

Sisekaitseakadeemia
Politsei-ja piirivalvekolledž

Marit Alas

DIGITAALSETE TÕENDITE KOGUMINE JA KÄITLEMINE INTERNETIS
TOIMEPANDUD AUTORIÕIGUSTE RIKKUMISTE MENETLEMISEL

Lõputöö

Juhendaja:
Tanel Järvet, MA
Kaasjuhendaja:
Kati Jehe, MA

Muraste 2013

ANNOTATSIOON

SISEKAITSEAKADEEMIA

Kolledž: Politsei- ja piirivalvekolledž	Kuu ja aasta: mai 2013. aasta
Töö pealkiri: DIGITAALSETE TÕENDITE KOGUMINE JA KÄITLEMINE INTERNETIS TOIMEPANDUD AUTORIÕIGUSTE RIKKUMISTE MENETLEMISEL	
Töö autor: Olen nõus oma lõputöö kättesaadavaks tegemisega digitaalses keskkonnas. Allkiri:	
<p>Lühikokkuvõte: Tänapäeval, kiiresti muutuv maailmas, on õiguskaitseorganitel üha suuremaks probleemiks kuritegevus digitaalses keskkonnas – internetis. Käesoleva lõputöö eesmärk oli anda teoreetiline ülevaade internetis toimepandud autoriõiguste rikkumiste menetlemisel digitaalsete tõendite kogumisest, analüüsida Eesti menetluspraktikat, mille põhjal teha ettepanekuid digitaalsete tõendite kogumise parendamiseks. Tegemist on empiirilise tööga ja töö maht on 44 lehekülge. Lõputöö esimeses osas analüüsis autor Eesti ja USA digitaaltõendite kogumise ja käitlemise juhendeid, maailma suurimat internetipiraatluse kaasust Megaupload ja Eesti ainsat Ringkonnakohtu otsust antud teemal. Töö teises osas viidi läbi uuring tuvastamiseks digitaaltõendite kogumisega esinevaid probleeme. Selleks analüüsis autor prokuratuuri loal lõpetatud 14 autoriõiguste rikkumistega seotud kriminaalasja ja viis läbi ekspertintervjuu nelja kriminaalmenetlejaga. Peamiste probleemidena saab välja tuua menetluse pikkuse, mis tuleneb nii välisriikidest õigusabipalvetele vastamise aeglusest kui ka ressursi puudusest. Kuna tegemist on spetsiifilise valdkonnaga, vajavad menetlejad IT alaseid teadmisi. Ideaalne oleks, kui menetleja omaks IT – alast haridust. Lisaks tuleks läbi viia IT alaseid koolitusi, et hoida menetlejaid kursis uute võimalustega näiteks võrk, tuletada meelde digitaaltõendite kogumise põhimõtted, analüüsida uusi kohtulahendeid või tutvustada teiste riikide seadusi õigusabipalvete osas. Menetlejate koormuse vähendamiseks võiksid õiguste valdajad proovida rohkem ettevõtetega suhelda. FBI ja USSS'i juhendites on välja toodud, milliseid digitaaltõendeid võib leida erinevate kuriteoliikide puhul ning näidisküsimused menetlusosalistele esitamiseks. Ka Eesti võiks kaaluda erinevatele kuriteoliikide omaste digitaaltõendite näidiskirja ja -küsimustiku lisamist IT kuritegude menetlemise käsiraamatusse.</p>	
Võtmesõnad: autoriõigus, internet, digitaaltõend, piraatkoopia, intellektuaalomand	
Võõrkeelsed võtmesõnad: copy right, internet, digital evidence, pirate copy, intellectual property	
Säilitamise koht: Sisekaitseakadeemia Politsei – ja piirivalvekolledži raamatukogu	
Kaitsmisele lubatud	
Kolledži direktor:	Allkiri:
Vastab lõputöö nõuetele	
Juhendaja:	Allkiri:
Kaasjuhendaja:	Allkiri:

SISUKORD

ANNOTATSIOON.....	2
SISUKORD	3
MÕISTETE JA LÜHENDITE SELGITUSED	4
SISSEJUHATUS	6
1. INTERNETIS TOIMEPANDAVAD AUTORIÕIGUSTEGA SEOTUD KURITEOD JA MENETLUSE ERISUSED	8
1.1. Autoriõigus ja selle rikkumisega seotud kriminaalvastutus.....	10
1.2. Kriminaalmenetluse erisused digitaalsete tõendite kogumisel	14
1.3. Digitaalsete tõendite kogumine ja käitlemine USA's	22
2. DIGITAALSETE TÕENDITE KOGUMINE AUTORIÕIGUSTEGA SEOTUD KRIMINAALASJADES EESTIS	28
2.1. Kriminaalasjade toimikute analüüs.....	28
2.2. Ekspertintervjuud autoriõiguste rikkumiste kriminaalmenetlejatega	32
2.3. Ettepanekud digitaalsete tõendite kogumise ja käitlemise parendamiseks.....	37
KOKKUVÕTE	40
SUMMARY	42
VIIDATUD ALLIKATE LOETELU	43
LISA 1. PÕHJA PREFEKTUURI KRIMINAALTOIMIKUTE VAATLUS	45
LISA 2. EKSPERTINTERVJUU IDA PREFEKTUURI MENETELJAGA	48
LISA 3. EKSPERTINTERVJUU LÕUNA PREFEKTUURI MENETELJAGA	49
LISA 4. EKSPERTINTERVJUU PÕHJA PREFEKTUURI MENETLEJAGA.....	52
LISA 5. EKSPERTINTERVJUU LÄÄNE PREFEKTUURI MENETLEJAGA	55

MÕISTETE JA LÜHENDITE SELGITUSED

AutÕS – Autoriõiguse seadus.

CART – *Computer Analysis Response Team* (arvuti analüüsi reageerimise meeskond)

Cookies – veebiserveri loodud kasutaja mälus talletatav kirje, mille poole veebiserver pöördub edasise suhtluse hõlbustamiseks.¹

FBI – *Federal Bureau of Investigation* (Föderaalne juurdlusbüroo).

FTP – File Transfer Protocol (Faili vahetamise protokoll).

EFÜ – Eesti Fonogrammitootjate Ühing.

Ex officio – Enamus allikaid defineerib *ex officio* mõistet „ametikohtuslikult, ameti ülesande korras“² või „ameti poolest, ameti tõttu“ (erikorraldust saamata)³. Seega tuleb autoriõiguse rikkumise korral menetlust alustada ehk menetlejal on kohustus alustada menetlust vastava käsuta või väljastpoolt tuleva nõudmiseta.

EKEI – Eesti Kohtuekspertiisi Instituut.

IO – Intellektuaalomand.

IP – *Internet protocol adress* (Internetiaadress).

IT – Infotehnoloogia.

ISP – *Internet Service Provider* (Interneti teenusepakkuja).

KarS – Karistusseadustik.

KrMS – Kriminaalmenetluse seadustik.

Piraatkoopia - AutÕS §80-1 tähenduses teose või autoriõigusega kaasnevate õiguste – objekti mis tahes vormis ilma teose autori, tema õiguste omaja või autoriõigusega kaasnevate õiguste omaja loata mis tahes riigis reprodutseeritud koopia ühes vastava pakendiga või ilma sellela.⁴

PPA- Politsei- ja Piirivalveamet.

RCFL – *Regional Computer Forensics Laboratory* (Regionaalne arvuti analüüsi laboratoorium)

Räsiväärtus - ehk räsi on vastava algoritmi (*hash function*) abil tekstistringist genereeritud fikseeritud pikkusega arv. Räsi on oluliselt väiksem kui tekst ise ja sobiva algoritmi

¹ Phare mestiprojekt EE 03 IB JH 04, „Infotehnoloogiakuritegude menetlemise käsiraamat“, 2001, lk 40.

² Maurer, K., „Õigusleksikon“, Tallinn: Interlex kirjastus, 2000, lk 73.

³ „Väike entsüklopeedia“, Tallinn: Eesti entsüklopeedia kirjastuse AS, 2006, lk 215.

⁴ Autoriõiguse seadus, 11.11.1992, jõustunud 12.12.1992 - RT - I 1992, 49, 615, §80-1.

kasutamine tagab selle, et mingist teisest stringist sama räsiväärtuse saamine on äärmiselt väikese tõenäosusega.⁵

Steganograafia kasutamine – info peidetakse teiste failide sisse.⁶

Swap files – fail, millesse programm või operatsioonisüsteem paigutab ajutiselt andmeid, et vabastada operatiivmälu.⁷

Torrent – väike fail, mis toimib kasutajalt – kasutajale failivahetussüsteemil. Kui kasutaja hakkab jagajalt faili alla laadima, siis temani jõudnud failiosad antakse kohe teistele jagamiseks, sellise tegevusega saavutatakse failide allalaadimisel suurem kiirus.⁸

USSS – *United States Secret Service* (Ühendriikide salateenistus).

⁵ Vallaste, H. „E-teatmik“, <<http://www.vallaste.ee/index.htm?Type=UserId&otsing=726>> (28.03.2013).

⁶ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *supra nota*, lk 40.

⁷ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 40.

⁸ Tõnis L. „Arvutiabi“ <<http://web.zone.ee/abi2/BitTorrent/bitTorrent.html#BitTorrent>> (31.03.2013).

SISSEJUHATUS

„Kõik inimesed on autorid, ainult suurem osa ei tea seda.“

Heiki Pisuke (Tartu Ülikooli professor)

Tänapäeval, kiiresti muutuv maailmas, on õiguskaitseorganitel üha suuremaks probleemiks kuritegevus digitaalses keskkonnas – internetis. Eestis kasutab internetti ca 75% elanikkonnast ja viimase kümne aastaga on interneti kasutamine kogu maailmas suurenenud 260%.⁹ Internet on kiire, mugav ja tekitab anonüümsuse tunde. Autoriõiguste rikkumiste rohkus internetis tuleneb interneti kasutajate intellektuaalomandialase teadlikkuse puudulikkusest ning hoolimatusest oma kaaskodanike omandi suhtes. Levinud on valearusaam, et kõik mis on internetis, on lubatud. Kõik internetti üleslaetud teosed on kaitstud autoriõigusega.

Autoriõigusega seonduv on viimasel ajal väga aktuaalne, eelkõige seadusloome tõttu. 2011. aastal asus Tartu Ülikooli dotsent Aleksei Kelli juhitud töörühm välja töötama süsteemset, selget ja kasutajasõbralikku seadustikku, mis sobiks hästi Eesti eraõiguslikule maastikule.¹⁰ Autoriõiguse temaatika on viimasel ajal taas leidnud meedias palju kajastamist, seda internetikeskkonna Megaupload'i kohtuasja pärast USA's. Teatavasti on üheks süüdistatavaks Eesti kodanik Andrus Nõmm.

Käesoleva lõputöö eesmärgiks on anda teoreetiline ülevaade internetis toimepandud autoriõiguste rikkumiste menetlemisel digitaalsete tõendite kogumisest ja analüüsida Eesti menetluspraktikat, mille põhjal teha ettepanekuid digitaalsete tõendite kogumise parendamiseks.

Lõputöös on kasutatud õigusakte, teooriakirjandust, seaduste kommenteeritud väljaandeid, ekspertide ettekandeid, juhendeid ja käsiraamatuid, mida kasutatakse nii Eestis kui ka USA's.

⁹ „Internet World Stats“ <<http://www.internetworldstats.com/stats4.htm>> (05.04.2012).

¹⁰ Michal, K. „Intellektuaalomandi reformist“ <http://juridica.ee/get_doc.php?id=1845> (01.12.2013).

Käesoleva lõputöö uurimisülesanneteks on:

- 1) anda ülevaade internetis toimepandud autoriõiguste rikkumisega seotud kuritegudest;
- 2) anda ülevaade teooria kirjanduse põhjal digitaaltõendite kogumise ja käitlemise kohta autoriõiguste rikkumiste korral;
- 3) analüüsida Eesti menetluspraktikat digitaaltõendite kogumisel ja käitlemisel autoriõigustega seotud kriminaalmenetlustes;
- 4) teha ettepanekuid autoriõiguste rikkumiste kriminaalmenetluses digitõendite kogumise ja käitlemise parendamiseks.

Lõputöö esimeses osas selgitatakse välja autoriõiguste rikkumiste kuritegude koosseisud, mis töö kontekstis omavad olulisemat tähtsust. Antakse ülevaade autoriõiguste vastaste kuritegude menetlemisel kogutavate digitaaltõendite kogumisele ja käitlemisele esitatavatest nõuetest Eestis ja USA's.

Töö teises osas analüüsib autor internetis toimepandud autoriõiguste rikkumiste kriminaalasjade toimikuid, mis on prokuratuuri loal lõpetatud. Samuti intervjuerib lõputöö autor igast prefektuurist ühte autoriõiguste rikkumistega tegelevat kriminaalmenetlejat. Selles osas teeb autor ka ettepanekuid digitaalsete tõendite kogumise ja käitlemise parendamiseks.

Tegemist on empiirilise uurimistööga, milles on kasutatud teoreetilist uurimismeetodit, mis hõlmab endas analüüsi ja sünteesi, üldistamist ning induksiooni ehk üksikjuhtudest või faktidest üldistuste ja seaduspärasuste tuletamist. Samuti on kasutatud võrdlusmeetodit.

Teema on nii uudne, et Eestis ei ole veel ühtegi Riigikohtu lahendit digitaalpiraatluse kohta. Antud töös analüüsib autor 01.06.2012 Tallinna Ringkonnakohtu otsust Eesti esimese *torrent* kaasuse kohta, mis on läbinud üldmenetluse.

1. INTERNETIS TOIMEPANDAVAD AUTORIÕIGUSTEGA SEOTUD KURITEOD JA MENETLUSE ERISUSED

Internetis toimepandud autoriõiguste rikkumiste puhul on kõige olulisem teoste reprodutseerimine ja üldsusele kättesaadavaks tegemine ilma autori loata. Digitaalkeskkonnas toimepandud autoriõiguste rikkumiste tuvastamisel on keeruline ärilise eesmärgi tõendamine. Arvutiprogrammide puhul on seadusandja selgesõnaliselt sätestanud karistuse mitte ainult kasutamise, vaid ka omamise eest, kuid muude teoste nt muusika ja filmide puhul on Eestis tavaline, et piraatkoopia laetakse internetti üles ja üleslaadija ei saa sellest mingit kasu. Seega on Eesti autoriõiguste rikkumise toimepanijad pigem kaasaegsed „Robin Hood’id“ kui tegelikul viisil raha teenivad inimesed.¹¹

Kuigi Eestis autoriõiguste rikkumiste toimepanijad oma teoga raha ei teeni, siis näiteks tuntud internetilehekülje www.megaupload.com loojad teenisid 5 aasta vältel, 175 miljonit dollarit, tekitades autoriõiguste omanikele kahju üle poole miljardi dollari. Menetluse käigus esitati süüdistus peale lehekülje omaniku Kim Dotcom’i veel kuuele inimesele erinevatest riikidest. Nende seas oli ka Eesti Vabariigi kodanik Andrus Nõmm, kes tegeles tarkvarade programmeerimisega ja juhtis tarkvaraarendus osakonda.¹² Andrus Nõmm on oma väljaandmise USA’le vaidlustanud Hollandi kohtus.¹³

Antud kaasuses said kõik seitse füüsilist isikut ja veel lisaks kaks korporatsiooni – Megaupload Limited ja Vestor Limited - süüdistuse väljapressimise vandenõus, vandenõus panna toime autoriõiguste rikkumine, vandenõus panna toime rahapesu ja kahes sisulises episoodis autoriõiguste rikkumiste kriminaalsüütegudes. Selliste rikkumiste eest võivad kõik süüdistatavad saada maksimaalselt 20 aastat vangistust väljapressimise vandenõu eest, 5 aastat vangistust autoriõiguste rikkumise vandenõu eest, 20 aastat vangistust rahapesu

¹¹ Kelli, A. „Intellektuaalomandi seadusandluse kodifitseerimisest“, ettekanne seminaril Criminal enforcement of Intellectual Property Rights, 16.03.2012.

¹² Press release <<http://www.info.gov.hk/gia/general/201201/20/P201201200626.htm>> (02.09.2012).

