatud selleks, et rinda pista digitaalsete tõendite poolt tekitatud väljakutsetega. [108]

Uuringu kokkuvõttes on välja toodud järgnev: „*Enamikel õiguskaitset teostavatel asutustel puuduvad endiselt piisavad infotehnoloogia alased teadmised uute digitaalsete tehnoloogiate juurutamiseks ja kasutuselevõtmiseks, et kiirendada digitaalsete tõendite kogumise, analüüsimise, säilitamise, haldamise ja jagamise protsessi. Uurijatel puudub ka koolitus selliste vahendite tõhusaks kasutamiseks.*"

Seega võib ühe ebapädevuse põhjusena välja tuua puudulikud teadmised. Sama on kinnitanud ka Suurbritannias töötav ekspert Dr. Jan Collie. Dr. Collie viitab asjaolule, et politseil ei ole tihti piisavalt raha, et töötajaid erinevatele koolitustele saata. Eelnev asjaolu on viinud aga olukorrani, kus politseinikud on kogemata ära rikkunud digitaalsed tõendid. Samuti on ette tulnud olukordi, kus tavapolitseinikel on vaja tõlgendada saadud informatsiooni, kuid sellise tegevuse jaoks ei ole neil vastavat haridust.[109] Vale tõlgendus võib aga viia täiesti vale järelduseni, mis kriminaalmenetluses võib viia drastiliste tagajärgedeni.

Suure andmemahu analüüsimise korral on oluline positsioon teatavasti töötajatel, kes kogu selle töö läbi peavad viima. Cellebrite'i uuringust selgus aga, et umbes 28% töötajatest, kes tegelevad digitaalsete tõenditega, teevad ületunde. Kuid ainult 6% vastanutest lubavad palgata juurde uusi eksperte. Eelnev võib aga tähendada, et suure tõendite hulgaga ei suudeta lihtsalt toime tulla, kuna puudub piisavalt töötajaid, kes suudaksid kõiki tõendeid analüüsida. Samas on problemaatiline ka rahastuse temaatika, kuna uute ekspertide juurde palkamine on Cellebrite'i uuringu näitel võrdlemisi ebatõenäoline. Kuid ka olemasolevate ekspertide ületöötamine võib pikemas perspektiivis viia vigadeni, mis on tingitud väsimusest. Ka Dr. Collie on viidanud asjaolule, et tõendite hulk on tõesti suur, kuid alarahastuse tõttu ei ole politseiametnikel piisavalt aega, et kõiki erinevaid tõendeid läbi uurida. [110] Seega võib järeldada, et tõendite liigselt suur koorem vajab rohkemate inimeste kaasamist uurimisprotsessi.

---

[108] Cellebrite. „2021 Digital Intelligence Benchmark Report". Arvutivõrgus kättesaadav: https://cellebrite.com/en/digital-intelligence-benchmark-report-2021/

[109] The Guardian. Bowcott, O. „Police mishandling digital evidence, forensic experts warn." Arvutivõrgus kättesaadav: https://amp.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn

[110] Samas

Kõiki eelnevaid asjaolusid arvesse võttes, võib väita, et eksisteerib erinevaid faktoreid, mis võivad mõjutada uurimise kvaliteeti. Teadmiste ja meetodite jagamine ning kindla reeglistiku seadmine võib tunduvalt vähendada erinevaid inimlikke vigu, mis esinevad digitaalses ekspertiisis ja seega ka tõsta tõendite kogumise ning uurimise kvaliteeti.

Samas alarahastus, töötajate puudujääk ning vähene koolitamine võib suurendada erinevaid vigu, mis menetluses tehakse ning resulteerida erinevate negatiivsete tagajärgedega - sealhulgas menetluse luhtumine ning alusetu karistamisega süüdimõistva otsuse puhul. Autor leiab, et on oluline rohkem tähelepanu juhtida teadmiste jagamisele ning ekspertide pidevale koolitamisele ning adekvaatsele rahastusele. Digitaalsete tõendite hulk on aina suurenemas ning on oluline, et olemas oleks piisavalt eksperte, kes jõuavad ja oskavad taolise suurenemisega kaasas käia.

2.4 Eelarvamused digitaalsete tõendite hindamisel

On selge, et kohtunikelt nõutakse, et nad suhtuvad oma töösse täielikult eelarvamusteta, kuna ainult nii saab kohtunik hinnata tõendeid tervikuna ning teha otsuse, mis on tema hinnangul kõige õiglasem. Loomulikult eeldatakse sellist eelarvamusteta suhtumist ka ekspertide puhul, kes tegelevad tõendite analüüsimisega, sh ka traditsiooniliste tõendite analüüsiga. Siiski võib raske olla täielikult erapooletu.

Nimelt on väliskirjanduses viidatud võimalusele, et tõendite uurimisega tegelevad isikud on ebaõigeid järeldusi teinud oma eelarvamuste tõttu. Eelnevat väidet toetab empiiriline uuring, mis viitab, et mõndades ekspertiisi valdkondades võivad eksperdid jõuda erinevate tulemusteni ka siis, kui neile on esitatud identsed tõendid erinevates kontekstides. Näiteks ekspertiisi tulemust mõjutab asjaolu, et ekspert usub, et kahtlusalune on üles tunnistanud või ekspert usub, et kahtlusalune on süüdi.[111]

Paratamatult tekib küsimus, kas taolised eelarvamused kanduvad üle ka digitaalkriminalistika maailma, kus mitmed eksperdid peavad tegelema erinevate digitaalsete tõendite uurimisega. Empiirilise uurimuse näites oli just kontekst see, mis mõjutas eksperdi hinnangut.

[111] Dror, I.E, Hampikian, G. „Subjectivity and bias in forensic DNA mixture interpretation" Science and Justice 51, 2011, lk 204.

Digitaalsete tõendite kogumisel on aga kokkupuude suure hulga informatsiooniga inimese eraelu kohta. Näiteks mobiiltelefoni läbiotsimisel võib ekspert saada telefoni omaniku kohta rohkem informatsiooni kui menetluse tarbeks vaja on. Autori hinnangul võib taoline lisainformatsioon tekitada aga eksperdile inimesest kuvandi. Taolise kuvandi loomine võib aga omakorda mõjutada eksperdi objektiivset tõlgendust tõendite osas.

Erinevad uuringud viitavad asjaolule, et ekspertiisis tuleb ette vigu, mis on mõnikord tingitud eksperdi eelarvamusest.[112] Taoline eelarvamus mõjutab aga ekspertiisi tulemusi ning eelnevaga võib kaasneda alusetu süüdimõistmine. Näiteks Brandon L. Garrett ning Paul J. Neufeld avaldasid 2009. aastal uuringu, milles nad uurisid 137 erinevat juhtumit, kus süütud inimesed on süüdi mõistetud võrdlemisi raskete kuritegude eest (sh näiteks vägistamine, mõrv) ning hiljem õigeks mõistetud tänu süüdimõistmise järgsele DNA ekspertiisile. Autorid tuvastasid, et 60% juhtumite puhul oli kohtuekspertiisi tulemused just need, mis viisid alusetu süüdimõistva otsuseni.[113] Samuti on leitud, et isegi erinevad seaduserikkujate stereotüübid võivad mõjutada kohtuekspertiisi analüüsi tulemusi. [114]

Taolisi juhtumeid, mis on seotud ekspertiisi teostava eksperdi eelarvamustega, on täheldatud erinevates ekspertiisi valdkondades ning mitmetes erinevates riikides. Näiteks on antud temaatikat täheldatud verepritsmete analüüsis, patoloogias, süütamiste uurimisel ning sündmuskohtade analüüsimisel.[115] Lisaks on Ameerika Ühendriikide, Austraalia, Inglismaa ning Wales'i põhjal tehtud alusetute süüdimõistvate kohtuotsuste hinnangutest teada, et umbes 23%-60% juhtumites võis leida „liialdatud" või vigaseid kohtuekspertiisi tulemusi. Just sellised tulemused on need tõendid, mis mängisid suurt rolli süütute inimeste süüdi mõistmisel. [116]

Erialakirjanduses viidatakse asjaolule, et tihti peetakse õiguse kogukonnas digitaalseid tõendeid usaldusväärseks ning õigeks.[117] Autori hinnangul võib taolise hinnangu põhjuseks

---

[112] Inglise keeles *bias.*
[113] Garrett, B.L, Neufeld, P.J. „Invalid Forensic Science Testimony and Wrongful Convictions" Virginia Law Review, 2009, lk 9.
[114] Smalarz, L. Madon, S. Yang, Y. Guyll, M. Buck, S. „The perfect match: do criminal stereotypes bias forensic evidence analysis?" Law and Human Behaviour, 40, 2016, lk 8.
[115] Sunde, N, Dror, I.E. „Cognitive and human factors in digital forensics: Problems, challenges, and the way forward" Digital Investigation Volume 29, 2019, lk 102.
[116] Samas, lk 101-102.
[117] Van Buskirk, E. Liu, V.T „Digital evidence: challenging the presumption of reliability" Journal of Digital Forensic Practice, 2006, lk 19.

olla veendumus, et arvutid ei eksi ja annavad alati tõepärast informatsiooni. Kuid tegelikkuses viitavad erinevad uuringud asjaolule, et taolised eelarvamused eksisteerivad ka digitaalsete tõendite ekspertiisi valdkonnas. 2018. aastal avaldatud uuringus analüüsiti 235-te erinevat Suurbritannia apellatsioonikohtus tühistatud süüdimõistvat otsust ning leiti, et ekspertiisitõendid (sh digitaalsed tõendid) olid probleemkohaks 32% juhtumite puhul. Uuringus tuvastati 4 erinevat juhtumit, kus digitaalsed tõendid olid just need asitõendid, mis andsid ebaõiget informatsiooni.[118]

Lisaks eelnevale tuvastas üks uuring, et on tavapärane praktika anda digitaalse ekspertiisiga tegelevatele isikutele uuritava juhtumi konteksti kohta informatsiooni ning mingi osa sellest informatsioonist ei pruugi tööülesande seisukohalt olla relevantne. Ebarelevantne kontekstuaalne informatsioon võib aga tekitada eksperdil eelarvamusi, mis omakorda mõjutavad digitaalsetele tõenditele objektiivse hinnangu andmist.[119]

Eelnevat väidet võib näitlikustada uuringus välja toodud asjaoluga, et kui ekspertiisi teostavale inimesele anda informatsiooni, mis viitab kahtlusaluse süütusele, siis võib ekspert leida uuritavast objektist vähem jälgi ning seega on tal ka vähem selgitusi selle kohta, milline võis teo sündmustik tema hinnangul olla. Kui aga ekspertiisi teostav inimene usub, et kahtlusalune on süüdi, leiab ekspertiisi teostav inimene uuritavas objektis rohkem jälgi ning rohkem põhjendusi. [120]

Erialakirjanduses viidatakse veel asjaolule, et taolist ebavajalikku infot on digitaalsete tõendite osas rohkem kui näiteks sõrmejälgede või tulirelvade analüüsis. Nimelt toob digitaalsete tõendite ekspertiis kaasa rohkem konteksti. Eelnevat saab näitlikustada lihtsa näitega. Kui ekspert uurib sõrmejälgi, on tal vaja väga limiteeritud informatsiooni sõrmejälgede paiknemise kohta, nende kogumise kohta jne. Digitaalsete tõendite otsimise puhul on seisukord veidi erinev ning ekspert saab kaasa suuremal määral kontekstuaalset informatsiooni, et oma tööd efektiivsemalt teha. [121]

---

[118] Smit, N.M, Morgan, R.M, Lagnado, D.A ,,A systematic analysis of misleading evidence in unsafe rulings in England and Wales" Science & Justice, Volume 58, 2018, lk 128.
[119] Sunde, N. Dror, I.E. ,,A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making" Forensic Science International: Digital Investigation, Volume 37, 2021, lk 9.
[120] Samas, lk 6-7.
[121] Sunde, N, Dror, I.E. ,,Cognitive and human factors in digital forensics: Problems, challenges, and the way forward" Digital Investigation Volume 29, 2019, lk 102.

