TARTU ÜLIKOOL
SOTSIAALTEADUSTE VALDKOND

ÕIGUSTEADUSKOND

Karistusõiguse osakond

Mari Luuk

DIGITAALSETE TÕENDITE KASUTAMISE ERISUSED

MAGISTRITÖÖ

Juhendaja: professor Jaan Ginter

Tartu

2017

Sisukord

SISSEJUHATUS

Igas ühiskonnas on aja jooksul välja kujunenud teatud tavad, kombed, kirjapandud õigus, mille rikkumisele võib järgneda tagajärg. Enim isiku õigustesse sekkuv riigi reaktsioon on kriminaalkaristuse (edaspidi karistus) kohaldamine. Karistuse eelduseks on kuriteokoosseisule vastava teo tuvastamine kohtumenetluse käigus. Selleks, et kohtumenetluseni jõuda, tuleb läbida kohtueelne menetlus. Nii kohtueelses kui ka kohtumenetluses peavad järgima selle osalised seaduses sätestatut. Eesti Vabariigi põhiseaduses[1] § 22 lauses 1 on sätestatud, et kedagi ei tohi käsitada kuriteos süüdi olevana enne, kui tema kohta on jõustunud süüdimõistev kohtuotsus.

Karistusõigus on lahutamatult seotud kriminaalmenetlusõigusega. Kriminaalmenetlusõigus näitab ette tee, kuidas seaduslikult jõuda kuriteo toimepannud isikuni, kuidas seaduslikult välja selgitada olulised tõendid. Eestis on kriminaalmenetluse reeglid paika pandud Kriminaalmenetluse seadustikus[2] (edaspidi ka KrMS). Samas tuleb arvestada ka ühiskonnas toimuvate protsessidega, millest tulenevalt on üha olulisem rahvusvaheline koostöö kriminaalasjade menetlemisel.

Kriminaalmenetluse seadustiku§ 1 lg 1 kohaselt sätestatakse nimetatud seadustikus kuritegude kohtueelse menetluse ja kohtumenetluse kord ning kriminaalasjas tehtud lahendi täitmisele pööramise kord. Samuti on nimetatud seadustikus sätestatud jälitustoimingute tegemise alused ja kord.

Kriminaalmenetlusõiguses tuleb arvestada Eesti Vabariigi põhiseadusega, rahvusvahelise õiguse üldtunnustatud põhimõtete ja normidega ning Eestile siduvate välislepingutega, samuti kriminaalmenetluse seadustiku enda ja kriminaalmenetlust sätestavate muude õigusaktidega. Lisaks on kriminaalmenetlusõiguse allikad ka Riigikohtu lahendid küsimustes, mida ei ole lahendatud muudes kriminaalmenetlusõiguse allikates, kuid on tõusetunud seaduse kohaldamisel.

Kriminaalmenetluse tõukejõuks ja raamistikuks on printsiibid, millele on ühe või teise riigi kriminaalõigus üles ehitatud. Inimene peab tänu nendele printsiipidele teadma, mis teda ees ootab ja printsiibid kohustavad ka riike teatud tegude puhul teatud viisil käituma. Selliste printsiipide olemasolu ja järgimine tagab õiguse rakendamisel subjektide võrdse kohtlemise.

[1] Põhiseadus - RT I, 15.05.2015, 2
[2] Kriminaalmenetluse seadustik - RT I, 31.12.2016, 16

Menetlust toimetatakse kokkulepitud ja kohustuslike reeglite järgi, mitte aga valikuliselt. Printsiipidega tuleb arvestada ka rahvusvahelise õiguskorra ülesehitamisel.