¹³ Tänavsuu, T. „Kim Dotcom’i eestlasest abilist ähvardab Amerikas 55 aastane vangistus“, Eesti Ekspress, 14.03.2013, < <http://www.ekspress.ee/news/paevauudised/eestiuudised/kim-dotcomi-eestlasest-abilist-ahvardab-ameerikas-55-aastane-vangistus.d?id=65816470>> (14.03.2013).

vandenõu eest ja 5 aastat vangistust iga sisulise episoodi eest autoriõigust rikkumiste kriminaalsüüteo.¹⁴

Antud kaasusega seoses väljastati üle 20 läbiotsimismääruse Ameerika Ühendriikides ja kaheksas teises riigis, arestiti vara umbes 50 miljoni dollari ulatuses ja suunatud lingid, kus Megauploadil olid serverid: Ashburn, Va., Washington, D.C., Hollandis ja Kanadas. Alexandria Ringkonnakohus määras 18 domeeni nime külmutamise, mis olid seotud väidetava „Mega vandenõuga“.¹⁵

Megaupload'i juurdluse algatas ja viis läbi FBI (*Federal Bureau of Investigation* – Föderaalne uurimise büroo) IPR keskus (*Intellectual Property Rights Coordination Center* – Intellektuaalomandi õiguste koordineerimise keskus) Ameerika Ühendriikide Immigratsiooni- ja Tolliameti Sisejulgeoleku uurimisasutuse (*U.S. Immigration and Customs Enforcement's Homeland Security Investigations*) abiga. Abi osutasid veel Uus-Meremaa politsei, Uus-Meremaa Organiseeritud- ja Majanduskuritegude amet (*OFCANZ - Organised and Financial Crime Agency of New Zealand*), Uus-Meremaa Põhiseaduse büroo (*the Crown Law Office of New Zealand*) ja Uus-Meremaa advokatuur (*the office of Solicitor General for New Zealand*). Samuti aitasid Hong - Kongi Toll (*Hong Kong Customs*) ja Hong Kongi Justiitsministerium (*Hong Kong Department of Justice*), Hollandi politsei (*the Netherlands Police Agency*) ja Rotterdami Tõsiste Pettuste ja Keskkonna Kuritegude Prokuratuur (*the Public Prosecutor's Office for Serious Fraud and Environmental Crime in Rotterdam*), Londoni politsei (*London's Metropolitan Police Service*), Saksamaa Föderaalne Kriminaalpolitsei (*Germany's Bundeskriminalamt*) ja Saksamaa Prokuratuur (*German Public Prosecutors*), Kuninglik Kanada Politsei seal hulgas GTA (*Greater Toronto Area*) föderaalse täideviimise osakond ja integreeritud tehnoloogia kuritegude üksus (*the Royal Canadian Mounted Police – Greater Toronto Area Federal Enforcement Section and the Integrated Technological Crime Unit*) ning Kanada Justiitsministeeriumi õigusabi grupp (*the Canadian Department of Justice's International Assistance Group*). Lisaks saadi abi veel Suurbritannialt, Austraalialt ja Filipiinidelt.¹⁶

¹⁴ Press release <<http://www.justice.gov/opa/pr/2012/January/12-crm-074.html>> *supra nota* (02.02.2013).

¹⁵ Press release <<http://www.justice.gov/opa/pr/2012/January/12-crm-074.html>> *ibid* (02.02.2013).

¹⁶ Press release <<http://www.justice.gov/opa/pr/2012/January/12-crm-074.html>> *ibid* (02.02.2013).

Lõputöö käigus vesteldi ka riigiprokurör Eve Olesk'iga, kes tegeleb Eesti õigusabipalvetega. Eve Olesk'i sõnade kohaselt antud kaasuse raames Eestisse õigusabipalvet ei tehtud ning Eesti ainus seos Megaupload'i kaasusega on asjaolu, et üheks süüdistatavaks on Eesti Vabariigi kodanik Andrus Nõmm.

Megaupload'i kaasus oli osa IP töögrupi (*Department of Justice Task Force on Intellectual Property* – Justiitsministeeriumi Intellektuaalomandi töögrupp) jõupingutustest tõkestamiseks intellektuaalomandi varguseid. Advokaat Eric Holder lõi selle töögrupi, et võidelda üha enam kasvavate intellektuaalomandi kuritegudega nii USA's kui ka mujal maailmas. IP töögrupi eesmärgiks on parandada intellektuaalomandi õiguste kaitset läbi kõrgendatud kriminaalkaristuste ja tsiviilhagide. Samuti üritatakse parandada koostööd föderaal-, riigi-, ja kohalikul tasandil, kaasa arvatud tugevdades suhteid peamiste välispartnerite ja USA majanduse juhtidega.¹⁷

1.1. Autoriõigus ja selle rikkumisega seotud kriminaalvastutus

Autoriõigus on originaalteoste autoritele antud õiguste kogum, mis laiemas tähenduses hõlmab ka autoriõigustega kaasnevaid õigusi.¹⁸ Autoriõigus kaitseb intellektuaalomandit ja termin „omand“ viitab juba, et see kuulub teatud isikule ja selle suhtes on võimalik panna toime süütegusid.

Autori õigused on välja toodud autoriõiguse seaduses ja nende rikkumiste vastutus on Karistusseadustikus.

Autoriõiguse seadus

Kuigi 2011. aastal alustas Justiitsministeerium uue autoriõiguse seaduse väljatöötamist, lähtub käesolevas lõputöös autor kehtivast, 12.12.1992. a jõustunud autoriõiguse seadusest.

¹⁷ The United States Department of Justice: Intellectual Property Task Force <<http://www.justice.gov/dag/iptaskforce/>> (02.02.2013)

¹⁸ Autoriõiguse seadus § 1.

Autoriõigus tekib kirjandus-, kunsti- ja teadustöödele nende loomisega ja kehtib 70 aastat peale autori surma.¹⁹ Autoriõiguse seaduse eesmärk on tagada kultuuri järjepidevus ja kultuurisaavutuste kaitse, autoriõigusel põhinevate tootmisharude ja rahvusvahelise kaubanduse areng ning luua autoritele, autoriõigusega kaasnevate õiguste omajatele ning teisele autoriõiguse seaduses nimetatud isikutele soodsad tingimused teoste ja muude kultuurisaavutuste loomiseks ja kasutamiseks.²⁰

Autori õigused jagunevad isiklikeks ja varalisteks õigusteks. Autori isiklike õigusi ei ole võimalik tehingutega üle anda ja need on autorist lahutamatud. Autori isiklikud õigused on.

- 1) õigus teose autorsusele;
- 2) õigus autori nimele;
- 3) õigus teose puutumatusel;
- 4) õigus teoste lisadele;
- 5) õigus autori au ja väärkuse kaitsele;
- 6) õigus teose avalikustamisele;
- 7) õigus teose täiendamisele;
- 8) õigus teos tagasi võtta;
- 9) õigus nõuda autorinime kõrvaldamist.²¹

Kui autori isiklikud õigused peavad tagama autori au ja kuulsuse, siis varaliste õiguste eesmärgiks on tagada tulu saamine teoste kasutamise eest. Autori varalisi õigusi võib müüa või anda luba ehk litsents nende kasutamiseks.²²

Internetikeskkonnas rikutakse peamiselt autori varalisi õigusi: reprodutseerides, levitades, üldsusele edastades ja üldsusele kättesaadavaks tehes autoriõigustega kaitstud teoseid.²³

Käesolevas töös keskendub autor olulisemate varaliste õiguste rikkumiste menetlemisele.

Autori varalised õigused on:

¹⁹ Autoriõiguse seadus §3 ja §38.

²⁰ Autoriõiguse seadus § 1.

²¹ Autoriõiguse seadus §12.

²² Kultuuriministeerium, Autor.ee Intellektuaalomandi infovõrk
<<http://www.autor.ee/est/vasak/autoriõigused/Autoriisiklikud>> (01.03.2013).

²³ Alas, „Autoriõiguste rikkumiste tuvastamine internetis“, *supra nota*, lk 8.

- 1) õigus oma teost kasutada ja saada selle kasutamisest tulu ning lubada ja keelata inimestel oma teose kasutamist. Autoril on õigus lubada ja keelata:
 1. oma teosest koopia tegemine, mis tahes kujul või vormil;
 2. oma teose või selle koopiade levitamine;
 3. oma teose tõlkimine;
 4. oma teose töötlemine;
 5. oma teostest kogumike tegemine;
 6. oma teose avalik esitamine;
 7. oma teose eksponeerimine;
 8. oma teose edastamine;
 9. oma teose üldsusele kättesaadavaks tegemine;
- 2) õigus oma teost rentida varalise või ärilise kasu saamise eesmärgil;
- 3) õigus oma teost laenutada varalise või ärilise kasu saamise eesmärgil;²⁴

Karistusseadustik

Nii nagu kõikide süütegude korral, järgneb ka autoriõiguste rikkumistele (sh internetikeskkonnas) vastutus. Kuritegude koosseisude tunnused ja kohaldatavad sanktsioonid on sätestatud karistusseadustikus, mille 14.ndass peatükki on koondatud intellektuaalse omandi vastased süüteod.²⁵ Autoriõiguste rikkumiste väärtegade kirjeldused ja sanktsioonid on sätestatud autoriõiguse seaduse peatükis 10-1.²⁶

KarS § 219 (autorsuse rikkumine) sätestab võõra isiku teose või teose esituse, samuti võõra leiutise, tööstusdisainilahenduse või mikrolülituse topoloogia oma nimel üldsusele teatavaks tegemise eest karistusena rahalise karistuse või kuni kolmeaastase vangistuse.²⁷

KarS § 222 sätestab sanktsioonina rahalise karistuse või kuni kolmeaastase vangistuse teose või autoriõigustega kaasnevate õiguste objekti reprodutseerimise eest levitamise

²⁴ Autoriõiguse seadus §13.

²⁵ Karistusseadustik, 06.06.2001, jõustunud 01.09.2004, RT – I 2001, 61, 364, ptk 14.

²⁶ Autoriõiguse seadus ptk 10’.

²⁷ Sootak, J., Pikamäe, P., „Karistusseadustiku kommenteeritud väljaanne“ (Tallinn: Juura 2002), lk 600.

eesmärgil ilma teose autori, tema õiguste valdaja või autoriõigustega kaasnevate õiguste valdaja loata.

KarS § 222-1 keskendub arvutiprogrammi valdamise erisusele. Antud paragrahv sätestab sanktsioonina arvutiprogrammi ebaseadusliku füüsilise kasutamise või valdamise st ärilisel eesmärgil rahalise karistuse või kuni kolmeaastase vangistuse.

KarS § 223 näeb karistusena ette rahalise karistuse või kuni üheaastase vanglakaristuse isikule, kes teost või autoriõigustega kaasnevaid objekte ebaseaduslikult avalikult esitab, üldsusele näitab, edastab, taasedastab või teeb kättesaadavaks.

KarS § 224 näeb piraatkoopiaga kauplemise eest karistusena ette rahalise karistuse või kuni kolmeaastase vangistuse. Antud paragrahv lõige kolm sätestab, et kohtul on kohustus konfiskeerida süüteo toimepanemise vahend. Aastal 2007 tunnistati kehtetuks AutÕS § 80-1 piraatkoopiaga kauplemise väärteoprejuditsioon, kuna leiti, et tegemist on tõsise õigusrikkumisega. Varem oli piraatkoopiaga kauplemine karistatav kuriteona ainult sellisel juhul, kui oli tõendatud levitamise eesmärk..²⁸

KarS § 226 sätestab rahalise karistuse või kuni kolmeaastase vangistuse isikule, kes rikub patendi, kasuliku mudeli, kaubamärgi, tööstusdisainilahenduse ja mikrolülituse topoloogia omaniku ainuõiguseid.

Kõik eelpool nimetatud autoriõiguste rikkumiste paragrahvid on koosseisutüübilt formaalsed ja blanketseid. KarS § 222-1 ja § 223 on veel ka alternatiivaktiilsed. Paragrahvide sisustamisel tuleb pöörduda AutÕS poole. Kõikide autoriõiguste rikkumiste puhul on koosseis täidetud vähemalt kaudse tahtlusega. Kuigi tavaliselt sõna „eesmärk“ näitab, et tegu on toime pandud kavatselt, siis KarS § 222 ja § 222-1 puhul loetakse süüteo koosseis täidetuks ka kaudse tahtlusega.²⁹

²⁸ Sootak, Pikamäe, „Karistusseadustike kommenteeritud väljaanne“, *ibid*, lk 613.

²⁹ Sootak, Pikamäe, „Karistusseadustiku kommenteeritud väljaanne“, *ibid*, lk 609.

1.2. Kriminaalmenetluse erisused digitaalsete tõendite kogumisel

Eesti õigusruumis on võistlev kriminaalmenetlus, kus põhirõhk on asetatud kohtumenetlusele, mille käigus vastaspoolled püüavad nende poolt kogutud tõenditele tuginedes veenda kohut oma versiooni õigsuses.³⁰ Seega on võistlev kriminaalmenetlus, menetlus, milles tõendeid koguvad menetluse pooled ja kohtunik üksnes juhib kohtu vaidlust.³¹ Seepärast on võistlevas kriminaalmenetluses tõendid otsustava tähtsusega. Intellektuaalomandi õiguse rikkumise korral nagu teiste süütegu puhul alustatakse tõendite kogumist peale kriminaalmenetluse alustamist.

Kriminaalmenetlust alustatakse esimese uurimis- või menetlustoiminguga.³² Teoreetiliselt on autoriõiguste rikkumiste korral võimalik alustada menetlust ka *ex officio*. Seega on menetlejal võimalus internetis info liikumist jälgides ise tuvastada autoriõiguste rikkumisi ja neid märgates on kohustus alustada kriminaalmenetlus ilma vastava käsuta. Tuginedes Politsei- ja Piirivalveameti Põhja prefektuuri kriminaalbüroo majanduskuritegude talituse kogemusele, siis suur töökoormus ja ressursside piiratus ei võimalda eriti sellisel viisil autoriõiguste rikkumisi tuvastada.³³

Vestlusest Politsei- ja Piirivalveameti Põhja prefektuuri kriminaalbüroo majanduskuritegude talituse menetlejaga selgus, et reeglina alustatakse internetis toimepandud autoriõiguste rikkumiste puhul menetlust Eesti Autoriõiguste Kaitse Organisatsiooni (EAKO) ja *Business Software Alliance*'lt (BSA) kuriteoteate põhjal.³⁴

2012.a märtsis läbiviidud ekspertintervjuu EAKO tegevdirektori Erik Mandre'ga, kelle selgituse kohaselt, „teeb tavapäraselt EAKO esindaja probleemset veebilehelt väljatrükid

³⁰ Künnapas, K. „Justiitsminister: õigusabi seaduse peamine eesmärk on kvaliteetne õigusabi vähekindlustatud elanikel” 11.02.2005 <<http://www.just.ee/6641>> (08.05.2012).

³¹ Terminibaas ESTERM <<http://mt.legaltext.ee/esterm/>> (05.04.2012).

³² Kriminaalmenetluse seadustik 12.02.2003, jõustunud 01.07.2004, RT I 2003, 27, 166, §193.

³³ Alas, „Autoriõiguste rikkumiste tuvastamine internetis“, *supra nota*, lk 12.

³⁴ Alas, „Autoriõiguste rikkumiste tuvastamine internetis“, *ibid*, lk 13.

ning kui tegemist on *torrent*failidega, siis teostab huvipakkuvate failide allalaadimised, salvestab need CD-plaadile ning lisab nii CD-plaadi kui väljatrukid kuriteoteatele.³⁵

Kohtueelse menetluse eesmärk on koguda tõendusteavet ja luua kohtumenetluseks muud tingimused.³⁶ Tõend on KrMS § 63 kohaselt kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoiming, kohtuistung ja jälitustoiming protokoll või muu dokument ning foto või film või muu teabesalvestis.

Digitaaltõend on igasugune digitaalses ehk numbrilises vormis esinev informatsioon, mida on võimalik kasutada kohtus tõendamiseseme asjaolude selgitamisel. Digitaalsete tõendite erisused on:

- 1) digitaalsed tõendid on enamasti silmale nähtamatud ja nende „nägemiseks“ on vaja spetsiaalset tark- ja riistavara ning koolitatud spetsialisti;
- 2) digitaalsed tõendid võivad kergesti kahjustuda või hävida, seetõttu peavad kõik nendega kokku puutuvad isikud teadma ja järgima käitumisjuhiseid;
- 3) digitaalsete tõendid sõltuvad ajategurist, mis tähendab, et paljudel võrguseadmete logid kirjutatakse üle lühikese aja jooksul;
- 4) digitaalsed tõendid ei tunne riigipiire, seega Eestis toime pandud autoriõiguste rikkumiste kohta on võimalik leida tõendeid ka väljastpoolt Eesti Vabariigi piire;
- 5) digitaalse tõendina on kasutatav nii kasutaja enda poolt arvutisse teadlikult sisestatud informatsioon, kuid ka arvuti töö käigus automaatselt tekkinud info.³⁷

Eesti Kohtuekspertiisi Instituudi Infotehnoloogia osakonna juhataja Pavel Laptev eristab nelja liiki digitaaltõendeid:

- 1) digitaaltõend – informatsioon, mida säilitatakse või edastatakse binaarsel kujul ning mida kohus aktsepteerib;
- 2) originaalne digitaaltõend – füüsilised andmekandjad ja muud andmekandjad, mis on seotud selle esemega võetuse ajal;

³⁵ Alas, „Autoriõiguste rikkumiste tuvastamine internetis“, *ibid*, lk 13.