Kokkuvõtvalt võib väita, et erinevad uuringud viitavad asjaolule, et inimeste puhul, kes tegelevad kohtuekspertiisiga, mis nõuab teatud määral subjektiivsust, tõlgendamist või avalduse arvamist, võib täheldada eelarvamusi. Võttes arvesse erinevaid uuringuid, inimloomust ning asjaolu, et ka digitaalne ekspertiis nõuab tihti eksperdilt tulemuste tõlgendamist, ei saa välistada, et eelarvamusi eksisteerib ka digitaalse kohtuekspertiisi valdkonnas.

3. Digitaalsete tõenditega tegelevate inimeste kogemused

Selleks, et paremini mõista digitaalsete tõendite kasutamist ja murekohti, mis võivad töös ette tulla, viidi käesoleva magistritöö raames läbi intervjuud 7 inimesega, kes antud temaatikaga oma tööalases elus palju kokku puutuvad. Intervjuu koosnes 20-st erinevast küsimusest, mis keskendusid digitaalsetele tõenditele ja nende problemaatikale. Autori eesmärgiks oli uurida, kas küsitlevate ringis leidus inimesi, kellel oleks digitaalsete tõenditega kokkupuutel tekkinud taolisi probleeme, mis autor on oma töös kirjeldanud.

Kõikidele vastanutele esitati täpselt samasugused küsimused ning vastanute ringis oli erinevate elukutsete esindajaid, sh abiprokurör, prokurör, kohtunik ning advokaat. Tulenevalt COVID-19 viiruse poolt tekitatud pandeemiast, viidi intervjuusid läbi nii *e-maili* teel kui ka kasutades *Zoom* programmi. Järgnevalt annab autor ülevaate läbi viidud intervjuudest ning nende järeldustest. Peatüki keskel antakse üldine ülevaade järeldustest, mis selgusid intervjuusid läbi viies. Peatüki lõpus annab autor ülevaate digitaalsete tõendite ja digitaalse ekspertiisi tulevikust.

3.1 Intervjuud

3.1.1 Intervjuu #1

Esimeseks intervjueeritavaks on abiprokurör, kes on vastaval ametikohal töötanud natukene alla nelja aasta, millest peaaegu 2 aastat on ta juhtinud kohtueelset menetlust ja esindanud prokuratuuri küberkuritegusid puudutavates kriminaalasjades. Intervjueeritaval on digitaalsete tõenditega suurel määral kokkupuuteid. Nimelt on tema töös ette tulnud erinevate digitaalsete tõendite kogumist ja vormistamist. Tema töös on kohtule esitatud muuhulgas erinevate serverite vaatluseid, võrguliiklust ja sagedust, kasutajakontode aktiivsuslogisid, krüptovaluutaga seonduvate tehingute kandeid, ID-kaardi sertifikaatide analüüse, õngitsusdomeenide ja võltsveebilehtede ülesehitusi, avalikult internetist kättesaadavat infot (nt kasutaja tegevused ja kättesaadavad andmed sotsiaalmeediast, blogidest jms), koopiaid erinevatest andmekandjatest (arvutid, nutiseadmed jne). Enim kasutatab ta oma töös aga koopiaid erinevatest andmekandjatest või -kogudest, kontode aktiivsuslogisid ning avalikult kättesaadavaid andmeid.

Kui aga intervjueeritava käest uurida, kuidas töö käigus tuvastatakse digitaalse tõendi objektiivsust ning usaldusväärsust, annab intervjueeritav vägagi sisutiheda ning informatiivse vastuse. Nimelt viitab intervjueeritav asjaolule, et digitaalse tõendi objektiivsuse ja usaldusväärsuse tuvastamine sõltub kogutava tõendi või kuriteojälje sisust, kuid põhiprintsiibid sarnanevad teiste tõendite usaldusväärsuse hindamisega. Intervjueeritav toob ka näite läbiotsimisest. Nimelt menetlejatelt nõutakse, et tõendi avastamine, fikseerimine, võtmine või kogumine ning analüüs oleks nõuetekohaselt dokumenteeritud. [122] Selle mõte on minevikku vaatavalt näidata kõiki nimetatud tõendi käitlemist hõlmavaid tegevusi, sest juristid (prokurörid, advokaadid, kohtunikud) enamasti ise ei kogu vahetult tõendit. Hiljemalt aga kohtus peavad menetluspooltel olema nn ,,võrdsed relvad'', kuidas veenda kohut tõendi usaldusväärsuses või seda testida. Nõnda peab olema võimalik näidata, et kohtu ette jõuab täpselt selle sama leitud ja ära võetud andmekandja ning seda pole vahepeal manipuleeritud. Kehtiva normistiku kohaselt on kahtlustatava valdusest leitud seade, mida ta kasutas kuriteo toimepanemiseks, originaaliks, mida hoitakse uurimisasutuse valduses kuni jõustunud kohtuotsuseni. Menetlejad ei analüüsi originaale, vaid tagatakse selle puutumatus ja terviklikkus, et vaidluse korral oleks võimalik avada sisu uuesti. Analüüsiks või ka vaatlemiseks tuleb teha seadmest koopia. Kõik sammud tuleb dokumenteerida.

Edasine analüüs, mida tehakse erinevate tarkvaraliste[123] lahendustega, peab välja selgitama, kas andmekandjal jne on kustutatud faile, kas faili atribuute ja meta-andmeid (nt ajatemplid, laiendid, autor, asukoht jne) on muudetud jne, st kas tõendit on manipuleeritud. See kõik sõltub sellest, mida on seadmest vaja tuua esile, st mis on kriminaalasja jaoks oluline. Eelnevale lisaks on ka teisigi võtteid – meta-andmete vaatamine, URL-i kontrollimine ja fikseerimine, veebitõmmise tegemise kuupäeva ja asukoha fikseerimine, digitõendi kõrvutamine teiste tõenditega jpt. Samuti on olemas, isegi internetist vabalt saadaval, erinevad tarkvaralised lahendused steganograafia[124] tuvastamiseks, kuid seda ei ole praktikas ette tulnud. Nende tarkvaraliste lahenduste mõte on kontrollida konkreetses failis tehtud bittide ja baitide muudatusi või anomaaliat, st ega nende sisse pole midagi peidetud.

---

[122] Intervjueeritav lisab, et Ameerika Ühendriikide õiguspraktikas on selle nimi *chain of custody*.
[123] Tegemist on erinevate digitaalkriminalistika tarkvaradega.
[124] Steganograafia näol on tegemist sõnumi peitmisega mingi digitaalse objekti sisse - näiteks pildi, video või heliklipi sisse. Vt täpsemalt: Mason, S. Seng, D. editors. *Electronic Evidence*. University of London Press, 2017, lk 333

Intervjueeritav lisab, et erandiks saab tuua õigusabitaotluse või Euroopa uurimismääruse alusel kogutud digitõendeid. Nimelt taolistel juhtudel kogub välisriik digitõendi originaali vastavalt enda riigis kehtivatele õigusaktidele ning prokuratuuril puudub sageli võimalus hinnata, kuidas see tõend avastati, fikseeriti, võeti ja mida on sellega veel vahepeal tehtud. Lähtutakse täitjariigi antavast autentsusgarantiist, mis tuleb sõltuvalt olukorrast õigusabilepingust või Euroopa uurimismääruse direktiivist.

Intervjueeritav peab aga digitaalseid tõendeid väga usaldusväärseks sellisel juhul, kui originaali käitlemine on jälgitavalt, järjepidevalt ja korrektselt dokumenteeritud. Ta lisab veel, et arvutid ja andmekogud on imelised jälgede talletajad aga ka haprad – teoorias on lihtne midagi kustutada, muuta või nt krüptograafia abil sulustada. Kui aga uurida, kas intervjueeritava praktika jooksul on ette tulnud olukordi, kus digitaalsete tõendite usaldusväärsus tuli kahtluse alla seada või need osutusid väärinfot andvaks, siis vastab intervjueeritav, et ei ole ette tulnud kogemus, kus kaitsja oleks seadnud kahtluse alla üksnes digitaalse tõendi usaldusväärsuse IT-tehnilisest vaatenurgast.

Kui aga uurida kui tihti kasutab intervjueeritav oma töös digitaalseid tõendeid ning millised on tüüpjuhtumid, mille korral on digitaalsete tõendite järgi vajadus, siis vastab intervjueeritav, et digitaalseid tõendeid kasutavad nad igapäevaselt. Tüüpjuhtumid seonduvad peamiste küberkuritegudega, mida menetletakse Riigiprokuratuuri tasandil. Samuti uuriti intervjueeritavalt, kas tema praktikas on ette tulnud digitaalsete tõendite võltsimist. Intervjueeritav seletab, et ette on tulnud ID-kaardi sertifikaatide võltsimist ning olukord, kus inimese teadmata on talle võltsimise abil loodud Smart-ID konto. Võltsimine on tehtud kindlaks digitõendi kõrvutamisel teiste tõenditega või tõendi enda analüüsimisega, palutud on ka ebakõla selgitada asjatundjal.

Samuti uuris autor intervjuu käigus, kas intervjueeritavat on digitaalsete tõendite kogumise ja kasutamise osas koolitatud ning ta seletab, et ta läbib veebi teel Rochesteri Tehnoloogia Instituudis pakutavat küberturbe mikromagistriõpet. Täiendõppel on nii teooria kui ka praktilised ülesanded. Lisaks viitab intervjueeritav, et enda pidev koolitamine on osa tema tööst.

Järgnevalt uuriti intervjueeritavalt, kas tema praktikas on ette tulnud olukordi, kus digitaalsete tõendite kogumine on olnud raskendatud. Intervjueeritav vastas jaatavalt ning tõi välja erinevad probleemid, mis võivad digitaalsete tõendite kogumisel ette tulla. Näiteks võib probleeme esineda ajaga - proukratuur jääb hiljaks, st teenusepakkuja kustutab andmed, kuna möödub õigusaktides kehtestatud andmete säilitamise tähtaeg. Samuti on probleemkohaks rahvusvaheline koostöö. Nimelt on erinevatel riikidel, vaatamata kehtivatele õigusabilepingutele ning Euroopa uurimismääruse direktiivile, erinev õiguskord ja praktika – vahepeal ei õnnestu andmeid saada üldse, täitja riigi hinnangul pole mingis ulatuses andmete saamine põhjendatud, saame puuduliku või kasutamiskõlbmatu digitõendi, täitja riik täidab Euroopa uurimismäärust või õigusabitaotlust liiga kaua ning asi tuleb tähtaegade tõttu saata enne tõendi saabumist kohtusse. Lisaks on oluline märkida, et intervjueeritava hinnangul on digitaalsete tõendite osakaal aja jooksul suurenenud ning suureneb veelgi. Tema isiklik seisukoht on, et mingi aja pärast pole üldse võimalik kriminaalmenetlust ilma info- ja kommunikatsioonitehnoloogia teadmisteta läbi viia.

Järgnevalt uuriti intervjueeritavalt, kas ta on täheldanud digitaalsete tõendite osas mingeid olulisi raskusi? Intervjueeritav leiab, et välja saab tuua suure andmemahu aspekti, mis raskendab nii kuriteo jälje avastamist, fikseerimist, kogumist kui ka analüüsi. Tegemaks seda edukalt, peavad eelkõige menetlejad (uurijad ja nendega koos töötavad tehnikud) olema piisavalt professionaalsed nii teadmistelt kui ka kasutatavate tehnikavahendite poolest. Näiteks peavad nad olema teadlikud erinevate operatsioonisüsteemide failisüsteemide eripäradest (kuhu ja missugusel kujul talletatakse paroolid, külastatud veebilehtede ajalugu, pildid, kuidas saada kätte kustutatud faile jne).

Vormistamise osas toob abiprokurör välja, et andmemahud on väga suured ning tihtipeale tuleb teha valik, mida kajastada protokollis ning mida mitte. Ta lisab veel, et menetlusosalised ei ole oma teadmistelt võrdsed. Kõige suuremat puudujääki on ta märganud just kohtu poolel, mis on hakanud seoses põlvkonnavahetusega siiski paranema. Tema praktikas ei ole aga olnud juhtumit, kus politseiametnikud (või teised eksperdid) koguvad sündmuskohal või mõne juhtumi raames digitaalseid tõendeid ning hiljem selgub, et need ei ole kasutamiskõlblikud.

Lisaks uuris käesoleva töö autor, kas intervjueeritava hinnangul esineb esineb digitaalsete tõendite kasutamise osas probleeme. Ning kui esineb, siis mis oleks tema ettepanekud nende

parandamiseks. Intervjueeritav kinnitab probleemide olemasolu ning leiab, et eelkõige aitab nende vastu protsessi osaliste koolitamine, probleemide teadvustamine ning õigusaktides suuremate valukohtade muutmine just suuremaid erimeelsusi tekitavates kohtades. Kui uurida, kas intervjueeritava hinnangul tuleks digitaalsete tõenditega tegelevaid töötajaid antud temaatika osas rohkem koolitada, leiab ta, et tuleks koolitada, kuna selle tulemusena võiks paraneda tõendi kvaliteet aga ka selle esitamise ja kriitilise hindamise oskus. Parim viis digitaalseid tõendeid muuta usaldusväärsemaks on aga tema hinnangul otsitavate andmete puhul nende seaduslikkuse ja usaldusväärsuse tagamiseks avastada, fikseerida, koguda ning analüüsida seaduslikult ning jälgitavalt originaali manipuleerimata. Märksõnaks on seega korrektne dokumenteerimine.

Digitaalsete tõendite tagamiseks on tema hinnangul aga parim viis läbiotsimistel sobiva tarkvaraga seadmes olev andmete seis n-ö külmutada või lukustada, et selles ei oleks võimalik teha nt kaugühendusega pahatahtlikke muudatusi. Ta lisab veel, et välisriigile on võimalik esitada taotlus hiljem õigusabitaotlusega palutavate andmete säilitamiseks. See annab mingiks ajaks ning mingisuguse garantii tõendi säilimise, puutumatuse ja terviklikkuse kohta. Viimase küsimuse juures uuriti, kas digitaalsed tõendid muudavad intervjueeritava töö lihtsamaks ning ta kinnitas, et ilma digitaalsete tõenditeta oleks seda tööd ,,lausa võimatu teha".

3.1.2 Intervjuu #2

Järgnevalt intervjueeris autor advokaati, kes on selles ametis töötanud 21 aastat. Advokaadi peamisteks töövaldkondadeks on süüteod ja tsiviilvaidlused. Kui autor uuris, millised on advokaadi kokkupuuted digitaalsete tõenditega, vastas ta, et puutub nendega kokku igapäevaselt, seda seoses vaidluste, aga ka nõustamist puudutavate ülesannetega. Kuna elu on digitaalne,[125] siis selle elu fakte tuvastada saabki vaid digitaalsete tõendite abil. Ka riigiasutused vastavad päringutele tüüpiliselt elektrooniliselt infot ja dokumente edastades. Ta lisab, et ka kohtuvaidlustes on tänapäeval reegel tõendite esitamine digitaalsena. Kuigi teatud osa neist digitaalsetest tõenditest on skaneeritud paberdokumendid. Kõige rohkem

[125] Siin advokaat täpsustab, et suhtleme interneti teel, kasutame digitaalallkirju

digitaalseid tõendeid näeb advokaat oma töös e-kirjade ja digitaalallkirjastatud dokumentide näol.

Samuti uuris töö autor intervjueeritavalt, kuidas ta tuvastab digitaalse tõendi objektiivsust ning usaldusväärsust. Advokaat leidis, et see sõltub tõendist. Digitaalallkirjastatud dokumendi osas saab kontrollida, kas see on konkreetse isiku digiallkirjaga. Mõnel juhul saab infot faili atribuutidest, nt millal konkreetne digifoto tehtud on. E-kirja failis sisaldub infot selle saatmise kohta. Mõnikord saab kontrollida ka nii, et vaadatakse, kas sama e-kiri on olemas ka teiste sama kirja saajate postkastis. Lisaks küsiti intervjueeritavalt kui usaldusväärsed on tema hinnangul digitaalsed tõendid. Ka antud küsimuse puhul usub advokaat, et eelnev sõltub tõendist. Kui digitaalallkirjastatud dokumendi puhul selle allkirjastaja ja allkirjastamise aja osas küsimusi tavaliselt üldse ei teki, siis fotode jms puhul ei ole võimalik tavaliselt nende endi abil veenduda, et need on tehtud sellest, millest need väidetakse tehtud olevat, ajal ja kohas, mida väidetakse jne. Samuti on vahe selles, kas e-kiri esitatakse .msg vormis, või nr PDF-failina, mis ei luba saada e-kirja metaandmeid, või hoopis kopeerituna *MS Word* faili.

Intervjueeritavalt uuriti ka selle kohta, kas tema praktika jooksul on ette tulnud olukordi, kus digitaalsete tõendite usaldusväärsus tuli kahtluse alla seada või need osutusid väärinfot andvaks. Advokaadile meenus üks olukord, kus vastaspool oli võltsinud tõendina esitatud e-kirja (mis oli esitatud nö pildina, mitte .msg-*failina*), nihutades selle saatmise kuupäeva ühe kuu võrra talle meelepärases suunas. Sellist võltsingut on raske avastada, kuna kirja sisu oli õige, ja teine pool kinnitas sellise sisuga kirjavahetuse toimumist. Vastaspool tegi aga selle vea, et esitas selle kirja tõendina kahel erineval korral, ja ühel neist oli ka korrektne kuupäev. Seega võltsing avastati, tehti päring e-postiteenuse pakkujale, kes kinnitas, et muudetud kuupäeval ja ajal kirja saatmise kohta logis andmed puuduvad.

Samuti uuris töö autor, kui tihti kasutab advokaat oma töös digitaalseid tõendeid ning kas intervjueeritavad on digitaalsete tõendite kogumise ja kasutamise osas koolitatud. Advokaat selgitas, et kasutab digitaalseid tõendeid oma töös igapäevaselt, neid on alati vaja, kui midagi tõendada tuleb. Koolituste osas täpsustas advokaat, et kunagi ammu oli advokaadibüroos, kus ta töötas väike koolitus meta-andmetest tekstifailides, kuid tõsisemat koolitust läbinud ta ei ole. Mida ja kuidas saab kontrollida on advokaat õppinud internetist ise infot otsides, aga ka kolleegidelt.

Lisaks eelnevale, uuris autor, kas advokaadi praktikas on ette tulnud olukordi, kus digitaalsete tõendite kogumine on raskendatud. Advokaat leidis, et võrreldes n-ö tavalite tõenditega ei ole digitaalsete tõendite kogumine tema hinnangul raskem. Ta lisab, et on mõned õigusvaldkonnad, kus millegipärast toimub edasi paberimajandus. Üks näide on väärteomenetlus – kuigi liiklusväärteod on ilmselt väga levinud, toimub toimiku koopia andmine jätkuvalt pabervormis, ja selle saamiseks on vaja kuhugi kohale minna. Muu praktika valguses on see arusaamatu – miks peab rutiinsete pisirikkumiste tõenditele juurdepääs olema mitteelekrooniline. Advokaadilt küsiti veel, et kas tema hinnangul on digitaalsete tõendite osakaal aja jooksul suurenenud ning advokaat kinnitas, et selles ei ole kahtlust.

Samuti uuris käesoleva töö autor, kas intervjueeritav täheldab digitaalsete tõendite osas mingeid olulisi raskusi. Advokaat selgitab, et tema hinnangul on kriminaalmenetluses halb praktika, kus digitaalseid tõendeid uurija poolt töödeldakse selliselt, et neid ei saa muud info kasutajad kopeerida, ega autentsust kontrollida. Advokaat näitlikustab eelnevat väidet näitega. Digitaalallkirjastatud dokumendi puhul on digikonteineris tüüpiliselt dokument kujul, mis võimaldab vähemalt teksti kopeerida (PDF, *.xdoc*-fail vms) ja digikonteiner ise võimaldab tuvastada allkirja andmist ja sellega seonduvat. Selle asemel, et anda tõendina välja konteiner, trükitakse selles olev dokument ja seotud digitaalallkiri paberile välja, kuna see läheb pabertoimikusse ning seejärel skaneeritakse PDF-failiks. Tulemuseks on PDF-pilt, mille teksti valida ja kopeerida ei saa, ning pildi kujul kinnitusleht allkirja kohta. Lisaks leiab advokaat, et probleemkohaks on ka see, kui infot kogutakse liiga hilja. Näiteks hakatakse kolme aasta pärast rääkima, et kõik peaks olema poe valvekaamerates salvestatud, kui ilmselt keegi neid salvestisi nii kaua ei säilita.

Kõigele eelnevale lisaks, küsiti advokaadilt, kas tema hinnangul esineb digitaalsete tõendite kasutamise osas probleeme ning millised oleksid tema ettepanekud taoliste probleemide parandamiseks. Advokaadi ettepanek on mitte käidelda digitaalseid tõendeid viisil, mis muudab nende kontrolli või töötlemise raskemaks. Digitaalsed tõendid tuleks edastada elektrooniliselt ja originaalkujul, mitte paberile trükituna. Lõpetada tuleks praktika, kus kaasaegse kaameraga tehtud digifotol puuduvad andmed selle tegemise aja ja asukoha kohta jms. Advokaadilt uuriti ka selle kohta, kas tema praktikas on ette tulnud olukordi, kus

menetlus on luhtunud digitaalsete tõenditega seotud problemaatika tõttu, kuid intervjueeritavale ei meenu, et selline olukord oleks aset leidnud.

Lisaks uuris töö autor, kas intervjueeritava hinnangul tuleks digitaalsete tõenditega tegelevaid töötajaid antud temaatika osas rohkem koolitada. Advokaat kinnitas, et kindlasti tuleks seda teha, kuid asi ei ole ainult koolitamises, vaid ka selles, et puuduvad reeglid, mis välistavad digitaalsete tõendite töötlemise viisil nagu eespool kirjeldatud, mille tulemusena need kaotavad midagi olulist oma sisus, nt autentsuse kontrolli võimaluse. Advokaadi hinnangul parimaks viisiks muuta digitaalseid tõendeid usaldusväärsemaks on nende uurimine võimalikult originaalsel kujul.

Parim viis aga digitaalsete tõendite tagamiseks on intervjueeritava advokaadi arvates mitte kustutada informatsiooni, mida võib tõendamisel vaja minna, sh politsei kehakaamerate salvestisi jms ning koguda infot õigel ajal ehk siis kui see on võimalik. Kui telekomid hoiavad kõneandmeid ühe aasta jooksul, tuleb neid küsida ka selle aja jooksul. Või kui on teada, et võib olemas olla valvekaamerate salvestused, siis need kirjutatakse mõnikord üle juba nädalate või isegi päevadega. Viimasena uuris töö autor advokaadi käest, kas digitaalsed tõendid muudavad tema töö lihtsamaks. Eelnevale küsimusele anti positiivne vastus.