³⁶ Kriminaalmenetluse seadustik § 211 lg 1.

³⁷ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *supra nota*, lk 8.

- 3) dublikaat digitaaltõend – füüsilistel andmetekandjatel olevate originaal andmete täpne digitaalne reprodutseerimine;
- 4) koopia – täpne reproduktsioon informatsioonist, mis on saadud füüsilisest esemest eraldi seisvatelt andmekandjatel.³⁸

Infotehnoloogia kuritegude menetlemise käsiraamatu järgi võib eristada kahte liiki digitaaltõendeid:

- 1) tõendid andmekandjatel – need on kõvakettad, mälukaardid, mälupulgad, SIM-kaardid jne. Andmekandjal oleva informatsiooni tuvastamiseks ja tõendina sobilikul kujul fikseerimiseks on kaks võimalust:
 1. politseiasutuse spetsialiseeritud üksuses teostatakse arvuti ja andmekandja uuring, mille tingimused, tulemused ja käik talletatakse vaatlusprotokollis ning vajadusel lisatud andmekandjal (tavaliselt CD või DVD plaat);
 2. arvuti ja andmekandja saadetakse menetleja ekspertiisimääruse alusel EKEI infotehnoloogiaekspertiisi. Tulemused ja käik talletatakse ekspertiisiaktis eksperdiarvamuseks.
- 2) Tõendid arvutivõrkudes – nt autoriõiguste rikkumised, mida pannakse toime internetis. Võrguseadmetes salvestatud logide abil on võimalik tuvastada isikute tegevus arvutivõrkudes, mille lõpptulemusena on võimalik teada saada kahtlustatava arvuti ja seejärel see juba ekspertiisi või politseiasutuse vastavasse osakonda edasiseks uurimiseks saata.³⁹

Tihti puutuvad tõenditega, kaasa arvatud digitaaltõenditega, sündmuskohal kokku esimesena just need isikud, kes esimesena sündmuskohale jõuavad. Esimestena võivad sündmuskohale jõuda ka politseinikud, kes igapäevaselt ei tegele digitaaltõenditega ja pole saanud vastavat väljaõpet. Esmane menetleja peab nagu DNA vms tõendite puhul ära tundma digitaaltõendeid ja kohad, kus neid võib leida. Samuti tagama digitaaltõendite puutumatus ja säilimise.⁴⁰

³⁸ Laptev, P ettekanne „Digitaalsete tõendite kohtuekspertiis“ USPTO konverents, 2010.

³⁹ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *supra nota*, lk 8.

⁴⁰ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 9.

Sündmuskohal tuleb esimese asjana tagada tõendite turvalisus. Digitaalsete tõendite puhul on kõige olulisem tagada, et mitte keegi ei katsuks võimalikke tõendeid sisaldavat seadet ega nende seadmete ühendusi. Tuleb tähele panna, et praegusel digiajastul võivad osad digitõendid peituda ka kahtlustatava taskus, näiteks mobiiltelefon või pihuarvuti. Pihuarvutite puhul peab politsei olema eriti tähelepanelik, kuna nende puhul saab nendes sisalduvat teavet hetkega hävitada üksnes aku eemaldamisega.⁴¹ Samuti peab valmis olema, et digitaaltõendid võivad olla erineva kujuga ja peidetud kõikvõimalike asjade sisse. Näiteks SIM kaardi suurus võib olla alla 0,5cm ja mälu pulgad võivad olla peidetud võtmehoidja või pehme mängulooma sisse.

Tõendite kogumisel enne läbiotsimise teostamist on vaja koguda võimalikult palju infot nii läbiotsitava koha kui ka sealviibivate inimeste kohta. Selline tegevus aitab vähendada ootamatusi. On oluline teada, kas läbiotsimisel ootab ametnikke ees üks või kümme arvutit, kui palju ja millised on ruumid, mida läbi otsima hakatakse. Samuti on oluline teada ruumides olevate inimeste hulk ning võimalusel ka nende isikuomadused - erilist tähelepanu tuleb pöörata kahtlustatava IT- alasele teadlikkusele.⁴²

Digitaaltõendite kogumisel, säilitamisel, transportimisel ja analüüsimisel tuleb järgida samu põhimõtteid, mis konventsionaalsete tõendite puhul.

- 1) asitõendite kogumisel tehtu ei tohi muuta asitõendit;
- 2) digitaaltõendile juurdepääsu vajav inimene peab olema saanud erialase koolituse;
- 3) kõik konfiskeeritud digitaaltõendiga seotud tegevused, ligipääs, säilitamine ja edastamine, peavad olema täielikult dokumenteeritud ja võimaldama uuesti läbivaatamist;
- 4) menetleja ja/või ekspert vastutavad tema valduses olevate digitaalsete tõenditega tehtavate toimingute eest.⁴³

⁴¹ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 10.

⁴² Baum, A. ettekanne „Current issues in digital copyright piracy“, USPTO Digitaalpiraatluse konverentsil, 2010.

⁴³ Laptev, P. „Digitaalsete tõendite kohtuekspertiis“, *supra nota*.

Digitaaltõendite säilitamise puhul on oluline teada, et IT seadmete kasutamisel jäävad tegevusest maha jäljed, mis võivad tagantjärele tuvastada, millal seade viimati töötas ning mida sellega tehti.⁴⁴

Digitaalseadmeid on erinevaid ja ka nende tööpõhimõtte võib olla erinev, seega peavad kõik autoriõiguste rikkumiste menetlejad teadma, kuidas sündmuskohal ümber käia arvuti, digitaalkaamera, digitaalkäekella, GPS seadme, pihuarvuti, andmekandjate ja mobiiltelefonidega.

On olemas erinevat tüüpi arvuteid – lauaarvutid, sülearvutid, pihuarvutid, suurarvutid, moodulitest koosnevad serverisüsteemid jne. Arvuti juurde võivad kuuluda veel kõikvõimalikud lisad nt modemid, printerid, skännerid, hoidikud, salvestusseadmed vms.

Arvuti võib olla eraldiseisev või ühendatud arvutivõrku. Tavaliselt koosneb arvuti keskprotsessorist, andmesalvestusseadmest, monitorist, klaviatuurist ja hiirest. Tõendeid võib arvutite puhul leida nii kõvakettalt kui ka muudest arvutiga ühendatud salvestusseadmetest. Andmeid on kahte tüüpi:

- 1) kasutaja poolt tekitatud andmed: video ja audio failid, dokumendid, e-kirjad, kontaktid, veebibrauserit järjehoidjad. Nende andmete kaitsmiseks võib kasutaja kasutada erinevaid viise: steganograafia kasutamine, failidele eksitava nime andmine, peitefailid ja failide pakkimine.
- 2) arvuti poolt tekitatud andmed: *backup files* (varundatud failid), ajutised failid, ajaloo failid, peitefailid, süsteemifailid, ajutised interneti failid, *Swap files* (saalefailid) ja *Cookies* (küpsised).

Iga fail sisaldab erinevaid komponente nagu ajamärgid, kasutajaga seonduv info vms, mis kõik omavad tõendamisel tähtsust ning, mis võivad muutuda ainuüksi arvuti sisselülitamisega. Lauaarvuti äravõtmisel on vaja teha kindlaks, kas arvuti on sisse lülitatud või mitte. Kindlasti tuleb see ka protokollis kajastada. Kui arvuti on välja lülitatud ei tohi seda mitte mingil juhul sisse lülitada, vaid peab ühendama lahti kõik juhtmed ja kõik täpselt protokollis kirja panema. Kui arvuti on sisse lülitatud, tuleb võimalusel konsulteerida spetsialistiga. Võimaluse puudumisel tuleb tegutseda järgmiselt:

- 1) kui printimine on pooleli, tuleb lasta printimine lõpetada;

⁴⁴ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *supra nota*, lk 10.

- 2) kui arvuti on ühendatud võrku, tuleb katkestada ühendus, ühendades lahti võrgujuhe, modemijuhe ja WiFi – kaart, GPRS kaart ja kõik muu;
- 3) tuleb teha kindlaks, kas monitor on sisse lülitatud või mitte, kas ekraanil on töökeskkond nähtav või mitte. Kui on nähtav, siis tuleb see jäädvustada videolindile ja kirjeldada protokollis. Kui monitor on välja lülitatud, lülita see eelnevalt sisse. Kui monitor on unerežiimil või näitab ekraanisäätjat, siis tuleb õrnalt hiirt liigutada. Hiire klahve, kerimisnuppu ja klaviatuuri ei tohi kasutada isegi kui monitori pilt ei muutu;
- 4) arvuti tuleb vooluvõrgust lahti ühendada, ühendades lahti toitejuhtme arvuti küljest, ainult seinapistikust eemaldamisest ei pruugi piisata;
- 5) tuleb ühendada lahti ülejäänud toitejuhtmed;
- 6) kogu tegevus tuleb protokollida.⁴⁵

Pihuarvuti on väike arvuti, mis sarnaneb oma tööpõhimõttelt lauarvutile. Seda saab kasutada, telefoni, faksi, interneti, e-posti kasutamiseks või failide transportimiseks ning andmetöötluseks. Pihuarvutis võivad olla pesad mälukaartide jaoks. Tõenditena on võimalik pihuarvutites leida kontakte, helisalvestisi, kalendreid, dokumente, pilte, e-kirju, salasõnu, tekstisõnumeid, käsitsi kirjutatud tekste jne. Kui pihuarvuti ei ole sisse lülitatud, tuleb toitekaabli olemasolul aku laadida. Kui pihuarvuti on sisse lülitatud, tuleb teha ekraanil nähtuvast videosalvestis, toitekaabli olemasolul laadida aku. Kui see ei ole võimalik, siis jätta pihuarvuti sisselülitatuks ja toimetada viivitamatult spetsialistile või ekspertiisi. Kui on ühendatud lisakaarte, tuleb need eemaldada ja isoleerida. Kui ei ole võimalik aku taset kindlaks teha, tuleb eeldada, et see on tühi ja toimetada pihuarvuti viivitamatult ekspertiisi. Kogu tegevus tuleb alati protokollida.⁴⁶

Andmekandjateks võivad olla kõvakettad, disketid, CD ja DVD plaadid, ZIP kettad, magnetoptilised kettad, salvestuslindid, minidiskid, USB mälu pulgad, mälu kaardid, USB-mäluga kirjutusvahendid, ehted, käekellad, taskunoad vms. Andmekandjatel talletatakse kõikvõimalik digitaalne informatsioon failidena. Andmekandjad tuleb toimetada spetsialisti või eksperdi kätte. Tegemist on õrnade seadmetega, mistõttu tuleb käsitseda

⁴⁵ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *supra nota*, lk 40.

⁴⁶ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 42-43.

neid väga ettevaatlikult. Transportimiseks tuleb kasutada antistaatilist ja põrutuskindlat pakendit.⁴⁷

Mobiiltelefon on seade, mis pakub mobiilset suhtlemisvõimalust, kasutades selleks erinevaid süsteeme ja sagedusi. Tänapäeva mobiiltelefonid on rohkem nagu lauarvutid ja helistamine on muutunud sekundaarseks funktsiooniks. Tõenditena on võimalik mobiiltelefonist saada fotosid, lindistusi, kalendri informatsiooni, kõnede ajalugu, kontakte, sõnumeid jne. Mobiiltelefoni käsitsemisel tuleb teha kindlaks, kas see on sisse lülitatud. Kui telefon on välja lülitatud, ei tohi seda sisse lülitada. Kui telefon on sisse lülitatud, ei tohi seda välja lülitada, sest see võib raskendada või muuta koguni võimatuks informatsiooni kättesaamise. Telefoni ekraanil olev tuleb jäädvustada videolindile. Kaasa tuleb võtta juhtmed, akulaadija ja olemasolu korral ka kasutamishend. Telefon tuleb toimetada viivitamatult spetsialistile või eksperdile. Kogu tegevus tuleb talletada protokollis.⁴⁸

Probleeme võib tekitada tõendite fikseerimine veebilehe haldaja/hostingu pakkuja juures. Üldjuhul problemaatilise sisuga veebilehti enda arvutis ei majutata. Ühel haldajal aga võib olla piiramatus koguses veebilehti, millest ainult üks sisaldab teadaolevalt illegaalset materjali. Praegu on Eestis võimalik teha võetus kogu serverile, kuhu on majutatud palju erinevaid veebilehti, millest võib olla ainult üks sisaldab illegaalset tarkvara. Sellise võimaluse väljapakkumine lehekülgede majutajale viib tihti soovitud koostööni kahtlustatava ja ametnike vahel, kuna kõikide kodulehtede üheaegne kasutajatele ligipääsmatuks tegemine kahjustab majutaja äritegevust.⁴⁹

Peale seda, kui sündmuskohalt on andmekandja kaasa võetud antakse see üle spetsialistile või saadetakse EKEI'sse. Edasi on spetsialisti ja eksperdi töö küllaltki sarnane. Kõigepealt tehakse andmekandjast täpne koopia. Seejärel uuritakse seda koopiat, kasutades spetsiaalset tarkvara, mis võimaldab suure hulga andmete seast välja sõeluda need, mis omavad tõenduslikku tähendust. Asja lihtsustavad menetleja esitatud märksõnad. Arvutikriminalistika puhul on võimalik kätte saada andmed, mis tavatarkvaraga ei ole

⁴⁷ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 44.

⁴⁸ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 45.

⁴⁹ Baum, „Current issues in digital copyright piracy“, *supra nota*, 2010.

võimalik, nt kustutatud failid. Spetsialisti vaatluse puhul talletatakse uuringu tulemused vaatlusprotokollis, eksperdi puhul ekspertiisiaktis.⁵⁰

Digitaaltõenditel on internetis toimepandud autoriõiguste rikkumiste menetlemisel väga oluline roll. Antud valdkonnas ei ole käesoleva ajani ühtegi Riigikohtu lahendit. 01.06.2012 tegi Tallinna Ringkonnakohtus esimese otsuse *torrent* kaasuse kohta. Tallinna Ringkonnakohtu otsusega jäeti jõusse Harju Maakohtu otsus 1-11-12296, milles KarS §222 lg1 järgi tunnistati süüdi isik, kes lõi internetilehekülje <http://orkut.planet.ee> ja jagas seal Eesti artistide albumeid. Samuti tegi isik omale konto internetileheküljele <http://thepiratebay.org/>, kus jagas Eesti autorite loomingut, olles need eelnevalt *torrent*-failideks muutnud. Tegu oli tõendatud lisaks kahtlustatava enda ütlustele veel ka ekspertide ütlustega, interneti lehekülgede vaatlustega ja uurimiseksperimentidega. Zone Media OÜ'st tehtud päringu alusel saadi teada, kes lõi internetilehekülje <http://orkut.planet.ee> ja kes seda kasutas. Veebilehe vaatlusprotokollist oli näha, et koduleheküljelt oli võimalik illegaalselt alla laadida autoriõigusega kaitstud muusikateoseid. Samuti on näha vaatlusprotokollis, et internetileheküljel sisaldas MP3 formaadis faile 22,5GB ulatuses. Lisaks tuvastati vaatlusega, et aadressil <http://thepiratebay.org/>, kasutaja „fedjaEST“ kataloogis asuvad *torrent* – failid.⁵¹

Digitaaltõendite usaldusväärse tõttu, mõistis Harju Maakohtus isikule 8 kuud vangistust, mis kuulub täitmisele vaid siis, kui isik paneb 3 aasta jooksul tahtlikult toime uue kuriteo. Kõik kannatanute tsiviilhagid rahuldati ja mõisteti välja Eesti Autorite Ühingule 2046,52 eurot, Terminaator MusicOÜ'le 2013, 75 eurot, Tartu Kontserdikorraldus OÜ'le 1491, 20 eurot, TK'le 82,65 eurot, MA'le 777, 45 eurot, MK'le 980, 91 eurot, Crunch Industry OÜ'le 25,55 eurot, AV'le 482, 58 eurot, ja Varnja Maja OÜ'le 25,55 eurot. Samuti mõisteti isikult välja kannatanute poolt kriminaalasja menetlemisega seotud kulud kokku 2780, 24 eurot, mis tuleb tasuda Eesti Fonogrammitootjate Ühingule. Lisaks tuleb isikul tasuda menetluskuludena II astme kuriteos süüdimõistva kohtuotsusega kaasneva 135 eurot ja kaitsja tasu 184 eurot.⁵² Ringkonnakohtus mõistis isikult veel lisaks välja kaitsja kuludena 57,60 eurot ja kannatanute poolt kriminaalasja menetlemisega seoses kantud

⁵⁰ Phare mestiprojekt, „Infotehnoloogiakuritegude menetlemise käsiraamat“, *ibid*, lk 10.