3.1.3 Intervjuu #3

Kolmandana intervjueeris käesoleva töö autor ringkonnakohtunikku, kes on ringkonnakohtunikuna töötanud umbes 2 aastat, kuid kohtunikuna umbes 5,5 aastat. Esmalt uuris töö autor kohtunikult seda, millised on tema kokkupuuted digitaalsete tõenditega. Intervjueeritav täpsustas, et kriminaalasju lahendades puutub ta digitaalsete tõenditega üsna sageli kokku, kuna neid kasutatakse paljudes kohtuasjades. Digitaalse tõendi liik, mida kohtunik näeb enim oma töös on videod.[126]

[126] Kohtunik täpsustas, et oma töös enim on kokkupuudet mingi turvakaamera, autokaamera või politsei paigaldatud salajase jälgimise kaamera videoga.

Järgnevalt uuris töö autor kohtunikult, kuidas tuvastada digitaalse tõendi objektiivsust ja usaldusväärsust. Intervjueeritav selgitas, et üldjuhul selliseid probleeme ei teki. Mõnikord vaieldakse selle üle, kas menetluslikel põhjustel tõendile tugineda saab. Videotega on ka vaidlused selle kohta, millal video tehtud on: videol kuvatakse mingit kellaaega, aga see ei pruugi olla õige, näiteks kella keeramise tõttu. On ka selliseid olukordi, kus alguses on olnud tegemist digitaalsete andmetega, aga menetluses on nad n-ö muundunud analoogseteks. Näiteks mingi elektroonse arve või elektroonse pangaülekande kinnituse väljatrükid. Nendega seoses on küll vaidlusi olnud. Tõstatatud on küsimus, kas nad olid oma algsel elektroonsel kujul ka sellised, nagu nad on väljatrükitult või on neid enne välja trükkimist muudetud (modifitseeriti, fabritseeriti). Üldjuhul on vaidlused siiski käinud tõendi sisu üle (mida tõendilt, eeskätt videolt, üldse näha on, kas sellel on mingi tähtsus jms). Kohtunikul ei ole oma mäletamist mööda tekkinud probleemi selle osas, kas digitaalne tõend on kuidagi fabritseeritud või modifitseeritud.

Kui uurida kohtunikult tema kokkupuutumist digitaalsete tõendite võltsimisega, siis selgitab ta, et võltsitud videosid ei ole tema praktikas ette tulnud. Küll aga on olnud olukordi, kus arvete ning pangaülekannete väljavõtete paberkandjatel väljatrükkide puhul on olnud juhtumeid, kus on selgunud, et algne elektroonne andmekandja oli mõneti teistsugune kui väljatrükk. Järgnevalt küsiti intervjueeritavalt digitaalsete tõendite kasutamise ja kogumise osas tehtud koolituste kohta. Kohtunik selgitab, et on võimalik, et kunagi on selline põgus koolitus olnud, kuid ta täpselt ei mäleta. Ise on ta digitaalsete tõendite kohta õppinud töö käigus. Samuti nõustub ta väitega, et digitaalsete tõendite osakaal on aja jooksul suurenenud, kuna elu on järjest enam liikunud „digimaailma".

Kui uurida intervjueeritavalt, kas ta on märganud digitaalsete tõendite osas mingeid olulisi raskusi,[127] märgib ta, et selliseid olukordi tuleb ikka ette. Ta näitlikustab eelnevat erinevate näidetega. Näiteks prinditakse mingi fail välja nii, et osa teksti jääb väljapoole väljaprinditavat ala. Või prinditakse mõni tabel välja mitmele lehele – ja on raskusi arusaamisega, kuidas erinevatel lehtedel olevad read või veerud omavahel kokku käivad. Segadusi on ette tulnud videote filmimise kellaaegadega. Videofaile talletatakse tihtipeale CD- või DVD-plaatidel. Need aga võivad ajapikku viga saada ja seetõttu võib nende avamine menetluse arenedes minna keerulisemaks või osutuda suisa võimatuks. Probleem on ka

[127] Näiteks probleemid vormistamise osas, vähesed tehnilised teadmised, raskused kogumisel või talletamisel.

failide n-ö pilves hoidmisega – ajapikku võib juurdepääs neile mingil põhjusel võimatuks osutuda. Videote kvaliteet on ajaga tugevasti paranenud. Kui veel mõne aasta eest oli resolutsioon väga madal ja inimeste äratundmine raske, on asjad selles plaanis järjest paremaks läinud.

Lisaks küsis töö autor, kas intervjueeritav on teadlik juhtumitest, kus politseiametnikud (või teised eksperdid) koguvad sündmuskohal või mõne juhtumi raames digitaalseid tõendeid ning hiljem selgub, et need ei ole kasutamiskõlblikud. Kohtunik vastas, et ta ei mäleta, et midagi sellist oleks juhtunud. Samuti uuris töö autor, kas intervjueeritava arvates tuleks digitaalsete tõenditega tegelevaid töötajaid antud temaatika osas rohkem koolitada. Intervjueeritav leidis, et ilmselt ei jookse koolitamine kellelgi mööda külgi maha.

Viimaseks uuris töö autor, mis on kohtuniku hinnangul parim viis digitaalseid tõendeid muuta usaldusväärsemaks ja kas digitaalsed tõendid muudavad tema töö lihtsamaks. Kohtunik nentis, et sellele küsimusele ei oska ta kuigivõrd vastata. Ilmselt peaks üritama säilitada võimalikult palju meta-andmeid, et ei tekiks ebaselgust tõendi päritolu ja selle loomise aja osas. Viimase küsimuse osas vastas kohtunik, et mõnes mõttes toovad digitaalsed tõendid tööd juurde, kuna on ju vaja täiendavaid tõendeid analüüsida. Teisalt aga võivad nad aidata tõe väljaselgitamisel. Nii et ilmselt võib vastata nii ja naa.

3.1.4 Intervjuu #4

Käesoleva töö autor intervjueeris ka ühte vandeadvokaati, kes on sellel ametikohal töötanud 9,5 aastat. Vandeadvokaat selgitas, et kohtumenetluses puutub ta digitaalsete tõenditega pidevalt kokku. Enim näeb ta oma töös arvutite ja muude IT-seadmete vaatluseid. Lisaks uuriti intervjueeritavalt, kui tihti taolisi tõendeid kasutatakse ning intervjueeritav selgitas, et kriminaalmenetluses on pidevalt kasutusel arvutivaatlused jms. Kui aga uurida, kuidas vandeadvokaadi töös tuvastatakse digitaalsete tõendite usaldusväärsust, selgitab ta, et kasutatakse failide räsi arvutamist ja vastavad numbrid on nähtuvad protokollidest.

Järgnevalt uuris töö autor intervjueeritavalt, kui usaldusväärsed on tema hinnangul digitaalsed tõendid ning intervjueeritav selgitab, et kui ei ole teisiti tõendatud, siis on

digitaalsed tõendid väga usaldusväärsed. Tema praktika jooksul ei ole ette tulnud ka olukordi, kus digitaalsete tõendite usaldusväärsus oleks tulnud kahtluse alla seada või need osutusid väärinfot andvaks. Samuti ei ole vandeadvokaati antud teema osas koolitatud ning tema praktikas ei ole ette tulnud olukordi, kus digitaalsete tõendite kogumine on olnud raskendatud. Intervjueeritava hinnangul on aga digitaalsete tõendite osakaal aja jooksul suurenenud.

Lisaks uuris töö autor, kas intervjueeritav on täheldanud digitaalsete tõendite osas mingeid olulisi raskusi. Vandeadvokaat viitas muredele vormistamisega ning kohtus esitamisega, kuid tema praktikas ei ole olnud juhtumeid, kus politseiametnikud (või teised eksperdid) koguvad sündmuskohal või mõne juhtumi raames digitaalseid tõendeid ning hiljem selgub, et need ei ole kasutamiskõlblikud. Samuti ei ole ette tulnud olukordi, kus menetlus on luhtunud digitaalsete tõendite problemaatika tõttu.

Kui uurida, mis aitaks intervjueeritava hinnangul digitaalsete tõendite kasutamise parandamist, leiab ta, et kasu võiks olla vastavatest koolitustest. Samuti nõustub vandeadvokaat väitega, et digitaalsete tõenditega tegelevaid töötajaid võiks antud temaatika osas rohkem koolitada. Lisaks leiab intervjueeritav, et inimeste koolitamine on ka parim viis muuta digitaalsed tõendid usaldusväärsemaks. Kui aga uurida vandeadvokaadilt, kas digitaalsed tõendid muudavad tema töö lihtsamaks, ütleb ta ausalt, et ta ei oska sellele küsimusele vastata.

3.1.5 Intervjuu #5

Järgnevalt vestles käesoleva magistritöö autor ringkonnaprokuröriga, kes on sellel ametikohal töötanud alates 2019. aastast. Kokkupuuteid digitaalsete tõenditega on ringkonnaprokuröril mitmeid, kuna tema hinnangul ei ole ilmselt kriminaalasju, kus ei puututa kokku digitaalse teabega. Kui uurida, kuidas intervjueeritava hinnangul tuvastada digitaalse tõendi usaldusväärsust, selgitab ta, et esmalt pead ise aru saama kuidas selline teave on tekkinud ning kuidas see konkreetne jälg on jäetud. Eelnev aitab ka kohtus paremini argumenteerida. Usaldusväärsuse eeldus on arusaamine. Alles siis kui oled aru saanud, kuidas tõend tekib, siis

on võimalus illustreerida, et see asi oli kogumise hetkel originaalkujul. Suureks abiks on ka eriteadmistega spetsialistide ülekuulamine.

Kui uurida, kui usaldusväärsed on intervjueeritava hinnangul digitaalsed tõendid, selgitab ringkonnaprokurör, et iga tõendi puhul on usaldusväärsus individuaalne ning kõike tuleb hinnata eraldi. Kui intervjueeritavalt aga uurida, kas tema praktika jooksul on esitatud tõendeid mis on osutunud väärinfot andvaks, informeerib ta, et ei ole. Lisaks uuris käesoleva magistritöö autor, kuidas toimub antud teema osas koolitamine prokuratuuris. Intervjueeritav selgitab, et prokuratuuris on läbi viidud erinevaid koolitusi, kuid mitmed prokurörid on osalenud ka infotehnoloogiaõiguse täiendõppes või on töö kõrvalt õppinud juurde infotehnoloogia eriala. Lisaks eelnevale uuris käesoleva töö autor, mis on digitaalsete tõendite kogumise juures kõige raskem asjaolu. Ringkonnaprokurör selgitas, et suurim probleemkoht on see, et teatakse, et kuskil on vajalikud andmed olemas, kuid neile puudub ligipääs. Näiteks andmed on krüpteeritud, andmete kogumisega jäädakse hiljaks või hävivad need väga kiiresti. Samuti viitab intervjueeritav asjaolule, et väljaspool Euroopa Liitu on väga raske saada digitaalseid tõendeid kätte, ta lisab veel, et ühele taotlusele ootab ta Kanadast vastust juba 1,5 aastat.