⁵¹ Harju Maakohtu otsus Kristjan Luik, nr 1-11-12296, 07.02.2011, lk 10-11.

⁵² Harju Maakohtu otsus 1-11-12296, *ibis*, lk 12-14.

kulud 230,08 eurot, mis läheb Eesti Fonogrammitootjate Ühingu arvele.⁵³ Kokku mõisteti isikult välja 11313,08 eurot.

1.3. Digitaalsete tõendite kogumine ja käitlemine USA's

2010. aasta aprillis avaldas nn Witteni komisjon Euroopa autoriõiguse koodeksi, mille eesmärgiks on luua näidisregulatsioon ühtlustamaks liikmesriikides kehtivat õigust. Väljapakutud koodeks sarnaneb pigem anglo-ameerika traditsioonidele, kuigi komisjon koosnes enamjaolt germaani-, kuid ka romaani-süsteemi järgivate riikide teadusasutustest ning veidi vähem oli anglo-ameerika süsteemile toetujaid. Näiteks, kui varaliste õiguste kogum oli eelnevalt lõplik, siis uues koodeksis on jäetud loetelu anglo-ameerika süsteemile omaselt avatuks.⁵⁴ Seetõttu valis lõputöö autor analüüsimiseks USA digitaaltõendite kogumise ja käitlemise juhendid.

Ameerika Justiitsministeeriumi FBI operatiivse tehnoloogia osakonna digitaaltõendite büroo, kuhu kuuluvad ka RCFL (*Regional Computer Forensics Laboratory*) programm ja CART (*Computer Analysis Response Team*) töötas välja juhendi digitaaltõendite õigeks kogumiseks, säilitamiseks ja käitlemiseks. Antud juhend on osa RCFL'i programmi koolituse sarjast.⁵⁵

RCFL eristab digitaaltõendite kohta viit olulist fakti, mida peaks teadma iga töötaja, kes võib kokku puutuda digitaaltõenditega:

- 1) Erinevat liiki kuriteod võivad sisaldada digitaaltõendeid.
- 2) Igalt sündmuskohalt võib leida digitaaltõendeid, seetõttu tuleb käituda igal sündmuskohal sama ettevaatlikult, et kindlustada enda ohutus ja säilitada igat liiki tõendeid.

⁵³ Tallinna Ringkonnakohtu otsus Kristjan Luik, nr 1-11-12296, 01.06.2012, lk 4-5.

⁵⁴ Elunurm, S., „Euroopa autoriõigus reformide teel“, 24.05.2010, <<http://www.blslawfirm.com/et/bls-estonia/uudised/uudis?nid=483>> (20.03.2013)

⁵⁵ U.S. Department of Justice Federal Bureau of Investigation Digital evidence field guide: What every peace officer must know, p 2.

- 3) Digitaaltõendid võivad olla õrnad. Nõudeid mitte täites võivad külm, kuumus ja magnetväli tõendid hävitada. Samuti võib digitaaltõend kukkumisel saada kahjustada.
- 4) Digitaaltõendid on kergesti muudetavad. Kui arvuti on välja lülitatud siis ei tohi seda sisse lülitada, et kogemata andmeid ei muudetaks.
- 5) Kunagi ei tohi eeldada, et arvuti on hävinenud. RCFL ja CART eksperdid on suutnud saada digitaaltõendeid läbipõlenud arvutitest ja seadmetest, mis on leitud järve põhjast. Igaks juhuks tuleb digitaalseade alati viia eksperdile edasisteks uuringuteks.⁵⁶

Digitaaltõendite käitlemise juhendi on välja töötanud ka Ameerika Sisejulgeolekuministeerium USSS. Selle juhendi väljatöötamiseks tehti koostööd mitmete erinevate agentuuridega. Võrreldes FBI juhendiga on USSS'i juhendis mõned printsiibid lisaks:

- 1) tuleb kontrollida, kas on seaduslik alus arvuti kaasa võtmiseks.
- 2) kui on alust arvata, et arvuti hävitab tõendeid tuleb see koheselt välja lülitada eemaldades toitejuhtme arvuti küljest.
- 3) tuleb pildistada monitori, arvuti asukohta ruumis ja kõiki elektroonika seadmeid, mis on arvuti külge ühendatud.
- 4) tuleb kindlaks teha, kas arvuti kasutajat seob tema professionist tulenevad konfidentsiaalsuse nõuded, näiteks arst, psühhiaater, advokaat, riigisaladuse luba vms.⁵⁷

Nii FBI kui ka USSS'i juhendis on välja toodud, milliseid digitaaltõendeid võib leida erinevate kuriteoliikide puhul. FBI juhendis on välja toodud, milliseid digitaaltõendeid tuleks otsida lapspornograafia, küberterrorismi, finantspettuste, tapmiste, identiteedi varguste ja narkokuritegude puhul.⁵⁸ USSS'i juhendis on välja toodud, milliseid digitaaltõendeid tuleks otsida lähisuhtevägivalla, finantskuritegude, ahistamiste,

⁵⁶ U.S. Department of Justice: What every peace officer must know, *ibid*, p 2.

⁵⁷ U.S. Department of Homeland Security United States Secret Service Best Practice for Seizing Electronic Evidence v.3: A Pocket Guide for First Responders, No 2.

⁵⁸ U.S. Department of Justice: What every peace officer must know, *supra nota*, p 4-6.

narkokuritegude, telekommunikatsiooni pettuste, identiteedivarguste ja autoriõiguste rikkumiste puhul. Autoriõiguste rikkumiste puhul tuleb tähelepanu pöörata:

- 1) vestlus - logidele.
- 2) e-mailidele, märkmetele ja kirjadele.
- 3) tarkvara sertifikaadi pildi failidele.
- 4) interneti töölogidele.
- 5) tarkvara seerianumbritele.
- 6) programmidele, mis murravad lahti teisi programme.
- 7) kasutaja loodud kataloogidele ja failide nimedele, mis kvalifitseerivad autoriõigustega kaitstud tarkvara.⁵⁹

FBI digitaaltõendite käsitlemise juhend jagab digitaaltõendid nelja kategooriasse:

- 1) tavalised: mobiiltelefonid, mälupulgad, digitaalsed kaamerad, DVD/CD, MP3 mängijad, mälukaardid.
- 2) ebatavalised: sisemäluga printerid, digitaalsed videosalvestajad (kordus TV), automaatvastajad, GPS vastuvõtjad, mängukonsoolid, digitaalsed diktofonid.
- 3) kaitstud: – ebatavaline digitaalne seade, mis on mõeldud tõkestamiseks loata sisenemist ja mis omakorda jagunevad:
 1. biomeetriliselt kaitstud seadmed, näiteks silma iiris skännerid, sõrmejäljelugejad.
 2. mehhaaniliselt kaitstud seadmed, näiteks sissepääsukaardid.
- 4) peidetud: – digitaalseaded, mis on varjatud kujul. Selliste esemete leidmine eeldab väga põhjalikku ja korralikku läbiotsimist.
 1. arvutid, mis on maskeeritud kastiks või pudeliks;
 2. USB mälupulgad, mis on maskeeritud käepaelaks, pastakaks, kellaks, kõrvarõngaks, taskunoaks, krediitkaardiks, mänguasjaks või igapäevasteks esemeteks.⁶⁰

FBI digitaaltõendite käsitlemise juhendis on ära märgitud, milline varustus peab olema menetlejal kaasas, kes hakkab sündmuskohal digitaaltõendid koguma:

- 1) fotoaparaat või videokaamera;

⁵⁹ U.S. Department of Homeland Security: A Pocket Guide for First Responders, *supra nota*, No 12-14 .

⁶⁰ U.S. Department of Justice: What every peace officer must know, *supra nota*, p 7-8.

- 2) kruvitsad koos valiku väikeste otsadega;
- 3) tavalised ja kitsaotsaga traaditangid;
- 4) asitõendi teip;
- 5) isoleerteip;
- 6) taskulamp;
- 7) pastakas;
- 8) kõvaketta hoiukarbid;
- 9) tõendi sildid;
- 10) kindad;
- 11) kotid;
- 12) karbid;
- 13) sildid;
- 14) märkmik;
- 15) asitõendi vastuvõtu aktid;
- 16) kummipaelad.⁶¹

FBI ja USSS juhendite järgi tuleb sündmuskohal tegeleda lauarvutiga samamoodi nagu seda näeb ette ka Eesti Infotehnoloogia kuritegude menetlemise käsiraamat. USSS digitaaltõendite käitlemise juhendis on eraldi välja toodud sülearvuti käsitlemise erinevus, mis seisneb selles, et kui sülearvuti ei lülitu korralikult välja toitejuhtme eemaldamisel, siis tuleb eemaldada sülearvutilt aku. Sülearvuti aku asetseb tavaliselt sülearvuti all, kus on ka nupp või lüliti, mis võimaldab aku eemaldamist. Eemaldatud akut ei tohi enam sülearvuti külge kinnitada. Sülearvuti aku eemaldamine aitab ennetada sülearvuti iseeneslikku sisselülitust.⁶²

Eesti infotehnoloogia kuritegude menetlemise käsiraamat lubab arvuti töötamise kontrollimiseks vaid hiirt liigutada. FBI ja USSS'i juhend lubab lisaks ka klaviatuuri kasutada. USSS'i juhendis tuleb liigutada hiirt ja vajutada klaviatuuril klahvi *space*.⁶³ FBI juhend näeb ette „*Bump/Shift/Feel*“ testi, mille käigus tuleb hiirt liigutada või vajutada

⁶¹ U.S. Department of Justice: What every peace officer must know, *ibid*, p 10.

⁶² U.S. Department of Homeland Security: A Pocket Guide for First Responders, *supra nota*, No 3.

⁶³ U.S. Department of Homeland Security: A Pocket Guide for First Responders, *ibid*, No 3.

selle klahvi, seejärel tuleb vajutada klaviatuuril *Shift* nuppu ning seejärel panna käsi arvuti ventilaatori juurde. Kui ventilaator ei liigu ja on jahe, siis on arvuti välja lülitatud.⁶⁴

Eesti Infotehnoloogia kuritegude menetlemise käsiraamat ja USSS'i juhend näevad ette toitejuhtme eemaldamise arvuti küljest ka juhul, kui arvuti on sisse lülitatud. FBI juhend eristab kahte väljalülitamise viisi: järsk või ettevaatlik väljalülitus. Järsk väljalülitamine tehakse juhul kui on kahtlus, et arvuti võib hävitada tõendeid. Selleks tõmmatakse toitejuhe seinast välja. Järsu väljalülitamise puhul tuleb arvestada, et positiivsest küljest säilivad mõned süsteemi failid, ennetatakse hävitava programmi tegevust, ajatemplite muutumist ja muutusi failide atribuutides. Samas järsu väljalülitamisega võidakse rikkuda operatsioonisüsteemi ja avatud dokumente. Samuti kaovad salvestamata avatud dokumendid. Ettevaatliku väljalülitamise puhul suletakse süsteem soovitatud viisil. Oluline on teada, et väljalülitamise meetodid erinevatel operatsioonisüsteemidel varieeruvad. Ettevaatlik väljalülitamine võib aidata tuvastada interneti ühendusi, tuvastada ja sulgeda avatud failid, kindlustada edukam arvuti käivitamine. Samas võivad kaduda osad süsteemi failid ja arvuti väljalülitamisel võib käivituda enesehävituslik programm.⁶⁵

Serverite puhul näeb USSS'i juhend ette konsultatsiooni arvuti spetsialistiga ja sündmuskoha puutumatus tagamise. Kedagi ei tohi lasta serveri juurde, välja arvatud vastava väljakutse saanud isikud. Serverite puhul toitejuhtme eemaldamine võib oluliselt kahjustada süsteemi, häirida legaalseid ärisid ja tekitada lisaprobleeme politseiametnikule.

Kõik kolm digitaaltõendite käsitlemise juhendit näevad ette kohustuse fotografeerida sündmuskohal asitõenditega tegelemise kõik etapid. FBI juhend näeb ette veel kohustuse võimalusel pildistada sündmuskohal olevaid arvutiga seotud raamatuid, sest see annab menetlejatele otsest infot kahtlustatava arvutioskuste kohta. Inimesed sageli kirjutavad arvuti kasutamiseks vajaminevat infot arvuti lähedusse. Seetõttu tuleb pildistada üles kõik salasõnad, mis leitakse.⁶⁶

⁶⁴ U.S. Department of Justice: What every peace officer must know, *supra nota*, p 15.

⁶⁵ U.S. Department of Justice: What every peace officer must know, *ibid*, p 15 ja 16.

⁶⁶ U.S. Department of Justice: What every pace officer must know, *ibid*, p 14.

USSS'i juhendis on välja toodud üldised küsimused, mida on võimalik küsida kõikide digitaaltöenditega kuritegude puhul Spetsiifilistest kuritegudest on näidisküsimused välja toodud identiteedivargusel, finants kuritegudel, lastevastastel interneti kuritegudel ja interneti jututubades toimepandud kuritegudel. Üldised küsimused on: millal ja kust saadi arvuti? Kas see oli uus või kasutatud? Kellel on ligipääs arvuti riist- ja tarkvarale? Kas nad pääsevad ligi kõigele arvutis või ainult teatud failidele ja programmidele? Kus arvutis on elektrooniline meedia salvestatud? Kelle sõrmejäljed võivad olla elektroonilisel meedial? Kui paljud kasutavad arvutit? Kes nad on? Millised arvutialased teadmised teistel kasutajatel on? Mis kellaegadel päevas on teistel isikutel juurdepääs arvutile? Mis on nende kasutajanimed arvutis? Mis programme iga kasutaja kasutab? Kas arvutisse sisenemiseks on vaja kasutajanime ja salasõna? Mis need on? Kas seal on tarkvara, mis nõuaks kasutajanime või salasõna? Kas ja kuidas on arvuti interneti ühendatud? Kas kasutajal/kahtlustataval on e-maili konto? Kes on teenusepakkuja? Kui e-mailid on kuriteoga seotud, siis tuleb kannatanult/kahtlustatavalt küsida nende e-maili aadressid. Millist e-maili programmi kannatanu/kahtlustatav kasutab? Kas kannatanul/kahtlustataval on arvutile kaugligipääs? Kas keegi kasutajatest kasutab interneti või välist mälu? Kas on kasutatud programme arvuti puhastamiseks? Kas arvuti sisaldab krüpteerimistarkvara või kõvaketta kustutusprogramme? Kas arvuti on alati sisse lülitatud?⁶⁷

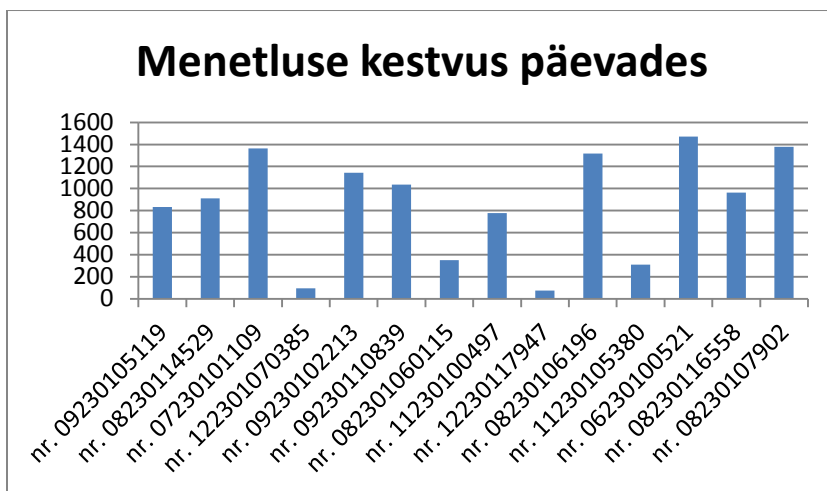
⁶⁷ U.S. Department of Homeland Security: A Pocket Guide for First Responders, *supra nota*, No 15-18.

2. DIGITAALSETE TÕENDITE KOGUMINE AUTORI - ÕIGUSTEGA SEOTUD KRIMINAALASJADES EESTIS

Käesoleva lõputöö uuringu meetod oli toimikute vaatlus ja menetlejate intervjuerimine. Autor vaatles Politsei- ja Piirivalveameti Põhja prefektuuri menetluses olnud ning prokuratuuri loal lõpetatud 14 kriminaalasia toimikut, kus on autoriõiguste rikkumine toime pandud internetis. Lisaks viis autor nelja kriminaalmenetlejaga läbi ekspertintervjuud, et selgitada välja nende hinnang digitaaltõendite osatähtsusele internetis toimepandud autoriõiguste rikkumiste kriminaalmenetlustes.