Lisaks uuris käesoleva töö autor, mis oleksid intervjueeritava ettepanekud digitaalsete tõendite kogumise ja usaldusväärsuse parandamiseks. Ringkonnaprokurör selgitas, et abiks tuleks kindlasti järjepidev koolitus ning eksimustest järelduste tegemine ja praktikas situatsioonide läbi harjutamine. Väga rangete reeglite kehtestamist erinevate teabevormide puhul ta ei poolda, kuna need jäävad ajale lihtsalt jalgu. Luhtunud menetlusi ei ole tema praktika jooksul olnud. Viimase küsimusena sai uuritud, kas digitaalsed tõendid muudavad ringkonnaprokuröri töö lihtsamaks ning intervjueeritav vastas, et digitaalsed tõendid annavad tööd juurde ja selle vastu ei ole tal midagi.

3.1.6 Intervjuu #6

Samuti intervjueeriti käesoleva magistritöö raames prokuröri, kes on oma ametit pidanud juba 15 aastat. Ta selgitas, et kriminaalmenetluses tegeletakse andmekandjatega seotud digitaalse teabega praktiliselt igas kriminaalasjas. Kui uurida, millist liiki digitaalset teavet ta näeb, siis

selgitab prokurör, et enim näeb ta serveri andmeid, pilte, videosid, ühelt andmekandjalt teisele kandmisi ning suhtlusprogrammides peetud vestlusi.

Lisaks uuriti intervjueeritavalt, kuidas tema hinnangul tuleks tuvastada digitaalse tõendi usaldusväärsust ja objektiivust. Prokurör selgitas, et prokuratuuri toimingud peavad tekitama kohtumenetluses usaldusväärsuse. Kehtib tavaline reegel, et menetleja peab tagama tõendi kogumise jälgitavuse, et vastaspool saaks veenduda, et teavet pole muudetud selliselt, et seda ei saaks kohtus kasutada. Kui vastaspool argumenteerib, et tõend ei ole usaldusväärne, siis kohtus on selline praktika, et tuleb välja tuua ka põhjus, miks teise poole hinnangul ei ole see tõend usaldusväärne. Selleks on vaja aga teadmisi. Suurimad probleemid on prokuröridel kannatanute ning tunnistajate esitatud digitaalse teave puhul. Nad esitavad ise pilte ja videofaile ja sellega tekib kõige rohkem usaldusväärsuse probleeme, kuna tegemist on teisese teabega, mis ei ole originaalformaat. Usaldusväärsust tuleb alati kontrollida, kõiki tõendeid tuleb hinnata kogumis.

Samuti uuris käesoleva magistritöö autor, kas prokuröri praktika jooksul on esitatud tõendeid mis on osutunud väärinfot andvaks? Intervjueeritav selgitab, et tema kolleegil oli selline juhtum, et tervisekahjustuse põhjustamise küsimuses esitas kannatanu oma hematoomidest foto. Hiljem selgus aga kohtus, et kannatanu oli fotot manipuleerinud selliselt, et vigastus oleks paremini näha ning see jätaks intensiivsema mulje. Eelnev mõjutas aga kannatanu ütluste usaldusväärsust. Samuti viitas intervjueeritav olukorrale, kus ta läbiotsimise käigus tegi pildiotsingut töötavast arvutist ning ta ei teadnud, et selline otsing muudab faili meta-andmeid. Sellise muutuse põhjalt oleks prokurör teinud eksliku järelduse, kui ta ei oleks hiljem olnud teadlik, et tema tegevus võis mõjutada meta-andmeid. Tegemist ei olnud pahatahtliku tegevusega, kuid paljud muutused võivad tulla seadme enda tegevusest või menetlejate pahaaimamatust tegevusest.

Lisaks uuris käesoleva töö autor, kas intervjueeritavat on digitaalsete tõendite kasutamise ja kogumise osas koolitatud? Prokurör selgitab, et ta on lõpetanud IT-kolledži ning samuti on tal olnud võimalusi osaleda koolitustel, mis on suunatud politseile. Prokurör lisab veel, et süsteemset haridust paraku praegu Eestis ei ole. Kui uurida aga intervjueeritavalt, et mis on digitaalsete tõendite kogumise juures kõige raskem selgitab ta, et digitaalne teave on latentne, me ei näe ja ei tea, kust seda saaks. Samuti on see aegkriitiline ning liigub mööda

jurisdiktsioone. Kohtus tekitab probleeme jurisdiktsioonipõhimõte ning Eestil pole selget reeglistikku, kuidas sellest üle saada.

Samuti uuris käesoleva töö autor intervjueeritavalt, mis on tema hinnangul raskused digitaalsete tõendite kogumisel. Prokurör selgitab, et eksimusi on juhtunud näiteks teabe talletamisel. Keerukad olukorrad on need, kus ollakse läbiotsimisel ning ei taheta süsteemi kinni panna, kuna süsteemi sulgemisega tekivad krüpteeringu ja parooli probleemid. Politseil on selleks oma sisemised reeglistikud. Tõendi koguja peab olema teema osas teadlik. Samuti on oluline programmidega kursis olemine ning koolitamine. Lisaks sai uuritud, kas on ette tulnud ka olukordi, kus menetlus on digitaalsete tõendite problemaatika tõttu luhtunud. Prokurör viitab oma kogemusele, mis juhtus umbes 10 aastat tagasi. Rumalusest ei kontrollinud, kas andmekandja sulgemisel toimub automaatne krüpteerimine. Andmekandja pandi kinni, toimus automaatne krüpteerimine ning seetõttu see menetlus ka luhtus.

Viimase küsimusena uuris autor, kas digitaalsed tõendid muudavad prokuröri töö lihtsamaks ning intervjueeritav selgitas, et nendega kaasneb palju väljakutseid ning palju olukordi, kus „pinnas ei ole kindel“. Digitaalne teave võimaldab palju uurida ja leida uusi lähenemisi. Samas leiab intervjueeritav, et on ka prokuröre, kelle jaoks on see temaatika pigem igav ja kes eelistavad teistsuguseid tõendeid.

3.1.7 Intervjuu #7

Viimasena intervjueeris käesoleva magistritöö autor eriasjade prokuröri, kes on eriasjade prokurör alates 2004. aastast, kuid prokuratuuris kokku on ta töötanud umbes 25 aastat. Prokurör selgitab, et igas kriminaalasjas puutub ta kokku igasuguse digitaalse teabega. Enim esineb kõneeristusi, videoid (nt turvakaamera salvestised), audiosalvestised, logifailid, pangaandmed.

Kui uurida intervjueeritavalt, kuidas tuvastada digitaalse tõendi usaldusväärsust või objektiivust, selgitab ta, et see oleneb eelkõige sellest, millega täpsemalt on tegu. Ühe hea võimalusena viitab intervjueeritav räsiarvude kontrollimisele. Nimelt pärast koopia saamist politseilt toimub selle koopia uurimine ja võrdlemine. Kui vaatlusprotokollis on kõik

räsiarvud samad, siis see kinnitab, et tegemist on originaaliga täpselt samal kujul digitaalse informatsiooniga. Teoorias on loomulikult võimalik ka videosid järgi teha, kuid intervjueeritav ei ole kuulnud kohtuvaidlusest, kus oleks tõstatatud küsimus video manipuleerimise kohta. Siiski võib see tema hinnangul olla murekoht, mis võib järgmise 5-10 aasta jooksul tõstatuda.

Kui uurida intervjueeritavalt, kas tema hinnangul on digitaalsed tõendid usaldusväärsed, siis selgitab ta, et see oleneb. Näiteks leiab ta, et video on näiteks usaldusväärsem kui inimese mälu. Samuti uuris autor, kas intervjueeritavat on digitaalsete tõendite osas koolitatud. Eriasjade prokurör selgitab, et ta on osa võtnud antud temaatika koolitusest, mis oli suunatud politseile. Kui aga uurida, kas on esinenud juhtumeid, kus eksperdid on digitaalseid tõendeid kogunud ja hiljem selgub, et need ei ole kasutuskõlblikud, selgitab intervjueeritav, et on olnud küll juhtumeid, kus politsei on näiteks märkinud video osas valed ajavahemikud. Ükski menetlus seetõttu siiski luhtunud ei ole. Lisaks sai uuritud, kas digitaalsete tõendite osas esineb murekohti ning intervjuueritav selgitab, et üheks murekohaks on kohtus digitaalse tõendi esitamine. Ehk kuidas seda kohtus visualiseerida selliselt, et see oleks kõigile ilusti nähtav ja arusaadav. Kui seda tõendit nähtavaks teha ei osata, siis kohtul läheb see kõrvust mööda. Ehk kui prokuratuur ei suuda visualiseerida eelnevat piltlikult, siis tõendi väärtus väheneb.

Samuti uuris töö autor, kas intervjueeritava hinnangul muudavad digitaalsed tõendid tema töö lihtsamaks, siis selgitab ta, et eelnev on tööd lihtsamaks muutnud küll ning ta valib alati pigem digitaalse tõendi kui muu paberkujul tõendi.

3.1 Intervjuude järeldused

Intervjuudest selgub, et digitaalsete tõenditega puutuvad kokku praktiliselt kõik õiguspraktikud ning oma töös näevad nad erinevaid tüüpi digitaalseid tõendeid ning konsensus on selle osas, et digitaalsete tõendite osakaal on aja jooksul suurenenud ning digitaalsete tõenditega tegelevaid inimesi tuleks koolitada.

Samuti selgus intervjuude põhjal, et mitmed õiguspraktikuid, keda antud temaatika osas intervjueeriti, ei ole otseselt digitaalsete tõendite osas koolitatud ning mitmed vastanutest on ainult töö käigus digitaalsete tõendite kohta õppinud või on ise otsustanud juurde õppida. Samas viitab konsensus koolitamise osas asjaolule, et erinevate koolituste läbiviimine on intervjueeritavate hinnangul positiivne.

Oluline on ka asjaolu, et intervjuudes on viidatud samadele probleemidele, mis autor on tõstatanud oma magistritöös. Nimelt on ühe probleemkohana on rõhutatud rahvusvahelist koostööd ja asjaolu, et puudub ühine reeglistik, mis annaks erinevatele riikidele selguse selle osas, kuidas digitaalseid tõendeid koguda. Eelnev võib viia aga situatsioonini, kus välismaiste uurimisasutuste digitaalsete tõendite kvaliteet on oluliselt madalam. See võib aga negatiivselt mõjutada menetlust. Samuti on üks intervjueeritav välja toonud, et puuduvad reeglid, mis välistavad digitaalsete tõendite töötlemise selliselt, et digitaalset tõendit ei esitada elektrooniliselt ja originaalkujul, vaid paberile trükituna.

Samuti on intervjueeritavad välja toonud ka situatsioone, kus inimesed on üritanud negatiivelt manipuleerida digitaalset tõendit. Näiteks on muudetud e-kirja saatmise kuupäeva ning töödeldud fotot. Ka see on probleemkoht, mille käesoleva magistritöö autor on oma töös tõstatanud. Eelnev viitab sellele, et digitaalsete tõendite kasutamise osas tuleb pöörata tähelepanu digitaalse tõendi terviklikkusele ning puutumatusele. Taolise võltsimise katse tõenäosust aitab autori hinnangul vähendada *chain of custody* jälgimine ning tõendi originaalversiooni säilitamine (antud juhul oli tegemist ekraanitõmmisega ning kannatanu poolt saadetud fotoga).

Positiivse asjaoluna võib välja tuua, et vastanute hulgast oli ainult üks õiguspraktik, kellel on ette tulnud olukord, kus menetlus on luhtunud digitaalsete tõendite problemaatika tõttu. Siiski on aga intervjuudes viidatud asjaolule, et vaidlusi on tekkinud selle üle, et digitaalne tõend on viidud n-ö paberkujule ja ei saa kindlad olla, kas paberil kujutatu vastab digitaalse tõendi tegelikule sisule. Seega võib järeldada, et kuigi on üritatud digitaalseid tõendeid muuta, ei ole siiski vastanute praktikas esinenud olukordi, kus taoliseks võltsimiseks oleks kasutatud *anti-forensic* tarkvara.