2.1. Kriminaalasiade toimikute analüüs

Valimiks oli Põhja prefektuuris 14 internetis toime pandud autoriõiguste rikkumiste kriminaaltoimikut, mille menetlemisel oli kogutud digitaaltõendeid ning mille menetlus oli prokuratuuri loal lõpetatud. Kriminaalmenetlused viidi läbi aastatel 2006-2013. Kriminaalmenetluste pikkus oli varieeruv alates 75 päevast kuni 1471 päevani.⁶⁸

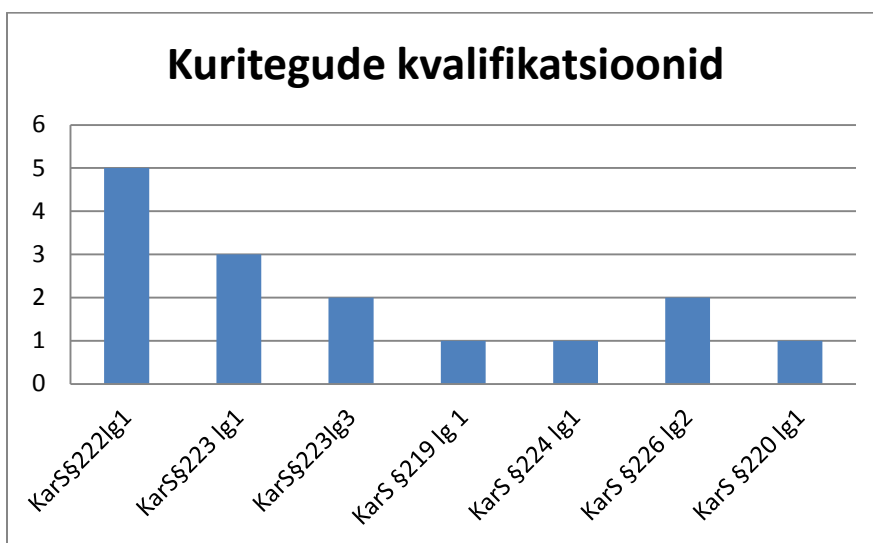


Joonis 1. Menetluse kestvus päevades

Autoriõiguste rikkumiste kuriteod olid kvalifitseeritud Karistusseadustik § 219 lg 1, § 220 lg 1, § 222 lg 1, § 223 lg 1 ja 3, § 224 lg 1 ja § 226 lg 2 järgi. Kõige enam, viiel korral, oli menetletud KarS § 222 lg 1 järgi kvalifitseeritavat kuritegu, mis on teose või

⁶⁸ Käesolev töö, Lisa 1. Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 43.

autoriõigusega kaasnevate õiguste objekti reprodutseerimine levitamise eesmärgil ilma teose autori, tema õiguste valdaja või autoriõigusega kaasnevate õiguste valdaja loata.⁶⁹

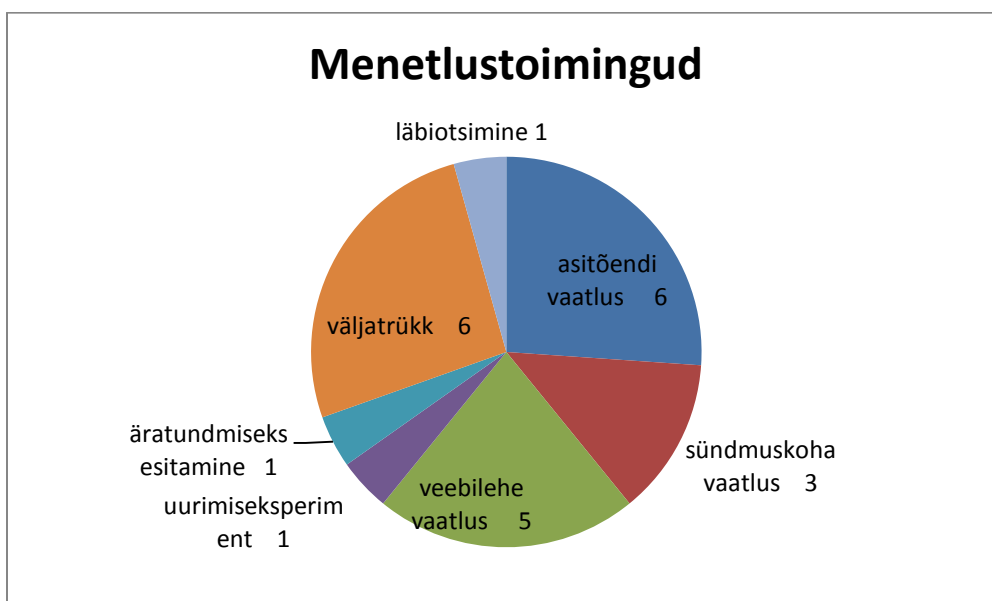


Joonis 2. Kuritegude kvalifikatsioonid

Kõikides kriminaalasjades olid üle kuulatud kannatanud ja tunnistajad. Kuues menetluses oli teostatud asitõendite vaatlusi. Asitõenditena vaadeldi DVD'sid, kaubamärke ja tarkvaraprogramme. Ühes kriminaalasjas teostati neli asitõendite vaatlust. Kolmes kriminaalasjas teostati sündmuskoha vaatlusi, kusjuures ühel juhul oli tegemist nelja ja teisel juhul kahe erineva sündmuskohaga. Tegemist oli ettevõtetega, kes kasutasid üldsusele suunamiseks fonogramme ilma Eesti Fonogrammitootjate Ühingu tasu maksmata. Veebilehtede vaatlusi teostati viies kriminaalasjas, milledest ühes teostati kahe erineva veebilehe vaatlused. Ühes kriminaalasjas tehti uurimiseksperiment, mille käigus Eesti Autoriõiguste Kaitse Organisatsiooni tegevdirektori Erik Mandre juuresolekul laeti internetikeskkonnast alla autoriõigustega kaitstud teoseid, mille levitamiseks puudus internetilehekülje omanikul luba. Ühes kriminaalasjas koostati kuus fotode järgi isikute äratundmise protokoll. Väljatrükke internetikeskkonnast teostati kuues kriminaalasjas. Väljatrükid olid ühel korral binaarsel kujul, ülejäänud kordadel oli tegemist internetilehekülgede vaadetega. Ühes kriminaalasjas teostati läbiotsimised kahtlustatava elukohas ja tema sõiduautos, mille käigus leiti ja võeti kaasa digitaaltõenditena piraattarkvara. Samas kriminaalasjas teostati mitmeid jälitustoiminguid ja määrati kaks

⁶⁹ Käesolev töö, Lisa1. Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 43.

tarkvaraekspertiisi. Ühes kriminaalasjas kuulati üle ka ekspert ning ühes kriminaalasjas määrati kujutise ekspertiis.⁷⁰



Joonis 3. Menetlustoimingud

Kaheksas kriminaalasjas neljateistkümnest on kahtlustatavate isikud kindlaks tehtud, kuid kedagi ei vahistatud. Kahes kriminaalasjas esialgu menetlust ei alustatud, kuid avaldaja vaidlustas mittealustamise. Ühes kriminaalasjas nõustus nii Põhja Ringkonnaprokuratuur, kui ka Riigiprokuratuur kriminaalmenetluse mittealustamisega, kuid Tallinna Ringkonnakohus asus seisukohal, et Ringkonnaprokuratuuril, kui uurimisasutusel on kohustus alustada antud asjas kriminaalmenetlust.⁷¹

Ühe kriminaalmenetluse käigus tuvastati, et kuritegu pandi toime USA's, üle jäänud juhtudel Eesti Vabariigis. USA toimepandud kuriteo puhul jõuti teha küll asitõendi vaatlus, kuid teo toimepannud isik jäi tuvastamata, sest veebileht suleti.⁷²

Kolmes kriminaalasjas päringuid ei tehtud. Ülejäänud kriminaalasjades koostati erinevaid päringuid kannatanutele, teenusepakkujatele, internetilehekülje haldajatele, pankadele,

⁷⁰ Käesolev töö, Lisa 1. Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 43-44.

⁷¹ Käesolev töö, Lisa 1. Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 43-44.

⁷² Käesolev töö, Lisa 1. Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 43.

kohtutele jne. Päringutega sooviti teada saada IP - aadresse ja nende omanikke, kasutaja - kontode omanikke, tekitatud kahju suurust või muusikateoste autoreid ja õiguste omajaid.⁷³

Viies kriminaalasjas olid vaatluste käigus teostatud videosalvestused jäädvustatud CD-plaatidele ning jäetud suletud ümbrikus kriminaaltoimikusse vaatlusprotokollide juurde. Ühes kriminaalasjas läbiotsimise käigus ära võetud kuus karpi Microsoft Office ja 12 karpi Microsoft Windows 7 Ultimate osutusid piraatkoopiatega ning kuuluvad hävitamisele.⁷⁴

Ühes kriminaalasjas lõpetati prokuröri poolt menetlus KrMS § 202 lg 1 tunnustel, kuna kahtlustatava süü ei olnud suur. Kahes kriminaalasjas lõpetati menetlus avaliku huvi puudumise tõttu KrMS § 202 lg 7. Prokurör selgitas kriminaalmenetluse lõpetamise määruses, et ettevõtte suhtes esinesid asjaolud, mis võimaldasid kriminaalmenetluse lõpetada KrMS § 202 alusel. Karistust raskendavaid asjaolusid ei olnud ja isik ei olnud varem kriminaalkorras karistatud, seega puudus eripreventiivsetest vajadustest lähtuvalt menetluse jätkamise ja isiku kriminaalkorras karistamise vajadus. Lisaks olid ettevõttel kriminaalmenetluse lõpetamise ajaks vajalikud litsentsilepingud sõlmitud. Kannatanu (EFÜ) oli nõus, et menetlus isiku suhtes lõpetati vastavalt KrmS §-le 202 lg 7 ja ei soovi menetluse jätkamist. Seega puudus tema tegude puhul avalik menetlushuvi ning kahtlustatav andis nõusoleku ja võtnud kohustuse tasuda kindel summa riigitulusesse. Kolmel juhul lõpetati kriminaalmenetlus KrMS § 200 – 1 järgi, kui ei suudetud kahtlustatavat kindlaks teha, nendest kahel korral internetileheküljelt suleti. Seitsmes kriminaalasjas lõpetati prokuratuuri loal menetlus KrMS § 200 tunnustel, kui menetluse käigus selgus, et KrMS § 199 lg 1 p1 sätete kohaselt puudus kriminaalmenetluse alus. Üks kriminaalasi lõpetati prokuratuuri loal KrMS § 200 - § 199 lg 1 p 4 tunnustel, kui menetluse käigus selgus, et peamine kahtlustatav on surnud. Viimati nimetatud kriminaalasjas on esitanud üks kannatanutest prokuratuuri loal lõpetamise määruse peale kaebus KrMS § 207 lg 1 järgi. Antud isik oli ainus, kes kõikide vaadeldud kriminaalasiade kannatanutest esitas KrMS § 38 lg 1 p 2 korras tsiviilhagi.⁷⁵

⁷³ Käesolev töö, Lisa 1Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 44.

⁷⁴ Käesolev töö, Lisa 1. Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 45.

⁷⁵ Käesolev töö, Lisa 1Põhja prefektuuri kriminaaltoimikute vaatlus, *infra*, lk 45.

2.2. Ekspertintervjuud autoriõiguste rikkumiste kriminaalmenetlejatega

Lõputöö raames läbiviidud uuringu teise osana on autor korraldanud ekspertintervjuu neljast prefektuurist ühe kriminaalmenetlejatega saamaks teada nende isiklik arvamus digitaaltõendite kogumisest, käitlemisest ja selle vajalikkusest.

Esimesena viidi läbi ekspertintervjuu Ida prefektuuri kriminaalmenetlejaga, kes on tegelema autoriõiguste rikkumiste menetlemisega juba 10 aastat. Keskmiselt menetleb ta aastas üks kuni kaks internetis toimepandud autoriõiguste rikkumist. Intervjueeritava hinnangul on internetis toimepandud autoriõiguste rikkumiste puhul probleemiks tõendusallikate tuvastamine ja kogumine. Selliste kuritegude puhul kasutatakse digitaaltõenditena andmekandjatel leiduvat informatsiooni. Digitaaltõendeid kogutakse sündmuskohal, läbiotsimistel ja asitõendi vaatlustega. Tõendina oluline info talletatakse andmekandjatele. Internetis toimepandud autoriõiguste rikkumisi lõpetatakse prokuratuuri loal tõendite puudumise või kriminaalmenetluse aluse puudumise tõttu. Kõige enam võtavad kriminaalmenetluses aega infotehnoloogiaekspertiisid ja õigusabipalved. Internetis toimepandud autoriõiguste rikkumiste kriminaalmenetluses digitaaltõendite kogumise parendamiseks võiks läbi viia IT alaseid koolitusi, uuendada töövahendeid ja hetkel puudub ka kohtupraktika.⁷⁶

Teisena viidi läbi ekspertintervjuu Lõuna prefektuuri juhtivuurijaga, kes tegeles põhitööna autoriõiguste rikkumiste menetlemisega aastatel 2004-2008. Viimastel aastatel on ta menetlenud mõnda üksikut autoriõiguste rikkumiste kriminaalasja. Lõuna prefektuuris on internetis toimepandud autoriõiguste rikkumisi väga vähe ja ressursi puudumise tõttu toimub menetlemine avalduse põhisel. Autoriõiguste rikkumiste menetlemisel esineb probleeme digitaaltõendite saamisega. Üks võimalus on läbiotsimise käigus ära võtta isiku arvuti ning sealt on võimalik leida tõendeid. Sellisel juhul tehakse *Encase* programmi abil arvuti kõvaketta koopia, mida siis tõendite otsimise eesmärgil läbi vaadatakse. Samuti on võimalik vaadata arvutis olev materjal *Encase* programmi abil läbi isiklikult ning seejärel otsustatakse info kopeerimise vajadus. Tehtud toiming ning kogutud andmed vormistatakse vaatlusprotokolliga. Selle juures on võimalik kopeerida tõenduslikku tähtsust omavate failide sisu otse vaatlusprotokollis või need eraldi lisada protokollis lisadena. Sõltuvalt asja

⁷⁶ Käesolev töö, Lisa 2. Ekspertintervjuu Ida prefektuuri menetlejaga, *infra*, lk 46.

keerukusest on võimalik tõenduslikku tähtsust omavad failid salvestada eraldi andmekandjale ning lisada need protokollile juurde. Kui digitaalsed tõendid saadakse läbiotsimise käigus ja kohapeal kopeerimine ei ole võimalik, siis pitseeritakse arvuti kinni ja võetakse asitõendina kaasa. Hiljem tuleb arvuti avada omaniku juuresolekul, vajalik informatsioon kopeerida või siis kaasasoleva USB abil fikseerida konkreetse räsiväärtuse, vältimaks hilisemaid pretensioone politsei tegevuse kohta.⁷⁷

Viimastel aastatel on probleemiks arutikasutajate IT teadlikkuse suurenemine ja on hakatud internetikelmuste toimepanemisel enda IP-aadressi varjama. Samasugune probleem esineb ka välisoperaatorite poolt kasutatavate meiliaadresside omanike kindlakstegemisega, kuna vajalikke andmeid on võimalik saada ainult õigusabipalvete raames, mis võtavad omakorda väga palju aega. Jälitustegevusega andmete kogumise probleemiks on arvutiühenduse tuvastamine ja saadud andmete interpreteerimine. Jälitustegevusega kogutakse digitaalseid tõendeid: email, IP aadress, avalikes internetiandmebaasides sisalduvat teavet (foorumid, oksjonikeskkonnad – osta.ee, okidoki jmt, internetiarhiiv – internet archive jne). Avalikust internetiruumist saadud tõenditest tehakse väljatrükk ekraanipildist ja fotost või salvestatakse elektroonilisel andmekandjal. Jälitustegevusega saadud andmed säilitatakse elektroonilistel andmekandjatel, väljatrüki kujul vms. Kõige enam võtavad aega õigusabipalved ja IT-alaseid teadmisi nõudvate andmete interpreteerimine. Kriminaalmenetlusi lõpetatakse tõendamatusena või kuriteo koosseisu puudumise tõttu.⁷⁸

Intervjueeritava hinnangul on internetipiraatlus kui „võitlus tuuleveskitega“. Aitaks ehk internetikasutaja täiendav maksustamine (näiteks tühja kasseti maks). See ei puuduta muidugi ärilisel eesmärgil piraattoodete levitamist. Eelkõige peab intervjueeritav tähtsaks aga IT-toe olemasolu prefektuurides. Praegustes IT-kuritegevusega tegelevate gruppide koosseisus puuduvad IT haridusega spetsialistid. Intervjueeritav meenutab juhtumit, kus jälitustegevusega saadud andmed oli vaja saata ekspertiisi, kuid eksperdil puudus õigus töötada riigisaladusega, temal endal aga puudusid ülisuure andmemahu seast ekspertiisiks vajalike andmete väljavalimiseks piisavad oskused. Suure hiline misega saadi lõpuks abi

⁷⁷ Käesolev töö, Lisa 3. Ekspertintervjuu Lõuna prefektuuri menetlejaga, *infra*, lk 47.

⁷⁸ Käesolev töö, Lisa 3. Ekspertintervjuu Lõuna prefektuuri menetlejaga, *infra*, lk 48.

politseinikust IT-spetsialistiks spetsialiseerunud ametnikult, kes nüüdseks on politseist lahkunud.⁷⁹

Kolmandana intervjueriti Põhja prefektuuri kriminaalmenetlejat, kes on töötanud autoriõiguste rikkumiste menetlejana kaheksa aastat. Internetis toimepandud autoriõiguste rikkumisi menetleb ta aastas keskmiselt viis kuni kümme. Digitaaltõendite kogumise probleemidena toob menetleja välja IP - aadressi omaniku tuvastamatuse, kuna arvutikasutaja oskab oma IP – aadressi varjata. Välismaal asuvate IP – aadresside omanikke ja välisoperaatorite meiliaadresside kasutajate tuvastamine on keeruline. Välismaalt on võimalik andmeid saada ainult õigusabipalvete raames, mis võtavad üldjuhul mitu kuud aega. Samuti raskendab positiivsete vastuste saamist välismaalt asjaolu, et Eesti Vabariigi ja välisriikide seadused on erinevad, mistõttu ei ole võimalik kõikides välisriikides Eesti õigusabitaotlust rahuldada, kuna selliseks tegevuseks on vajalik kohtu luba vms. Lisaks säilitatakse IP- logisid erinevates riikides erinevalt, mistõttu võivad jõuda õigusabitaotlused välisriiki alles siis, kui andmed on kustutatud.⁸⁰

Digitaaltõendite olulisus internetis toimepandud autoriõiguste rikkumiste menetlustes on kriminaalasjast. Alati ei ole kriminaalmenetluses vajalik internetis vaadeldavate veebilehtede materjalide salvestamine CD-le. Kriminaalmenetluses vajaminevate veebilehtede kohta koostatakse vaatlusprotokollid ning nendest tehakse väljatrükkid, mis jäetakse kriminaaltoimikusse vaatlusprotokolli lisadena vaatlusprotokolli juurde. Selleks, et tuvastada, kas on võimalik teost alla laadida, tuleb läbi viia uurimiseksperiment, mille käigus salvestatakse kõigepealt teos arvutisse ning uurimiseksperimenti lõpus kopeeritakse eelnevalt salvestatud fail CD-plaadile, mis jäetakse uurimiseksperimenti käigus koostatud protokolli juurde.⁸¹

Digitaalseid tõendeid kogutakse jälitustegevusega, erinevate päringutega, õigusabipalvetega, vaatlustega, uurimiseksperimentidega. Jälitustegevusega kogutud andmed säilitatakse väljatrükkidena või salvestatuna CD-le. Erinevate veebilehtede väljatrükkid säilitatakse kriminaaltoimikus, mahukad materjalid salvestatakse CD-le ja

⁷⁹ Käesolev töö, Lisa 3. Ekspertintervjuu Lõuna prefektuuri menetlejaga, *infra*, lk 49.

⁸⁰ Käesolev töö, Lisa 4. Ekspertintervjuu Põhja prefektuuri menetlejaga, *infra*, lk 50.

⁸¹ Käesolev töö, Lisa 4. Ekspertintervjuu Põhja prefektuuri menetlejaga, *infra*, lk 51.

samuti säilitakse kriminaaltoimikus. Arvuti kõvaketastest ja serveritest tehtud koopiad säilitatakse samuti vastavalt vajadusele. Autoriõiguste rikkumiste menetlusi on lõpetatud toimepaneja tuvastatamatuse tõttu või kui ei olnud võimalik tõendada isiku tahtlus kuriteo toimepanemiseks või kuriteo toimepaneja on surnud. Menetlusi pikendab lisaks õigusabipalvete keerukusele ka menetlejate suur töökoormus.⁸²

Intervjueeritava hinnangul oleks võimalik parendada digitaaltõendite kogumist menetlejate koormust vähendades. Samuti aitab tõendite kogumisele kaasa kiirem vastuste saamine õigusabitaotlustele. Menetlejad võiksid tunda teiste riikide seadusi. Seda eriti õigusabitaotluste puhul, kuna esineb juhuseid, kus tuleb vastust oodata 9-10 kuud ja siis selgub, et ei ole võimalik IP - aadressi omanikku välja selgitada, sest andmeid ei säilitata üldse või säilitatakse lühiajaliselt, tuvastamiseks vajatakse kohtu luba või õigusabitaotlustele ei vastata üldse.⁸³

Sama menetlejaga viidi läbi ekspertintervjuu 2012.a aprillis, kus ta selgitas, millised toimingud peab menetleja tegema peale avalduse laekumist politseisse:

1) tuvastama, kas kuriteoteade ja lisad sisaldavad kuriteo tunnuseid. Kuriteotunnuste olemasolu korral alustatakse kriminaalmenetlus ning edastatakse kuriteoteate esitajale teatis kriminaalmenetluse alustamise kohta. KrmS § 198 lg 1 kohaselt on uurimisasutus või prokuratuur kohustatud kuriteoteate saamisest alates 10 päeva jooksul teatama kuriteoteate esitajale kriminaalmenetluse alustamata jätmisest ning ei kohusta edastama teatist kriminaalmenetluse alustamise kohta,⁸⁴ kuid üldjuhul Põhja prefektuuri kriminaalbüroo majanduskuritegude talituses vastav teatis edastatakse kuriteoteate esitajale.

2) läbi viima uurimiseksperimenti. Internetikuritegude puhul on väga oluline teha esimesel võimalusel uurimiseksperiment, kuna veebileht võidakse sulgeda või muudetakse veebilehele sisenemise paroole vms. Eksperiment on vaja läbi viia, et teha kindlaks, kas ja mis ulatuses piraatkoopiaid levitatakse, samuti tuvastada faili üleslaadija isik. Eksperimenti puhul laetakse probleemset veebilehelt teoseid alla ja salvestatakse plaadile, mis lisatakse kriminaaltoimikusse.

⁸² Käesolev töö, Lisa 4. Ekspertintervjuu Põhja prefektuuri menetlejaga, *infra*, lk 51.

⁸³ Käesolev töö, Lisa 4. Ekspertintervjuu Põhja prefektuuri menetlejaga, *infra*, lk 51-52.

3) läbi viima vaatluse. Veebilehe vaatlusprotokollis märgitakse ära, kuidas toimub veebilehele sisenemine ning kirjeldatakse veebilehel olevat eeluurimiseks vajaliku täpsusega. Veebilehe vaatlusprotokollile lisatakse väljatrükiid vaadeldud veebilehtedest. Veebilehtede vaatluseks reeglina ei ole vajalik ekspertiise määrata.

4) esitama päringud. Päringuid saadetakse nii Eesti siseselt kui ka välisriikidesse. Päringuid tehakse eeluurimise käigus vajamineva informatsiooni saamiseks. Näiteks pangapäringutega tuvastatakse konto omanik, samuti saadakse teada, kas isik või ettevõtte omab pangas kontot ning vajadusel saadakse ka konto väljavõte. Vajadusel tehakse päringuid ettevõtetesse ja asutustesse dokumentide koopiade saamiseks, samuti kahtlustatava kohta informatsiooni kogumiseks jne Välisriikidesse saab reeglina teha Interpoli kaudu infopäringuid IP aadressi omaniku tuvastamiseks. Selleks edastatakse IP aadressi kasutamise kuupäeva ja kellaaja sekundilise täpsusega, samuti kasutamise asukoha koordinaadid.

5) esitama teistesse riikidesse õigusabipalved. Rahvusvahelise kriminaalmenetluselase koostöö keskasutus on Justiitsministeerium, mistõttu kõik õigusabipalved kriminaalmenetluses teostatakse läbi Riigiprokuratuuri.

6) korraldama ülekuulamised. Menetleja kuulab üle kannatanu või kannatanu esindaja, tunnistajad ja kahtlustatavad. Isikud tuleks üle kuulata nii kiiresti kui võimalik, et vältida olulise informatsiooni ununemist.⁸⁵

Neljandana intervjueriti Lääne prefektuuri menetlejat, kes on töötanud autoriõiguste rikkumiste menetlejana ühe aasta. Ta ei ole siiani menetlenud mitte ühtegi internetis toimepandud autoriõiguste rikkumist, kuid digitaaltõenditega on siiski kokku puutunud. Digitaaltõendeid kogutakse päringutega või nõudekirjadega vajalikku informatsiooni omavalt isikult või asutuselt. Muudes majanduskuritegude talituse menetlusalluvusse kuuluvates kriminaalasjades kogutud digitaalsed tõendid säilitatakse eraldi failidena selleks ettenähtud dokumendihaldusprogrammis (Delta) ning lisaks säilitatakse tõendit CD-plaadil, mis hoiustatakse asitõendite laos.⁸⁶

⁸⁵ Alas, „Autoriõiguste rikkumiste tuvastamine internetis“, *supra nota*, lk 13-14.

⁸⁶ Käesolev töö, Lisa 5. Ekspertintervjuu Lääne prefektuuri menetlejaga, *infra*, lk 54-55.

2.3. Ettepanekud digitaalsete tõendite kogumise ja käitlemise parendamiseks

Internetis toimepandud autoriõiguste rikkumiste kriminaalmenetlused on väga pikad ja aeganõudvad. Menetlusi pikendavad digitaaltõendite kogumise keerukus ja välisriikide õigusabipalved. Peamiselt lõpetatakse menetlusi prokuratuuri loal selle tõttu, et ei suudeta teo toimepanijat kindlaks teha, koosseis puudub või puudub avalik huvi.⁸⁷

Probleeme tekitavad veel antud kuritegude lahendamisel ressursi puudus. Kui aastal 2005 alustati intellektuaalse omandi vastaste kuritegude puhul 116 kriminaalmenetlust, siis järgnevatel aastatel on kriminaalmenetluste alustamiste arv vähenenud ning aastal 2012 alustati ainult 51 puhul kriminaalmenetlus.⁸⁸ See on otseses seoses 23.08.2005 allkirjastatud Laulasmaa deklaratsiooniga, millega määrati kindlaks kuritegevusega võitlemise prioriteedid.⁸⁹ Prioriteetsematesse valdkondadesse suunatakse rohkem ressursi. Seetõttu tuleks kaaluda intellektuaalomandi vastase kuritegude prioritseerimist.

Intellektuaalomandi vastased kuriteod on spetsiifilised ja nõuavad eriteadmisi, mistõttu on uute menetlejate leidmine raskendatud. Lisaks võib probleeme tekkida, kui spetsialistil, kelle ülesandeks on arvutist vajalikke tõendamiseesemete leidmine, ei oma näiteks riigisaladuse luba, kuid arvutis on riigisaladusega kaitstud infot. Seega on vaja inimesi, kellel on suurepäraseid oskused IT –alal, kuid oskus kriminaalmenetlusi läbi viia. Näiteks Lõuna prefektuuri juhtivmenetleja tõi intervjuus välja juhtumi, kus sellise isiku leidmine osutus väga keeruliseks.

USSS'i digitaaltõendite kogumise ja käitlemise juhendis on välja toodud vastavalt kuriteole küsimused, mida peaks välja selgitama menetlusosalistelt kriminaalmenetluse käigus. Autor leiab, et ka Eesti digitaaltõendite kogumise ja käitlemise juhendis oleks selliste näidisküsimuste olemasolu kasulik. See aitaks kriminaalmenetlejaid, kes alles alustavad tööd politseis ja ka neid, kes on küll varem töötanud kriminaalmenetlejana, kuid

⁸⁷ Kriminaalmenetluse seadustik § 200 – 1 ja § 202.

⁸⁸ Laanet, K., Lang, R., „Laulasmaa deklaratsioon kuritegevusevastase võitluse eelistustest“, (23.08.2005) <<http://www.just.ee/30140>> (09.05.2013).

⁸⁹ Justiitsministeerium, Aastaülevaated, „Kuritegevus Eestis 2012 ja lisad“, <<http://www.just.ee/15087>> (09.05.2013).

teistes valdkondades. Samuti saavad sellisest juhendist kasulikku informatsiooni ka sündmusele esmareageerija, kes peab mõnikord koos sündmuskohal oleva isikuga ootama menetlejat pikka aega. Selle käigus arendatakse vestlust ja kui küsida õigeid küsimusi, võib isik pahaaimamatult avaldada menetluse seisukohalt olulist informatsiooni.

Kriminaalmenetlejate koormuse vähendamiseks võiksid EFÜ ja Eesti Autorite Ühingu esindajad ise aktiivsemalt suhelda rikkujatega. Näiteks analüüsitud toimikutes oli kaks kaasust, kus EFÜ esindaja oli esitanud politseisse avalduse, et ettevõtetes suunatakse üldsusele autoriõigustega kaitstud teoseid. Eelnevalt oli EFÜ saatnud ettevõtete juhatustele informeeriva emaili selle kohta, et nende ettevõttel on kohustus sõlmida EFÜ'ga leping ja maksta ruutmeetri pealt tasu, kui nad soovivad üldsusele teoseid suunata. Kui peale paari meeldetuletust ettevõtte ei allkirjastanud lepingut ja tasu ei maksnud, tegi EFÜ esindaja politseile avalduse. Kõik menetlused kestsid seni kuni oli kahtlustatavatena ülekuulatud ettevõtete esindajad. Pärast seda pöördusid ettevõtete esindajad EFÜ poole lepingute sõlmimiseks. Seejärel puudus EFÜ'l huvi menetluse jätkamiseks ja menetlused lõpetati prokuratuuri loal. Selleks ajaks olid menetlejad pidanud, tegema päringuid, teostama sündmuskohavaatlused ning kannatanud ja tunnistajad üle kuulama. Mõlemas kaasuses ei saanud kahtlustatavad aru, miks EFÜ neile lepingud allkirjastamiseks saatis. Selliste kaasuste puhul võiks EFÜ aktiivsemalt üritada ettevõtete esindajatele selgeks teha, millise nende poolse tegevuse tõttu on nad kohustatud lepingu sõlmima. EFÜ on see, kes lepingust kasu saab, seega on nende huvi tasu maksmiseks lepingu sõlmimine, mitte ettevõtete karistamine.

Kolm intervjuueeritavat menetlejat toovad välja probleemina õigusabipalvete aeglase menetlemise. Põhja prefektuuri kriminaalmenetleja täpsustas, et välismaalt õigusabipalvel vastuse saamine võtab aega kuid. Lisaks säilitatakse IP- logisid erinevates riikides erinevalt, mistõttu võivad jõuda õigusabitaotlused välisriiki alles siis, kui andmed on kustutatud. Õigusabipalvetele vastuste saamine võtab küll kaua aega, kuid andmete aegumise probleemi lahendamiseks on loodud rahvusvahelise koostöö võrk G8 24/7. Igas riigis on sideisik, kellele selgitatakse, millist infot on vaja asitõendina salvestada. Seejärel võtab sideisik ühendust teenusepakkujaga, kes vajalikud andmed külmutab. Andmete väljaandmise taotlused tehakse õigusabipalvetega. Näiteks Norra pangast 10 miljonit dollarit varastanud ja politseiniku tapnud isiku otsimisel tegi Norra Suurbritanniale taotluse

säilitada digitaalandmeid, mis juhtisid kahtlustatavani. Hispaania politseinikud pidasid paar päeva hiljem kinni kahtlustatava ühest Hispaania internetikohvikust.⁹⁰

Erinevalt Eesti Infotehnoloogia kuritegude käsiraamatust on FBI ja USSS'i juhendites välja toodud, milliseid digitaaltõendeid võib leida erinevate kuriteoliikide puhul. Selline tähelepanu pööramine kindlatele aspektidele lihtsustab menetleja tööd ja vähendab vigade tegemist. Ka Eesti võiks kaaluda erinevatele kuriteoliikide omaste digitaaltõendite näidismekirja lisamist IT kuritegude menetlemise käsiraamatusse.