3.2 Ettepanekud

Toetudes erialakirjanduses välja toodud asjaoludele ning intervjueeritute kogemustele, leiab töö autor, et digitaalseid tõendeid aitaks muuta usaldusväärsemaks inimeste järjepidev ja süsteemne koolitamine. Koolitamine annab antud temaatika osas paremaid teadmisi, mis omakorda aitab autori hinnangul kriitilisemalt suhtuda digitaalse tõendi usaldusväärsusesse. Samuti selgus intervjuude põhjal, et mitmed intervjueeritavad on pidanud ise antud temaatika osas juurde õppima. Ühtne koolitamine annaks aga võimaluse jagada kõikidele võrdseid teadmisi antud teema kohta ning seeläbi potentsiaalselt muuta ka kohtumenetluse pooli võrdsemaks ning tagada, et manipuleeritud digitõendid saaksid välja selgitatud ja menetlusest kõrvaldatud. Kõikide kohtumenetluse poolte koolitamine on autori hinnangul asjaolu, mis kätkeb endas mitmeid positiivseid aspekte.

Asjaolu, et koolituste osas peegeldub ebaühtlane tase, viitab aga laiema uurimisküsimuse vajadusele, mille põhjal saaks täpsemalt hinnata, milliseid teadmisi on antud temaatika osas õiguspraktikutele edasi antud ja kas neil on huvi antud teema osas lisateadmiste saamiseks. Samuti võib ühtlane koolitamine Euroopa Liidu tasandil muuta suhtluse erinevate riikide organite vahel efektiivsemaks, kuna paraneksid tehnilised teadmised digitaalsete tõendite osas ning eelnev võiks suurendada ka koostöö tulemuslikkust. Samuti võib see parandada digitaalsete tõenditega tegelevate inimeste valmisolekut aina enam asjakohaseks muutuvate probleemide osas – näiteks andmemahu pidev kasv.

Lisaks leiab autor, et kaalutleda tuleb ka eelarvamuste rolli digitaalses ekspertiisis. Eelnevat asjaolu saab aga vähendada, kui kontrollida, millist kontekstuaalset informatsiooni ekspertidele antakse ja tagada, et püsiks informatsiooni osas neutraalsus ehk ebavajaliku teabe teatavaks saamine ei kallutaks eksperti arvama, et kahtlusalune on süüdi või vastupidi. Samuti on oluline pöörata tähelepanu *chain of custody* hoidmisele, et tagada digitaalse tõendi terviklikkus ja usaldusväärsus. Eelnev aitab minimaliseerida ka potentsiaalseid vaidlusi, mis võivad tekkida antud küsimuse osas. Samuti oleks positiivne kaalutleda ühtse meetodi loomist, mis aitaks eksperdil hinnata, kui tõenäolised on tema järeldused.

Lisaks on oluline pöörata rohkem rõhku ühtsete reeglite ning kontrollnimekirjade loomisele. Ühtsed reeglid või soovitused aitaksid paremini veenduda, et välismaa organite käest saadud digitaalne tõend on usaldusväärne ning terviklik. Autori hinnangul muutuks ka

rahvusvaheline koostöö seeläbi efektiivsemaks, kuna kõik osapooled oleks rohkem teadlikud digitaalsete tõendite olemusest. Samuti on oluline pöörata tähelepanu suhtlusele kolmandate riikidega, st riikidega väljaspool Euroopa Liitu. Parem ettevalmistus rahvusvaheliseks koostööks võib autori hinnangul vähendada möödarääkimisi ning arusaamatusi erinevate riikide organite vahel. Samas võib loota, et sõbralikud suhted võivad kaasa aidata ka õigusabitaotlustele kiiremate vastuste andmise osas.

Viimasena soovitab autor kaalutleda ekspertide tasemetestide rakendamist. Töö autor on mitmeid kordi käesolevas magistritöös viidanud asjaolule, et tehnoloogia areng on äärmiselt kiire ning eksperdid ei pruugi taolise arenguga nii kiiresti kaasas käia ja võivad seetõttu teha digitaalsete tõendite kogumisel ning ka tõlgendamisel vigu. Tasemetestid aitaksid analüüsida, millised on ekspertide puudujäägid ja kuidas saaks taolisi puudujääke korrigeerida ning teadmisi edasi arendada. Samas selgitaksid tasemetestid ka välja kitsaskohad, millele tuleks keskenduda järjepideval koolitamisel. Lisaks on oluline teadvustada, et võrdlemisi levinud arusaam, et digitaalsed tõendid on usaldusväärsed, kuna need on loodud tehnoloogia abiga, ei ole tõene ning igasugune tõend vajab hinnangut selle usaldusväärsuse kohta. Ka digitaalne tõend.

Autori hinnangul võivad kõik eelnevad ettepanekud aidata vähendada potentsiaalseid probleeme digitaalsete tõendite kasutamisel ja kogumisel ning muuta neid ka usaldusväärsemaks. Kõige eelneva abil saab aga ka kohtumenetlust muuta kõikide osapoolte jaoks selgemaks ning potentsiaalselt ka võrdsemaks.

Kokkuvõte

Käesoleva magistritöö eesmärgiks oli analüüsida, kas on olemas asjaolusid, mis viitavad, et digitaalsete tõendite osas on alust kahelda nende usaldusväärsuses. Samuti oli eesmärgiks lugejale tutvustada digitaalseid tõendeid, digitaalset ekspertiisi ja erinevaid murekohti, mis eelnevatega kaasneda võivad. Et leida vastust uurimisküsimusele, analüüsis autor erinevat erialakirjandust, viis läbi intervjuud inimestega, kes puutuvad oma töös kokku digitaalsete tõenditega ning tegi eelnevale teabele tuginedes vastavad järeldused.

Käesolev magistritöö on jagatud kolmeks erinevaks peatükiks ning igas peatükis anti lugejale ülevaade erinevatest teemadest. Esimeses peatükis andis töö autor lugejale ülevaate sellest, mis on digitaalsed tõendid ning digitaalne kriminalistika. Teises peatükis käsitles autor digitaalsete tõendite potentsiaalseid kitsaskohti ning kolmandas peatükis keskendus autor intervjuudele ning ettepanekutele.

Esimese potentsiaalse probleemkohana tõi autor välja digitaalsete tõendite usaldusväärsuse küsimused. Nimelt on üheks probleemkohaks see, et digitaalset ekspertiisi teostav ekspert peab olema suuteline hindama oma järelduste tõenäosust, kuid digitaalses ekspertiisis puudub konkreetne matemaatiline meetod selle tegemiseks. Oma järelduste tõenäosuse hindamine on aga autori hinnangul digitaalsete tõendite usaldusväärsuse seisukohast oluline, kuna see annaks infot selle kohta, kui usaldusväärne on tõend. Eelnev aitaks aga kohtunikul kaalutleda, kas ja millises ulatuses antud tõendile otsuse tegemisel tugineda.

Lisaks on töö autor viidanud asjaolule, et seadmete pideva arengu tõttu ei ole välistatud, et digitaalsed tõendeid analüüsiv ekspert satub vastamisi olukorraga, mida ei ole veel tema praktikas ning potentsiaalselt ka laiemalt ette tulnud. Eelnev asjaolu aga tähendab, et taolise situatsiooni lahendamiseks ei ole veel koostatud mingisugust dokumenteeritud käitumissoovitust. Samuti on oluline viidata asjaolule, et tehnoloogia kiire areng võib limiteerida uurimismeetodite katsetamise ning hindamise ajalist pikkust ja efektiivsust. Ehk uued meetodid ei pruugi piisavalt kaua aega viita testimisfaasis. See, aga omakorda tähendab, et uurimismeetod ei pruugi olla piisavalt usaldusväärne ning tähelepanuta võivad jääda vead, mis võivad esineda programmis. Seega võivad potentsiaalselt probleeme tekitada ekspertide ebaõiged tõlgendused, mis on tingitud uuest tehnoloogiast või teadmiste puudumisest ning ka

asjaolu, et uued meetodid ja tarkvarad ei pruugi olla piisavalt läbi testitud ning võivad seega sisaldada endis vigu, mis mõjutavad digitaalse tõendi järeldusi.

Käesoleva magistritöö raames pööras autor tähelepanu ka *anti-forensic* tööriistadele ning digitaalsete tõendite võltsimisele. Autor selgitas, mis on *anti-forensic* tööriistad ning kuidas need võivad mõjutada digitaalseid tõendeid. Tegemist on erinevate tarkvaradega, mille eesmärk eksitada eksperte, varjata mingi sündmuse juhtumist, segada informatsiooni kogumist ning ka seada kahtlusi tõendi usaldusväärsuse osas. Autor viitab asjaolule, et *anti forensic* tööriistade efektiivne kasutamine võib täielikult muuta tõendi väärtust, legitiimsust ning terviklikkust. Eelnev võib suunata digitaalse ekspertiisi tarkvara valedele jälgedele ja luua vale kuvandi asjaoludest, mis omakorda mõjutavad ekspertide järeldusi. See võib aga omakorda muuta digitaalse tõendi usaldusväärsust, kuna eksperdi analüüs ei peegelda tegelikku olukorda.

Samuti rõhutas käesoleva töö autor, et digitaalseid tõendeid võidakse üritada muuta ka kergemaid viise kasutades. Autor juhtis tähelepanu asjaolule, et üks lihtsamaid viise digitaalsete tõendite muutmiseks on digitaalsete tõendite sisu muutmine. Autor on selgitanud, et tegemist on mitmetel juhtudel võrdlemisi lihtsa protsessiga, mis ei pruugi vajada mingisuguseid eriteadmisi. Näiteks on võrdlemisi lihtne teha mingist vestlusest kuvatõmmis, ning seda erinevate töötlusprogrammidega muuta. Seejärel võib inimene proovida taolist muudetud tõendit kohtule esitada. Erinevad katsed esitada kohtule võltsitud tõendeid on küll haruldased, kuid autor on viidanud, et erialakirjanduses on jõutud seisukohale, et selliste katsete arv on suurenemas. Seega on oluline alati kontrollida digitaalse tõendi originaali, et kindlustada, et digitaalse tõendi terviklikkus on täielikult säilinud.

Järgnevalt analüüsis käesoleva magistritöö autor erinevaid inimlikke vigu, mis võivad digitaalsete tõendite kasutamisel ja analüüsis ette tulla. Esmalt on autor juhtinud tähelepanu asjaolule, et Euroopa Liidus ei ole otseselt määratletud, millise haridusliku taustaga peab olema digitaalkriminalistika ekspert. Analoogne seis on ka Norras, kus on Norra Politsei Direktoraat selgitanud, et kriminaalmenetluses peaks digitaalsete tõenditega tegelema vaid adekvaatse õppega ja vastava kompetentsiga inimesed, kuid ei ole selgitatud, mida need terminid praktikas tähendavad. Autori hinnangul tähendab aga eelnev, et ekspertide taset võiks testida rutiinsete tasemetestidega. Taolisele seisukohale on jõutud ka autori poolt eelnevalt viidatud erialakirjanduses. Autor leiab, et taoline testimine annaks parema ülevaate

ekspertide oskuste kohta. Kui sellist testimist rakendada ühtselt erinevates riikides, oleks võimalik saavutada ekspertide seas ühtlaselt kõrge kvaliteet, mis tagab omakorda ka digitaalsete tõendite suurenenud usaldusväärsuse. Samuti on autor teinud ülevaate kurikuulsast lahendist *Connecticut v. Amero*, kus on näitlikustatud, kui oluline roll on eksperdi teadmistel ning milliseid drastilisi tagajärgi võivad eksperdi vähesed teadmised tuua kohtumenetluses.

Samuti on autor välja toonud, et digitaalsete tõendite uurimisel on protseduurilised puudujäägid. Nimelt on olemas suurel hulgal erinevaid põhimõtteid, mida tuleb järgida digitaalses ekspertiisis, kuid kuigi printsiipe on mitmeid ja erinevaid, ei anna need erilist infot selle kohta, millised peaksid olema digitaalses ekpertiisis rakendatavad protseduurilised reeglid. Puuduvad ettekirjutused selle kohta, et kuidas uurimisprotsessi kui sellist läbi viia. Konkreetsed kohustuslikud protseduurilised reeglid võivad aga tugevalt kaasa aidata uurimise efektiivsusele ja kvaliteedile. Autor on viidanud asjaolule, et olukorda parandaks ühtsete protseduuriliste reeglite ja kontrollnimekirjad loomine.

Nimelt kindel reeglistik ja kontrollnimekirjad aitaksid ekspertidel paremini meeles pidada ka pisemaid tööülesandeid, mille tegemise vajadusest on nad teadlikud, kuid mis võivad töö käigus tahtmatult ununeda. Samuti on autor juhtinud tähelepanu asjaolule, et erinevate teadmiste ja meetodite jagamine erinevate korrakaitseorganite vahel võib endaga kaasa tuua digitaalsete tõendite usaldusväärsuse suurenemise. Esiteks suurendaks see erinevate digitaalkriminalistika ekspertide teadmisi ning oskusi. Teiseks võib välja tuua kvaliteedi paranemise. Kui omavahel jagada erinevaid meetodeid, siis suureneb ka inimeste hulk, kes selliseid meetodeid läbi katsetavad ning veenduvad selle töökindluses.

Samuti on autor viidanud erinevatele asjaoludele, millest võib järeldada, et digitaalsete tõendite probleemkohaks on ka teadmiste puudumine ning tihti alarahastus ning liigselt suur digitaalsete tõendite hulk. Need on kõik asjaolud, mis võivad negatiivselt mõjutada digitaalse tõendi usaldusväärsust. Autori hinnangul on tegemist temaatikaga, mis vajaks ka Eestis edasist uurimist. Teadmiste kvaliteedi taseme hindamine aitaks paremini mõista Eesti digitaalse ekspertiisi kvaliteeti. Samuti on oluline pöörata tähelepanu alarahastuse negatiivsetele aspektidele.

Lisaks andis käesoleva töö autor ülevaate ka eelarvamustele, mis võivad esineda digitaalses ekspertiisis. Nimelt viitavad erinevad uuringud asjaolule, et ekspertiisis tuleb ette vigu, mis on mõnikord tingitud eksperdi eelarvamusest. Autor viitas erinevatele uuringutele ning katsetele, mis on tuvastanud, et ka digitaalses ekspertiisis võib esineda taolisi eelarvamusi. Autori hinnangul on võimalik eksperdi eelarvamusi vähendada, kui kontrollida, et kontekstuaalne informatsioon, mis eksperdile antakse, piirdub ainult ekspertiisiks vajaliku informatsiooniga ning on võimalikult neutraalne ning võimaluse korral ei viita kellegi süüle või süütusele.

Töö viimases peatükis andis autor ülevaate inimeste kogemustest, kes tegelevad antud temaatikaga. Erinevad õiguspraktikud räägivad oma kokkupuutumistest digitaalsete tõendite võltsimisega ning andsid hinnangu koolitamise vajalikkuse osas.

The Reliability of Digital Evidence

Abstract

There is no doubt about the fact that the world we live in is becoming more and more digital. There are examples of this all around us. When we work out, we wear smartwatches, our pockets hold our smartphones and there are numerous new gadgets being released by tech companies almost monthly. Many digital appliances have also proven to be a great source of information. Different technical details can offer us some notion about the behaviour and movement of its users that can then be used in a court of law as proof. Due to the vast range of appliances used by people, it can be concluded that there is a wide array of information that these appliances can generate. This information can be used as evidence - digital evidence[128] to be precise.

It is often noted that it is quite difficult to give a strict definition to the concept of digital evidence due to the fast development of technology. This does not mean that there have not been attempts to give a definition. Eoghan Casey, a well known expert on digital forensics, has defined digital evidence as "any data stored or transmitted using a computer that support or refute a theory of how an offence occurred or that address critical elements of the offence such as intent or alibi." Due to the fast growing nature of technology, the amount of digital evidence in different proceedings is becoming more and more notable. It is also important to keep in mind that these proceedings are not always criminal in their nature. Digital evidence is used as a source of evidence in intellectual property claims, labour disputes, industrial espionage and even civil proceedings.

The vast and increasing use of this type of evidence inevitably raises the question about its reliability and the problems it may face. In order to understand if such questions are justified the author of this paper analyses different academic papers and works as well as notable court cases and statistics surrounding this topic. The author has also conducted interviews with some experts whose profession is closely related to the topic of digital evidence in Estonia, in order to illustrate what kind of obstacles and problems these people face in their area of expertise.

[128] Also known as electronic evidence or e-evidence.

To offer the reader a clear overview, this paper is divided into three separate parts. The first part of this paper gives an overview about the essence of digital evidence and digital forensics, the past and future of said topics and the notion of chain of custody in digital forensics. The second part of this paper focuses on the reliability of digital evidence and digital forensics. The reader will have an overview of the general trustworthiness of digital evidence as well as anti-forensic tools and forgery of digital evidence, human error and bias in digital forensics. The final part of this paper focuses on interviews conducted by the author which give an overview about the experience of Estonian legal practitioners. Lastly the author has offered some recommendations. The more detailed descriptions of all three parts are as follows.

The first part of this paper is divided into four subchapters. Firstly, the author of this paper explains how this topic is regulated in the Estonian Code of Criminal Procedure. It is important to note that at the time of writing this paper, Estonia does not have a special regulation concerning digital evidence. Both the Ministry of Justice and the Chancellor of Justice have pointed out that special regulation concerning the use and collection of digital evidence should be under consideration. It is important to note that digital evidence can be a valuable source of information. Not only can it give information about the crime that has been committed, it can offer information about the user of the appliance as well. For instance, in the 1996 murder case of Sharon Lopatka digital evidence was able to give much needed information about the unconventional interests of the murder victim.

Secondly, the author sheds light on the history of digital forensics and the use of digital evidence. The reader will get an overview about the beginning and growth of digital forensics and digital evidence. The author introduces the first book that details crimes committed with the help of computers and the information such crimes can produce. This book is called “Crime by Computer” and it is written by Donn Parker. This book captured the interest of the United States Federal Bureau of Investigations and the Ministry of Defence. These agencies foresaw the potential for such crimes and created the first organisation devoted to digital forensics. Experts understood the potential growth of cybercrime and the need for digital forensics and thus this area of forensics continued to grow and develop further. The need for further training of police officers and experts was also recognized. Even in more modern settings, statistical data verifies that digital forensics is a forensic practice that is still

growing. Interpol has estimated that the digital forensics market grows about 15,9% every year.

Thirdly, the author explains the concept of a digital chain of custody and why it is necessary to maintain said concept. Different countries have different rules for evidence collection and admissibility. For instance in the Russian Federation it is stated that the gathering of evidence should be done under the supervision of two witnesses who can later testify about the legality of the collection process. In Nigeria, the evidence has to be relevant to the case, meaning it is possible to still use the evidence, even if the means to obtain it were illegal. For instance, in the United States evidence must be collected in accordance with the law.

These kinds of different rules can be an obstacle as it can raise suspicions about which countries maintain the digital chain of custody and which countries do not. This in turn can create doubts about the quality of the evidence received in cases where cooperation between different countries is needed.

The digital chain of custody is a concept in which the whole process of evidence collection and preservation is well documented. The main goal of this principle is to ensure the authenticity, originality and reliability of the digital evidence that has been collected. If the digital evidence has been collected in such a way, there is a lower chance that the argument of reliability of the digital evidence used will be brought up in a court of law. This in time can save valuable time and other resources that would be wasted spending on needless argumentation in court.

Legal literature has highlighted that many laws in different countries have been adopted before the birth of digital evidence and have remained unchanged when it comes to this topic. This means that in many countries there is a possible lack of legislation regarding this concept. It can be concluded then that there is a general insufficiency of unified rules that could improve the quality and trustworthiness of digital evidence. The author believes that unified rules regarding collection and preservation of digital evidence could lead to a higher quality of digital evidence and more efficient court proceedings as well as better international cooperation.

The fourth and last subchapter focuses on the future of digital evidence and digital forensics. This subchapter firstly highlights the growth of technology by giving the reader an overview of different statistical data. This kind of growth inevitably leads to the introduction of new gadgets. Although this is great news for the user, this is becoming an increasingly difficult issue in digital forensics.

Legal literature draws attention to the fact that although the growth of digital forensics has been relatively fast, it is still quite difficult to make breakthroughs in this field. Different aspects about the quick development of technology cause digital forensics some problems. For instance numerous different file formats can be an obstacle when it comes to creating unified tools. The wide use of cryptography and copious amounts of data are also some of the issues that digital forensics faces. This, of course, does not mean that there are no new future directions for digital forensics. There have been multiple advancements and innovative ideas created by experts of this field.

For instance, digital forensics experts have proposed an idea of forensic triage for smartphones to be available on the scene of the crime. Legal literature has also noted that artificial intelligence can also be used to further develop digital forensics as well as cloud forensics. There is also room for development when it comes to digital evidence. For instance, the European Union is working towards a second additional protocol to the Budapest Convention, which is an international cybercrime convention. Additionally, in 2019 the negotiations regarding the use of digital evidence between the European Union and The United States started and, at the time of writing this paper, are still ongoing. This means that there are numerous changes happening in the future. Both in the field of digital forensics and digital evidence.

The second part of this paper focuses on some of the aspects that can affect the reliability of digital evidence and digital forensics. This part of the paper is divided into four separate subchapters that all discuss different features that influence the reliability of both digital evidence and digital forensics.

The first subchapter details different issues that can influence the reliability of digital evidence. For instance, the author sheds light on the fact that due to the rapid development of technology, digital forensics experts may face situations that they have never seen before and

this can lead them to make false conclusions. Another aspect worthy of consideration is the short term that many digital forensics tools are being tested out and bugs in the software that can create experts to make false assumptions. Digital forensics experts have also pointed out that there are no unified criteria or rules for experts to give a fair assessment about the reliability of their findings. If such criteria were to exist, judges could better assess the value of the digital evidence presented to them.

Secondly, the author has shed light on anti-forensics software and the topic of forgery in digital evidence and digital forensics. There is a growing number of cybercrimes being committed and there is an increase of digital forensics being used. This means that people who are trying to evade the law need to come up with tools that suppress the ability to collect digital evidence against them. These are called anti-forensic tools and the primary goal for these tools is to mislead the experts, hide the fact that some sort of occurrence has happened and to disrupt the gathering of digital evidence. These kinds of tools, if they go unnoticed, can seriously affect the digital evidence that is being analysed. This can also, in turn, affect the conclusions that the expert makes about the digital evidence in question.

Another way that someone might try to manipulate digital evidence, is forgery. One of the most simple ways to forge digital evidence is the attempt to change the contents of a file and then submit it to the court. Legal literature has stated that these attempts are rare but they are on the rise. It is also possible that people will try to create fictional files that they then try to submit to evidence. The author of this paper also explains how simple it is to create a false digital alibi, that can lead investigators to make false conclusions. Thus the author has shed light on the fact that digital evidence forgery can be quite easily achieved and oftentimes it does not require extensive computer knowledge.