⁹⁰ Protocol Statement „The G8 24/7 Network of contact points“
<http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf> (23.03.2013)

KOKKUVÕTE

Käesoleva lõputöö eesmärk oli anda teoreetiline ülevaade internetis toimepandud autoriõiguste rikkumiste menetlemisel digitaalsete tõendite kogumisest, analüüsida Eesti menetluspraktikat, mille põhjal teha ettepanekuid digitaalsete tõendite kogumise parendamiseks.

Lõputöö eesmärk sai täidetud. Autor analüüsis Infotehnoloogia kuritegude menetlemise käsiraamatut ja USA FBI ning USSS'i digitaaltõendite kogumise ja käitlemise juhendeid, tuues välja ka USA juhendite erinevused: „*Bump/Shift/Feel*“ test, ning näidisküsimuste olemasolu esitamiseks menetlusosalistele ning digitaaltõendite nimekiri, mida tuleks otsida erinevate kuritegude puhul. Samuti analüüsis autor maailma suurimat internetis toimepandud autoriõiguste rikkumiste kaasust – Megaupload, andes ülevaate rahvusvahelisest koostööst. Eesti ainsas internetis toimepandud autoriõiguste rikkumiste ringkonnakohtu otsuses olid välja toodud digitaaltõendid, mis näitab nende usaldusväärset.

Lõputöö teises osas viidi läbi uuring tuvastamiseks digitaaltõendite kogumisega esinevaid probleeme. Selleks analüüsis autor prokuratuuri loal lõpetatud 14 autoriõiguste rikkumistega seotud kriminaalasja ja viis läbi ekspertintervjuu nelja kriminaalmenetlejaga. Peamiste probleemidena saab välja tuua menetluse pikkuse, mis tuleneb nii välisriikidest õigusabipalvetele vastamise aeglusest kui ka ressursi puudusest. Kuna tegemist on spetsiifilise valdkonnaga, vajavad menetlejad IT alaseid teadmisi. Ideaalne oleks, kui menetleja omaks IT – alast haridust.

Lisaks tuleks läbi viia IT alaseid koolitusi, et hoida menetlejaid kursis uute võimalustega näiteks võrk G8 24/7, tuletada meelde digitaaltõendite kogumise põhimõtted, analüüsida uusi kohtulahendeid või tutvustada teiste riikide seadusi õigusabipalvete osas

Menetlejate koormuse vähendamiseks võiks EFÜ proovida rohkem ettevõtetega suhelda. Tihti peale ei piisa ainult e-maili saatmisest, et ettevõtte esindaja mõistaks, mida nad rikuvad, vaid tuleb helistada või esindajaga kokku saada. EFÜ saab sõlmitud lepingutest kasu, seega peaksid nad rohkem olukorra selgitamisega vaeva nägema.

FBI ja USSS'i juhendites on välja toodud, milliseid digitaaltõendeid võib leida erinevate kuriteoliikide puhul. Samuti on juhendites välja toodud küsimused, mida menetleja võiks menetlusosalistelt küsida. Selline tähelepanu pööramine kindlatele aspektidele lihtsustab menetleja tööd ja vähendab vigade tegemist. Ka Eesti võiks kaaluda erinevatele kuriteoliikide omaste digitaaltõendite näidismekirja ja -küsimustiku lisamist IT kuritegude menetlemise käsiraamatusse.

Antud teemat saab edasi arendada, kus oleks võimalik läbi viia ekspertintervjuusid lisaks menetlejatele ka veel prokuröride ja kohtunikega. Samuti on võimalik analüüsida kriminaaltoimikuid, mis on läinud kohtusse.

SUMMARY

Nowadays, in the rapidly changing world the law enforcement agencies are dealing with the growing problem of crime in the digital environment – on the internet. The objective of this thesis was to give a theoretical overview of gathering digital evidence on copyright infringements on the internet, to analyse Estonian procedural practice and to suggest improvements about the way digital evidence is gathered. The thesis is empirical and consists of 44 pages. In the first part of the thesis, the author analysed Estonian and USA handbooks on gathering digital evidence, the largest case of internet piracy Megaupload and the only Estonian District Court case on the subject of copyright infringements. In the second part the author conducted a survey to find out the problems in gathering digital evidence. In this survey the author examined 14 criminal cases involving copyright infringements which were terminated by the district attorney and interviewed 4 investigators. The main problem that has arisen from the survey is the length of the investigation which is directly linked to shortage of resources and the length of time it takes to receive mutual legal assistance from foreign countries. Since the field is very specific the investigators should have IT skills. Ideally the investigators should have degrees in IT. All investigators should have regular IT- related training to keep them up to date on the latest changes and procedures and attend refresher courses on digital evidence gathering. To relieve some of the workload of the investigators the rights holders should communicate more with the companies. The FBI and the USSS manuals on gathering digital evidence have example questions for the all the relevant parties, and examples of what kind of digital evidence can be found in various types of crime. These two points should be added to the Estonian version of the Handbook on gathering digital evidence.

VIIDATUD ALLIKATE LOETELU

- Phare mestiprojekt EE 03 IB JH 04, „Infotehnoloogiakuritegude menetlemise käsiraamat“, 2001, lk 40.
- Maurer, K., „Õigusleksikon“, Tallinn: Interlex kirjastus, 2000, lk 73.
- „Väike entsüklopeedia“, Tallinn: Eesti entsüklopeedia kirjastuse AS, 2006, lk 215.
- Autoriõiguse seadus, 11.11.1992, jõustunud 12.12.1992 - RT - I 1992, 49, 615, §80-1.
- Vallaste, H. „E-teatmik“, <<http://www.vallaste.ee/index.htm?Type=UserId&otsing=726>> (28.03.2013).
- Tõnis L. „Arvutiabi“ <<http://web.zone.ee/abi2/BitTorrent/bitTorrent.html#BitTorrent>> (31.03.2013).
- „Internet World Stats“ <<http://www.internetworldstats.com/stats4.htm>> (05.04.2012).
- Michal, K. „Intellektuaalomandi reformist“ <http://juridica.ee/get_doc.php?id=1845> (01.12.2013).
- Kelli, A. „Intellektuaalomandi seadusandluse kodifitseerimisest“, ettekanne seminaril Criminal enforcement of Intellectual Property Rights, 16.03.2012.
- Press release <<http://www.info.gov.hk/gia/general/201201/20/P201201200626.htm>> (02.09.2012).
- Tänavsuu, T. „Kim Dotcom'i eestlasest abilist ähvardab Amerikas 55 aastane vangistus“, Eesti Ekspress, 14.03.2013, <<http://www.ekspress.ee/news/paevauudised/eestiudised/kim-dotcomi-eestlasest-abilist-ahvardab-ameerikas-55-aastane-vangistus.d?id=65816470>> (14.03.2013).
- The United States Department of Justice: Intellectual Property Task Force <<http://www.justice.gov/dag/iptaskforce/>> (02.02.2013)
- Alas, M., „Autoriõiguste rikkumiste tuvastamine internetis“, kursusetöö, Sisekaitseakadeemia (2012), lk 6.
- Kultuuriministeerium, Autor.ee Intellektuaalomandi infovärv <<http://www.autor.ee/est/vasak/autoriõigused/Autoriisiklikud>> (01.03.2013).
- Karistuseseadustik, 06.06.2001, jõustunud 01.09.2004, RT – I 2001, 61, 364, ptk 14.
- Sootak, J., Pikamäe, P., „Karistuseseadustiku kommenteeritud väljaanne“ (Tallinn: Juura 2002), lk 600.
- Künnapas, K. „Justiitsminister: õigusabi seaduse peamine eesmärk on kvaliteetne õigusabi vähekindlustatud elanikel“ 11.02.2005 <<http://www.just.ee/6641>> (08.05.2012).
- Terminibaas ESTERM <<http://mt.legaltext.ee/esterm/>> (05.04.2012).
- Kriminaalmenetluse seadustik 12.02.2003, jõustunud 01.07.2004, RT I 2003, 27, 166, §193.
- Laptev, P ettekanne „Digitaalsete tõendite kohtuekspertiis“ USPTO konverents, 2010.
- Baum, A. ettekanne „Current issues in digital copyright piracy“, USPTO Digitaalpiraatluse konverentsil, 2010.
- Harju Maakohtu otsus Kristjan Luik, nr 1-11-12296, 07.02.2011, lk 10-11.
- Tallinna Ringkonnakohtu otsus Kristjan Luik, nr 1-11-12296, 01.06.2012, lk 4-5.
- Elunurm, S., „Euroopa autoriõigus reformide teel“, 24.05.2010, <<http://www.blslawfirm.com/et/bls-estonia/uudised/uudis?nid=483>> (20.03.2013)
- U.S. Department of Justice Federal Bureau of Investigation Digital evidence field guide: What every peace officer must know, p 2.

U.S. Department of Homeland Security United States Secret Service Best Practice for Seizing Electronic Evidence v.3: A Pocket Guide for First Responders, No 2.

Laanet, K., Lang, R., „Laulasmaa deklaratsioon kuritegevusevastase võitluse eelistustest“, (23.08.2005) <<http://www.just.ee/30140>> (09.05.2013).

Justiitsministeerium, Aastaülevaated, „Kuritegevus Eestis 2012 ja lisad“, <<http://www.just.ee/15087>> (09.05.2013).

Protocol Statement „The G8 24/7 Network of contact points“ <http://www.oas.org/juridico/english/cyb_pry_G8_network.pdf> (23.03.2013)

LISA 1. PÕHJA PREFEKTUURI KRIMINAALTOIMIKUTE VAATLUS

Kriminaalasi	Kvalifikatsioon	Menetluse kestvus	Kahtlustatavad	Vahistamine
nr. 09230105119	KarS §222 lg1	01.04.2009-01.09.2011	1	ei
nr. 08230114529	KarS §223 lg1,3	23.12.2008-22.06.2011	1, firma esindaja	ei
nr. 07230101109	KarS §223 lg1	11.01.2008-05.10.2011	1, firma esindaja	ei
nr. 122301070385	KarS §222 lg1	04.06.2012-07.09.2012	ei	ei
nr. 09230102213	KarS §222 lg1	06.02.2009-26.03.2012	ei	ei
nr. 09230110839	KarS §223 lg3	08.07.2009-10.05.2012	2	ei
nr. 082301060115	KarS §222 lg1	22.04.2008-06.04.2009	ei	ei
nr. 11230100497	KarS §224 lg1	12.01.2011-27.02.2013	3	ei
nr. 12230117947	KarS §226 lg2	20.12.2012-05.03.2013	ei	ei
nr. 08230106196	KarS §219 lg1	22.05.2008-30.12.2011	1	ei
nr. 11230105380	KarS §226 lg2	25.04.2011-29.20.2012	ei	ei
nr. 06230100521	KarS §220 lg1	28.03.2006 - 07.04.2010	3	ei
nr. 08230116558	KarS §222 lg1	03.10.2008-24.05.2011	ei	ei
nr. 08230107902	KarS §223 lg1	21.05.2008-29.02.2012	1	ei
Kriminaalasi	Läbiotsimine	Tolmeapanemine	Ekspertisi liigid	Menetluskulud
nr. 09230105119	ei	Eesti	ei	76.70 €
nr. 08230114529	ei	Eesti	ei	ei
nr. 07230101109	ei	Eesti	ei	ei
nr. 122301070385	ei	Eesti	ei	ei
nr. 09230102213	ei	USA	ei	ei
nr. 09230110839	ei	Eesti	ei	ei
nr. 082301060115	ei	Eesti	ei	ei
nr. 11230100497	2	Eesti	tarkvara 2	ei
nr. 12230117947	ei	Eesti	eksperdi ütlused	ei
nr. 08230106196	ei	Eestis	ei	ei
nr. 11230105380	ei	Eestis	ei	ei
nr. 06230100521	ei	Eesti	ei	ei
nr. 08230116558	ei	Eesti	ei	ei
nr. 08230107902	ei	Eesti	kujutise ekspertiis	ei

Kriminaalasi	Tõendite kogumine	
nr. 09230105119	vaatus; uurimiseksperiment+salvestus DVD, asitõendi vaatus;	
nr. 08230114529	4 sündmudkoha vaatluse lisa DVD'l, veebilehe vaatus	
nr. 07230101109	2 sündmuskoha vaatus lisa dvd	
nr. 12230107038	väljatrükk binaarsel kujul	
nr. 09230102213	asitõendi vaatus	
nr. 09230110839	asitõendi vaatus; sündmuskohavaatus;	
nr. 08230106011	film dvd'l asitõendi vaatus	
nr. 11230100497	asitõendi vaatus x5 (veebi leht; 4tarkvara); 6 isiku äratundmiseks esitamise; telefoni väljavõte, 2x1P jälitus	
nr. 12230117947	2x veebilehe vaatus;	
nr. 08230106196	ei	
nr. 11230105380	ei	
nr. 06230100521	väljatrükk	
nr. 08230116558	väljatrükk	
nr. 08230107902	asitõendi vaatus; asitõendi (veebilehe) vaatus; väljatrükk	
Kriminaalasi	Päringud	Päringud päevades
nr. 09230105119	2x EAÜ;	164
nr. 08230114529	4x EFÜ, kahtlustatav	4; 3; 8
nr. 07230101109	3x EFÜ	3; 2; 8
nr. 12230107038	Harju Maakohus	3
nr. 09230102213	ei	
nr. 09230110839	Elkdata OÜ	02/12/2009
nr. 08230106011	ei	
nr. 11230100497	3x osta.ee; okidoki; Danske Bank; AS Krediidibank; dokumendi nõue HM; mupo	6; 5; 12; 16; 0; 6; 0; 6
nr. 12230117947	ei	ei
nr. 08230106196	Eesti Hariduse ja Teaduse Andmesidevõrk; päring HM	13; 2
nr. 11230105380	Zone Media OÜ; EENet; Eesti Interneti Sihtasutus; OÜ Virtual.com; OÜ Holz Prof dok nõu	2; 1; 14; 1; 13
nr. 06230100521	foorum.private.pri.ee; Elion2; Starman	3; 5; 8; 2
nr. 08230116558	Zone Media OÜ; EeNet; HM dok nõue; Starman AS; SEB; Hansapank2	16; 12; 1; 5; 5; 13; 21
nr. 08230107902	OÜ Bestok KV; Tallinna ettevõtlusamet; Tallinna Kultuuriväärtuste Amet; Tallinna Ettevõtlusamet; EENet	8; 22; 1; 14 11 2008; 4; 10

Kirjumaalasi	Digitaaltöendite hoiustamine	Lõpetamine
nr. 09230105119	dvd plaat plaadi ümbrises ja ümbrikus, toimikus	KrM/S § 202 lg 1
nr. 08230114529	dvd plaat plaadi ümbrises ja ümbrikus, toimikus	KrM/S § 202 lg 7
nr. 07230101109	dvd plaat ümbrikus, toimikus	KrM/S § 202 lg 7
nr. 122301070385	ei	KrM/S § 200 ¹
nr. 09230102213	dvd plaat ümbrikus, toimikus	KrM/S § 200 ¹
nr. 09230110839	ei	KrM/S § 200 - § 199 lg 1 p1
nr. 082301060115	dvd plaat plaadi ümbrises ja ümbrikus, toimikus	KrM/S § 200 - § 199 lg 1 p1
nr. 11230100497	piraattarkvara 6 M. Office; 12 M. Windows 7 Ultimate hävitada	KrM/S § 200 - § 199 lg 1 p4
nr. 12230117947	ei	KrM/S § 200 - § 199 lg 1 p1
nr. 08230106196	ei	KrM/S § 200 - § 199 lg 1 p1
nr. 11230105380	ei	KrM/S § 200 - § 199 lg 1 p1
nr. 06230100521	ei	KrM/S § 200 - § 199 lg 1 p1
nr. 08230116558	ei	KrM/S § 200 ¹
nr. 08230107902	ei	KrM/S § 200 - § 199 lg 1 p1

LISA 2. EKSPERTINTERVJUU IDA PREFEKTUURI MENETELJAGA

Ekspertintervjuu kriminaalmenetlejaga

Lõputöö teema: „Digitaalsete tõendite kogumise ja käitlemise erisused autoriõiguste rikkumiste kriminaalmenetluses“

Intervjuueerija: Marit Alas, Politsei- ja Piirivalveamet, Põhja Prefektuur, Ida-Harju politseijaoskond (Sisekaitseakadeemia, Politsei kaugõppe rühma PK111 üliõpilane)

Kuupäev: 21.02.2013. a

Sissejuhatus

Kui kaua olete töötanud autoriõiguste rikkumiste menetlejana? 10. a

Kellena Te hetkel töötate? m. h. flejana

Kui palju internetis toime pandud autoriõiguste rikkumisi Te aastas keskmiselt menetlete? keskmiselt 1-2 kriminaalasja

1. Milliseid probleeme esineb digitaaltõenditega internetis toime pandud autoriõiguste rikkumiste menetlemisel?

Vastus: tõendiallkate tuvastamine ja kogumine

2. Mis osa on digitaaltõenditel internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: põhiosa

3. Milliseid digitaaltõendeid on Teie praktikas kasutatud internetis toime pandud autoriõiguste rikkumiste kriminaalasjades?