In the third subchapter, the author brings out errors that are caused by human experts. Firstly the author of this paper points out that it is possible that some experts lack in their knowledge of digital forensics. The author brings out an example of a known case about digital forensics, where the experts gave misleading information. Legal literature also points out that it is important for a digital forensics expert to know and recognize the limitations of their knowledge. This subchapter also points out the need for standardised schooling and sheds light on some other cases where the errors made by digital forensics experts have caused negative consequences.

The final subchapter in this part of the paper highlights bias as a potential threat to the objectivity of digital evidence. Different studies show that bias exists in many different forensic investigations and exaggerated forensic testimonies have caused a number of false convictions. There are studies that suggest that bias exists in digital forensics as well and the contextual information that is given to experts can influence their decision making process. Due to the fact that digital forensics often requires more contextual information than more "traditional" forensic practices, it can be concluded that there is a need for discussion regarding this topic.

The final part of this paper focuses on interviews with different legal practitioners - lawyers, prosecutors and a judge. The interviewees give some insight about their experiences with digital evidence and their opinions regarding this topic. This gives the reader a chance to better understand the experiences that legal practitioners have in the Estonian judicial system. The final part also includes conclusions that the author has made about the interviews conducted and some recommendations the author has made regarding the topic of digital evidence and digital forensics.

Kasutatud kirjandus

1. Browning, J.G. Angelo, L. „New sources of evidence from the internet of things.” Texas Bar Journal. Vol 82, 2019.

2. Casey, E. „Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet” Elsevier Inc, 2012.

3. Casey, E. „Error, Uncertainty and Loss in Digital Evidence.”International Journal of Digital Evidence, 2002.

4. Caviglione, L. Mazurczyk, W. Wendzel, S. „The Future of Digital Forensics: Challenges and the Road Ahead“ IEEE Security and Privacy Magazine, 2017.

5. De Santis, A. Castiglione, A. Cattaneo, G. De Maio, G. Ianulardo, M. „Automated Construction of a False Digital Alibi" 2011.

6. Dokko, J. Shin, M. „A Digital Forensic Investigation and Verification Model for Industrial Espionage” Digital Forensics and Cyber Crime, 2019.

7. Doyle, A.C „The Return of Sherlock Holmes” George Newnes Ltd., 1905.

8. Dror, I.E, Hampikian, G. „Subjectivity and bias in forensic DNA mixture interpretation” Science and Justice 51, 2011.

9. Endicott-Popovsky, A. E . „Digital Evidence Education in Schools of Law," Journal of Digital Forensics, Security and Law: Vol. 7, 2012

10. Garfinkel, S.L. „Anti-forensics: Techniques, detection and countermeasures” 2015.

11. Garrett, B.L, Neufeld, P.J. „Invalid Forensic Science Testimony and Wrongful Convictions” Virginia Law Review, 2009.

12. Horsman, G „ACPO principles for digital evidence: Time for an update?” Forensic Science International: Reports. Volume 2, 2020.

13. Horsman, G „Part 2:- quality assurance mechanisms for digital forensic investigations: Knowledge sharing and the Capsule of Digital Evidence (CODE)” Forensic Science International: Reports. Volume 2, 2020.

14. Horsman, G. Sunde, N. „Part 1: The need for peer review in digital forensics”. Forensic Science International: Digital Investigation, Volume 35, 2020.

15. Horsman, G. Sunde, N. Part 1: The need for peer review in digital forensics, Forensic Science International: Digital Investigation, Volume 35, 2020.

16. Kasper, A. Laurits, E. ,,Challenges in Collecting Digital Evidence: A Legal Perspective", Springer, 2016.

17. Laptev, P. ,,Digital Forensics view from the Estonian Forensic Science Institute" Estonian Forensic Science Institute. Cybercrime forensics & digital evidence, 2014.

18. Laurits, E. ,,Mõned probleemid arvutisüsteemi läbiotsimisel" Kohtute aastaraamat, Riigikohus, 2015.

19. M.N.O Sadiku, A.E. Shadare, S.M. Musa ,,Digital Chain of Custody" International Journals of Advanced Research in Computer Science and Software Engineering. Volume 7, 2017.

20. Mason, S. Seng, D. ,,Electronic Evidence" University of London Press, 2017.

21. Mislan, R.P, Casey, E. Kessler, G.C. ,,The growing need for on-scene triage of mobile devices" Digital Investigation 6, 2010.

22. Mitchell, F ,,The Use of Artificial Intelligence in Digital Forensics: an Introduction" Digital Evidence and Electronic Signature Law Review, 2010.

23. Mohammad, N. Fayyad-Kazan, H. Saab, M. ,,Anti-Forensics: The Tampering of Media" International Journal on Recent and Innovation Trends in Computing and Communication, 2020.

24. Pollitt, M. ,,A History of Digital Forensics". International Conference on Digital Forensics, 2010.

25. Reedy, P. ,,Interpol review of digital evidence 2016 - 2019" Forensic Science International: Synergy Vo 2, 2020, lk 608.

26. Schneider, J. Wolf, J. Freiling, F. ,,Tampering with Digital Evidence is Hard: The Case of Main Memory Images" Forensic Science International: Digital Investigations, Volume 32, 2020.

27. Skulrattanakulchai, A. ,,Charles Babbage, A Man before His Time" 2017.

28. Smalarz, L. Madon, S. Yang, Y. Guyll, M. Buck, S. ,,The perfect match: do criminal stereotypes bias forensic evidence analysis?" Law and Human Behaviour, 40, 2016.

29. Smit, N.M, Morgan, R.M, Lagnado, D.A ,,A systematic analysis of misleading evidence in unsafe rulings in England and Wales" Science & Justice, Volume 58, 2018.

30. Stoykova, R. ,,Digital evidence: Unaddressed threats to fairness and the presumption of innocence" Computer Law & Security Review, Volume 42, 2021.

31. Sunde, N, Dror, I.E. ,,Cognitive and human factors in digital forensics: Problems, challenges, and the way forward" Digital Investigation Volume 29, 2019.

32. Sunde, N. ,,Non-technical Sources of Errors When Handling Digital Evidence within a Criminal Investigation", 2017.

33. Sunde, N. Dror, I.E. ,,A hierarchy of expert performance (HEP) applied to digital forensics: Reliability and biasability in digital forensics decision making" Forensic Science International: Digital Investigation, Volume 37, 2021.

34. Vacca, John R. Computer Forensics: Computer Crime Scene Investigation. Charles River Media Inc. Massachusetts, 2002.

35. Van Buskirk, E. Liu, V.T ,,Digital evidence: challenging the presumption of reliability" Journal of Digital Forensic Practice, 2006.

36. Van Buskirk, E. Liu, V.T ,,Digital evidence: challenging the presumption of reliability" Journal of Digital Forensic Practice, 2006.

Kasutatud õigusaktid ja kohtupraktika

1. Kriminaalmenetluseseadustik - RT I, 22.12.2021, 45
2. The Nigerian Evidence Act - 2011
3. Tsiviilkohtumenetluse seadustik - RT I, 22.12.2021, 23
4. Уголовно-процессуальный Кодекс Российской Федерации от 18.12.2001 N 174-ФЗ

Kastutatud kohtupraktika

1. EIKo 12.07.1988, 10862/84, Schenk vs Šveits
2. Riigikohtu lahend 1-09-4486 p 40, 22.05.2020
3. *Silverthorne Lumber Co. v. United States*
4. Tartu Maakohtu kohtuotsus nr 1-20-4575, 21.04.2021
5. *Tassone v Kirkham* (2014) SADC 134

Kasutatud muud allikad

1. Cellebrite. „2021 Digital Intelligence Benchmark Report" https://cellebrite.com/en/digital-intelligence-benchmark-report-2021
2. Council of the European Union „Access to e-evidence: Council authorises member states to sign international agreement", 2022. https://www.consilium.europa.eu/en/press/press-releases/2022/04/05/access-to-e-evidence-council-authorises-member-states-to-sign-international-agreement/
3. Council of the European Union „Better access to e-evidence to fight crime", 2022. https://www.consilium.europa.eu/en/policies/e-evidence/
4. Council of the European Union „Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence„ Explanatory Report. https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b
5. European Commission „Frequently Asked Questions: New EU rules to obtain electronic evidence." https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
6. European Commission „Frequently Asked Questions: New EU rules to obtain electronic evidence." https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
7. European Commission „Frequently Asked Questions: New EU rules to obtain electronic evidence." https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
8. European Commission. „FAQ: New EU rules to obtain electronic evidence" 2018. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345
9. Europol „SIRIUS Project" https://www.europol.europa.eu/operations-services-innovation/sirius-project
10. Europol. „SIRIUS: EU Digital Evidence Situation Report 2nd Annual Report". 2020. https://www.ejn-crimjust.europa.eu/ejnupload/DynamicPages/SIRIUS_REPORT_20.pdf
11. Gillum, J. Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned. ProPublica, 2019 https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned
12. Human Rights Watch „Letter to US Department of Justice About Child Protection System Software", 2019. https://www.hrw.org/news/2019/04/03/letter-us-department-justice-about-child-protection-system-software
13. Interpol. „Cybercrime" https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
14. Interpol. „Digital Forensics" https://www.interpol.int/How-we-work/Innovation/Digital-forensics

15. Justiitsministeerium „Kriminaalmenetlusõiguse revisjoni lähteülesanne“ Tallinn, 2015. 2015 https://www.just.ee/sites/www.just.ee/files/kriminaalmenetluse_revisjoni_lahteulesanne.pdf
16. Justiitsministeerium „Küberkuritegude statistika“ https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/kuberkuriteod.html
17. Justiitsministeerium „Kuritegevus Eestis 2021“ https://www.kriminaalpoliitika.ee/kuritegevus2021/arvutikuriteod_page.html
18. Justiitsministeerium. „Kuritegevus Eestis“ https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/
19. Justiitsministeerium. „Süüteomenetlus muutub digitaalseks ning asjatut bürokraatiat vältivaks”. 2021. https://www.just.ee/uudised/suuteomenetlus-muutub-digitaalseks-ning-asjatut-burokraatiat-valtivaks
20. National Police Chiefs' Council „Digital Forensic Science Strategy” 2020. https://www.npcc.police.uk/Digital%20Forensic%20Science%20Strategy%202020.pdf
21. Õiguskantsleri arvamus eelnõule: kriminaalmenetluse seadustiku jt seaduste muutmise eelnõu (295 SE), 2012. https://www.oiguskantsler.ee/et/seisukohad/seisukoht/arvamus-eeln%C3%B5ule-kriminaalmenetluse-seadustiku-jt-seaduste-muutmise-eeln%C3%B5u-295
22. Sava, J. A. „Information technology (IT) worldwide spending from 2005 to 2023” Statista, 2022. https://www.statista.com/statistics/203935/overall-it-spending-worldwide/
23. Statista „Number of consumer cloud-based service users worldwide in 2013 and 2018”, 2014. https://www.statista.com/statistics/321215/global-consumer-cloud-computing-users/
24. The Guardian. Bowcott, O. „London rape trial collapses after phone images undermine case” 15.01.2018 https://www.theguardian.com/law/2018/jan/15/london-rape-trial-collapses-after-phone-images-undermine-case
25. The Guardian. Bowcott, O. „Police mishandling digital evidence, forensic experts warn.” https://amp.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn
26. The Guardian. Dodd, V. „MET to review all ongoing rape cases after second trial collapses” 19.12.2017. https://www.theguardian.com/uk-news/2017/dec/19/met-to-review-all-ongoing-cases-after-second-trial-collapses
27. World Intellectual Property Organization. WIPO Proof https://www.wipo.int/wipoproof/en/