Vastus: andmekandjatel leiduv informatsioon

4. Kuidas kogutakse Teie praktikas digitaalseid tõendeid?

Vastus: sündmuskohtl läbiotsmiskohas, asitõendi

5. Kuidas säilitatakse digitaalseid tõendeid?

Vastus: andmekandjatel

6. Mis põhjusel olete autoriõiguste rikkumiste kriminaalmenetlusi prokuröri loal lõpetanud?

Vastus: nt, ei leitud tõendite tõttu, krim. menetluse

7. Milline toiming pikendab enim internetis toime pandud autoriõiguste rikkumiste kriminaalmenetlust?

Vastus: infotehnoloogiatekspertis, õigusabi paeve

8. Kuidas parendada digitaaltõendite kogumist ja käitlemist internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: IT koostiste saamine, töövahendite uuendamine, koostupraktika

LISA 3. EKSPERTINTERVJUU LÕUNA PREFEKTUURI MENETELJAGA

Lõputöö teema: „Digitaalsete tõendite kogumise ja käitlemise erisused autoriõiguste rikkumiste kriminaalmenetluses“

Inetrvjuerija: Marit Alas, Politsei- ja Piirivalveamet, Põhja Prefektuur, Ida-Harju politseijaoskond (Sisekaitseakadeemia, Politsei kaugõppe rühma PK111 üliõpilane)

Kuupäev:04.03.2013

Sissejuhatus

1. Kui kaua olete töötanud autoriõiguste rikkumiste menetlejana?

Vastus: Autoriõiguste rikkumistega tegelesin põhitööna aprill 2004 – juuli 2008 (menetlus/jälitus). Sel ajal moodustasid autoriõiguste rikkumiste põhiosa piraatkoopiatega kauplemine, muusikateoste ebaseaduslik esitamine, arvutiprogrammide ebaseadusliku kasutamise seotud süüteod jmt. Peale seda on minu menetluses olnud ainult mõned autoriõiguste rikkumisega seotud kriminaalasjad, millest üks on seotud autoriõigusega kaitstud teoste ilma autori loata reprodutseerimise ja levitamise internetis ning see võib Teile ehk huvi pakkuda.

2. Kellena Te hetkel töötate?

Vastus: Lõuna prefektuuri majanduskuritegude talituse juhtivuurijana.

3. Kui palju internetis toime pandud autoriõiguste rikkumisi Te aastas keskmiselt menetlete?

Vastus: Minu põhitöö ei ole hetkel kuritegude menetlemine ning autoriõigusega seotud kriminaalasjadest on minu menetluses on ainult üks, juba eelmainitud kriminaalasi. Mis puudutab muidugi autoriõigustega seotud rikkumiste menetlemisi Lõuna prefektuuris üldse, siis võin öelda, et selliseid kriminaalasju on väga vähe ning meil toimub ressursi puudumisel taoliste kriminaalasjade menetlemine avalduse põhisedelt.

4. Milliseid probleeme esineb digitaaltõenditega internetis toime pandud autoriõiguste rikkumiste menetlemisel?

Vastus: Probleemid seisnevad eelkõige selles, kuidas neid üldse saada. Ühe moodusena on läbiotsimise käigus ära võtta isiku arvuti ning leida sealt tõendeid. Sellisel juhul kas tehakse Encase programmi abil arvuti koopiat, mida siis tõendite otsimise eesmärgil läbi

vaadatakse või vaadatakse jällegi Encase programmi abil läbi arvuti ise ning siis juba otsustatakse vastavalt vajadusele koopia tegemine. Saadud andmed vormistatakse vaatlusprotokolliga ning siin on võimalik kopeerida tõenduslikku tähtsust omavate failide sisu otse vaatlusprotokolli või need eraldi lisada (protokolli lisad). Sõltuvalt asja keerukusest on võimalik tõenduslikku tähtsust omavad failid salvestada eraldi andmekandjale ning lisada need protokolli juurde. Kui digitaalsed tõendid saadakse läbiotsimise käigus ja kopeerida kohapeal ei saa, siis on võimalik pakkida ja pitseerida arvuti ning avada see kohapeal isiku juuresolekul ja panna kopeerima või siis kaasasoleva USB abil fikseerida konkreetne räsiväärtus, vältimaks hilisemaid pretensioone, et a'la midagi muudeti või lisati juurde politsei poolt.

Probleemiks on kindlasti vilunud arvutikasutajate poolt enda IP-aadressi varjamine internetikelmuste toimepanemisel (jäetakse mulje, et on mingile leheküljele sisenetud teise riigi teenusepakkuja aadressivahemikku jäävalt aadressilt). Samasugune probleem välisoperaatorite poolt kasutatavate meiliaadressidega, kust on võimalik saada andmeid ainult õigusabi palve raames ning võtab üldjuhul mõistusevastaselt palju aega. Jälitustegevusega andmete saamiseks probleemiks arvutiühenduse tuvastamine saadud andmete interpreteerimine.

5. Mis osa on digitaaltõenditel internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: Sõltuvalt juhtumist omavad need määravat tähtsust (minu kogemuse põhjal).

6. Milliseid digitaaltõendeid on Teie praktikas kasutatud internetis toime pandud autoriõiguste rikkumiste kriminaalasjades?

Vastus: Jälitustegevusega saadud digitaalsed tõendid, meilid, IP aadressid, avalikes internetiandmebaasides sisalduv teave (foorumid, oksjonikeskkonnad – osta.ee, oki.doki jmt, internetiarhiiv – internet archive jne).

7. Kuidas kogutakse Teie praktikas digitaalseid tõendeid?

Vastus: Jälitustegevuse ja avalikus internetiruumis sisalduvate andmete kogumise läbi.

8. Kuidas säilitatakse digitaalseid tõendeid?

Vastus: Avalikust internetiruumist saadud tõendid ekraanipildi ja foto abil väljatrüki kujul ja/või elektroonilise andmekandja peal (C-R, DVD-R, kõvaketas jmt). Jälitustegevusega saadud andmed elektroonilise andmekandjate peal, väljatrüki näol jmt.

9. Mis põhjusel olete autoriõiguste rikkumiste kriminaalmenetlusi prokuröri loal lõpetanud?

Vastus: Lõpetanud olen tõendamatusena (autoriõiguste rikkumisega mitteseotud menetluse käigus ära võetud ja vaadeldud arvutis tuvastati ettevõtluses kasutatav arvutiprogramm, mille kohta ei olnud arvuti omanikul esitada litsentsi), kuna isik keeldus ütluste andmisest ja puudus võimalus tuvastada, kellele kuulus/kes kasutas arvutit programmide installimise ajal (täpsustus: isik ei olnud ettevõtte juhatuse liige ajal, kuid failid arvutis loodi ning ei olnud täpselt selge, kes oli arvuti algne omanik). Samuti olen lõpetanud koosseisu puudumisega kriminaalasja, milles autode müügikuulutustega tegeleva firma väidatel teine firma kopeeris nende kuulutusi ja avaldas need enda lehel.

10. Milline toiming pikendab enim internetis toime pandud autoriõiguste rikkumiste kriminaalmenetlust?

Vastus: Õigusabitaotlused ja IT-alaseid teadmisi nõudvate andmete interpreteerimine.

11. Kuidas parendada digitaaltõendite kogumist ja käsitlemist internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: Mis puudutab internetipiraatlust, siis see on võitlus „tuuleveskitega“. Aitaks ehk internetikasutaja täiendav maksustamine (a’la tühja kasseti maks). See ei puuduta muidugi ärilisel eesmärgil piraattoodete levitamist. Eelkõige on tähtis aga IT-toe olemasolu prefektuurides (ei pea silmas SMIT’i). Praegustes IT-kuritegevusega tegelevate gruppide koosseisus puuduvad IT haridusega spetsialistid. Arvatavasti on palju loota, et neid tuleks politseinike hulgast, kuid spetsialistina (riigisaladuste käitlemise õigusega) oleks vastavate eriteadmistega isikut võimalik kindlasti kaasata (palgaküsimus). Enda kogemuste pinnal meenub juhtum (seda võib käsitleda ka küsimuse nr.4 vastuse osana), kus jälitustegevusega saadud andmed oli vaja saata

ekspertiisi, kuid eksperdil puudus õigus töötada riigisaladusega, endal aga puudusid ülisuure andmemahu seast ekspertiisiks vajalike andmete väljavalimiseks piisavad oskused. Hädast aitas suure hilinemisega välja politseinikust IT-spetsialistiks spetsialiseerunud ametnik, kes nüüdseks on politseist lahkunud.

LISA 4. EKSPERTINTERVJUU PÕHJA PREFEKTUURI MENETLEJAGA

Lõputöö teema: „Digitaalsete tõendite kogumise ja käitlemise erisused autoriõiguste rikkumiste kriminaalmenetluses“

Inetrvjuerija: Marit Alas, Politsei- ja Piirivalveamet, Põhja Prefektuur, Ida-Harju politseijaoskond (Sisekaitseakadeemia, Politsei kaugõppe rühma PK1111 üliõpilane)

Kuupäev:.....

Sissejuhatus

Kui kaua olete töötanud autoriõiguste rikkumiste menetlejana?- 8 aastat

Kellena Te hetkel töötate? - majanduskuritegude talituse eriasjade uurijana (Intellektuaalse omandi vastaste kuritegude kriminaalmenetlus)

Kui palju internetis toime pandud autoriõiguste rikkumisi Te aastas keskmiselt menetlete?

-

Olenevalt aastast- keskmiselt 5-10

1. Milliseid probleeme esineb digitaaltõenditega internetis toime pandud autoriõiguste rikkumiste menetlemisel?

Vastus: Probleemid on : a) IP aadressi omanikku ei ole võimalik tuvastada, kuna arvutikasutaja oskab oma IP-aadressi varjata. b) välismaal asuvate IP-aadressside omanike ning välisoperaatorite meiliaadresside kasutajate tuvastamine. Välismaalt on võimalik andmeid saada ainult õigusabipalvete raames, mis võtab üldjuhul mitu kuud aega. Samuti raskendab positiivsete vastuste saamist välismaalt asjaolu, et Eesti Vabariigi ja välisriikide seadusandlused on erinevad, mistõttu ei ole võimalik kõikides välisriikides meie õigusabitaotlust rahuldada, kuna selliseks tegevuseks on vajalik kohtu luba jne. c) IP-logisid säilitatakse erinevates riikides erinevalt, mistõttu jõuavad õigusabitaotlused välisriiki alles siis, kui andmed on aegunud.

2. Mis osa on digitaaltõenditel internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: oleneb kriminaalasjast. Alati ei ole kriminaalmenetluses vajalik internetis vaadeldavate veebilehtede materjale salvestada CD-le. Kriminaalmenetluses vajaminevate

veebilehtede kohta koostatakse vaatlusprotokollid ning nendest tehakse väljatrükkid, mis jäetakse kriminaaltoimikusse vaatlusprotokolli lisana vaatlusprotokolli juurde. Kui on tegemist uurimiseksperimendiga, siis tuleb tulemus salvestada CD-plaadile. (Näiteks kui on tegemist veebilehtedega, kus toimub näiteks muusikateoste või filmide jne. jagamine torrentfailide abil.) Selleks, et tuvastada, kas on võimalik mingit teost alla laadida, tuleb läbi viia uurimiseksperiment, mille käigus salvestatakse kõigepealt teos arvutisse ning uurimiseksperimendi lõpus kopeeritakse eelnevalt salvestatud fail CD-plaadile.

3. Milliseid digitaaltõendeid on Teie praktikas kasutatud internetis toime pandud autoriõiguste rikkumiste kriminaalasjades?

Vastus: Jälitustegevusega saadud digitaalsed tõendid, meilid, IP aadressid, avalikes internetiandmebaasides sisalduv teave (foorumid, oksjonikeskkonnad – osta.ee, oki.doki jmt, internetiarhiiv – internet archive jne).

4. Kuidas kogutakse Teie praktikas digitaalseid tõendeid?

Vastus: jälitustegevusega, erinevate päringutega, õigusabipalvetega, vaatlustega, uurimiseksperimentidega.

5. Kuidas säilitatakse digitaalseid tõendeid?

Vastus: jälitustegevusega kogutud andmed säilitatakse väljatrükkidena või salvestatuna CD-le. Erinevate veebilehtede väljatrükkid säilitatakse kriminaaltoimikus, mahukad materjalid salvestatakse CD-le ja samuti säilitakse kriminaaltoimikus. Arvuti kõvaketastest ja serveritest tehtud koopiad säilitatakse samuti vastavalt vajadusele.

6. Mis põhjusel olete autoriõiguste rikkumiste kriminaalmenetlusi prokuröri loal lõpetanud?

Vastus: kuriteo toimepanejat ei ole olnud võimalik tuvastada, ei ole olnud võimalik tõendada isiku tahtlus kuriteo toimepanemiseks, kuriteo toimepaneja on surnud.

7. Milline toiming pikendab enim internetis toime pandud autoriõiguste rikkumiste kriminaalmenetlust?

Vastus: õigusabitaotlused teistesse riikidesse, menetluses olevate kriminaalasjade arv on väga suur

8. Kuidas parendada digitaaltõendite kogumist ja käsitlemist internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: menetleja koormuse vähendamine, kiirem õigusabitaotlustele vastuste saamine, teiste riikide seadusandluse tundmine (eriti õigusabitaotluste puhul, kuna esineb juhuseid, kus ootad 9-10 kuud vastust õigusabipalvele ja siis selgub vastusest, et ei ole võimalik IP

aadressi omanikku välja selgitada, sest andmeid ei säilitata üldse või säilitatakse lühiajaliselt, tuvastamiseks vajatakse kohtu luba, õigusabitaotlestele ei vastata üldse.

LISA 5. EKSPERTINTERVJUU LÄÄNE PREFEKTUURI MENETLEJAGA

Lõputöö teema: „Digitaalsete tõendite kogumise ja käitlemise erisused autoriõiguste rikkumiste kriminaalmenetluses“

Inetrvjuueerija: Marit Alas, Politsei- ja Piirivalveamet, Põhja Prefektuur, Ida-Harju politseijaoskond (Sisekaitseakadeemia, Politsei kaugõppe rühma PK111 üliõpilane)

Kuupäev: 28.03.2013

Sissejuhatus

Kui kaua olete töötanud autoriõiguste rikkumiste menetlejana? umbes 1 aasta.

Kellena Te hetkel töötate? uurijana.

Kui palju internetis toime pandud autoriõiguste rikkumisi Te aastas keskmiselt menetlete? Hetkeseisuga ei ole menetlenud ühtegi internetis toimepandud autoriõiguste rikkumist.

1. Milliseid probleeme esineb digitaaltõenditega internetis toime pandud autoriõiguste rikkumiste menetlemisel?

Vastus: Kuna olen sellega (autoriõigused) suhteliselt vähe kokkupuutunud ning ma ei ole konkreetselt internetis toimepandud autoriõiguste rikkumisi menetlenud, ei oska seetõttu probleeme digitaaltõenditega välja tuua.

2. Mis osa on digitaaltõenditel internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: vt. eelmine vastus.

3. Milliseid digitaaltõendeid on Teie praktikas kasutatud internetis toime pandud autoriõiguste rikkumiste kriminaalasjades?

Vastus: Ei ole menetlenud internetis toimepandud autoriõiguste rikkumisi.

4. Kuidas kogutakse Teie praktikas digitaalseid tõendeid?

Vastus: Digitaaltõendeid kogutakse päringutega/nõudekirjadega võimalikult vajalikku informatsiooni omavalt isikult või asutuselt.

5. Kuidas säilitatakse digitaalseid tõendeid?

Vastus: Muudes majandusalastest kriminaalasjades (mitte autoriõigustega seotud asjades) kogutud digitaalsed tõendid säilitatakse eraldi failidena selleks ettenähtud

dokumendihaldusprogrammis (Delta) ning lisaks säilitatakse tõendit CD-plaadil, mis hoiustatakse asitõendite laos.

6. Mis põhjusel olete autoriõiguste rikkumiste kriminaalmenetlusi prokuröri loal lõpetanud?

Vastus: Ei ole lõpetanud.

7. Milline toiming pikendab enim internetis toime pandud autoriõiguste rikkumiste kriminaalmenetlust?

Vastus: Ei oska vastata.

8. Kuidas parendada digitaaltõendite kogumist ja käsitlemist internetis toime pandud autoriõiguste rikkumiste kriminaalmenetluses?

Vastus: Ei oska vastata.