Keelatu-lubatu piiritlemise vajaduse iseloomustamiseks toob käeoleva töö autor siinkohal välja Jules Colemani ja Scott Shapiro koostatud kogumikus *The Oxford Handbook of Jurisprudence and philosophy of law* Christopher Kutzi poolt väljatoodud mõtte: „ Kriminaalõiguse normid on traditsiooniliselt kaitsnud kõige olulisemaid huvisid elus – keha puutumatust ning valduse kaitset. Kaitstes neid huvisid lubamatu sekkumise eest, teeb kriminaalõigus võimalikuks ühiskondliku elu võimalikuks tehes ühiskondliku usalduse võimalikuks.“[3]

Magistritöö on kirjutatud eesti keeles, kokkuvõte vene keeles. Töö on kirjutatud 78-l leheküljel.

Magistritöö läbivad teemad on : Digitaalsed tõendid ja nende erinevused klassikalistest tõenditest, digitaalsete tõendite leidmine, kasutatavus ja säilitamine, digitaalsete tõendite lubatavus, olulisemad küberkriminalistika omapärad, kohtumenetlus seoses digitaalsete tõenditega.

Lõputöö eesmärgiks on välja selgitada, kas digitaalsete tõendite kogumise ja kasutamise osas on vajalik ja otstarbekas kehtestada eriregulatsioon seaduse tasandil. Eesmärgi saavutamiseks toob autor välja selle, kuidas käitutakse hetkel Eestis seoses digitaalsete tõenditega ja kuhu Eesti õiguskord liigub.

Lõputöös antakse ülevaade hetkel aktuaalsetest probleemidest ja aruteludest seoses digitaalsete tõenditega - seoses nende kogumisega, kuidas on sätestatud teiste riikide seadusandluses digitaalsete tõenditega seotu jne. Samuti toob autor välja selle, millised on riigiülesed kokkulepped digitaalsete tõenditega seoses. Lisaks eeltoodule on käesolevas töös vaatluse all see, millised probleemid on praktikas kriminaalmenetluses üles kerkinud seoses digitaalsete tõenditega.

Lõputööd koostama asudes püstitas autor hüpoteesi: digitaalsed tõendid on oma olemuselt erinevad füüsilistest tõenditest ja seetõttu tuleks nendega seoses põhiõiguste tagamise kontekstis kehtestada kriminaalmenetluses seaduse tasandil eri regulatsioon.

Esimeses peatükis toob käesoleva lõputöö autor välja selle, mis on digitaalsed tõendid, milline on nende erinevus klassikalistest tõenditest kriminaalmenetluses, käsitleb digitaalset tõendit, kui tõendi eriliiki, samuti toob välja rahvusvahelise koostöö võimalused.

[3] C.Kutz. The Oxford Handbook of Jurisprudence and philosophy of law, lk 565.

Teises peatükis toob töö autor välja pilveandmetöötluse omapärad. Samuti on töös välja toodud digitaalsete tõendite saamisel tekkida võivad probleemid seoses territoriaalsuspõhimõttega ja suveräänsusega ning sellega, millist õigust tuleks kohaldada digitaalsete tõenditega seoses.
Kolmandas peatükis toob autor välja digitaalsete tõenditega seotud hetkel kehtivad teiste riikide seadustes sätestatud regulatsioonid.
Neljandas peatükis analüüsib käesoleva töö autor seda, milline arutelu on hetkel tekkinud Eestis seoses digitaalsete tõenditega ja milliseid muudatusi plaanitakse meie kriminaalmenetluse seadustikku sisse viia.
Läbivalt toob autor töös välja ja analüüsib digitaalsete tõenditega seotud kohtupraktikat nii Eestis kui ka mujal Euroopas.
Magistritööd kõige enam iseloomustavad märksõnad on: kriminaalmenetlus, tõendamine, uurimistoimingud, kaugläbiotsimine, õigusloome.

1. DIGITAALSED TÕENDID - ERINEVUS KLASSIKALISTEST TÕENDITEST

1.1 Digitaalsete tõendite üldiseloomustus

Legaaldefinitsiooni sõnapaarile digitaalne tõend Eesti kehtivas Kriminaalmenetluse seadustikus ei ole. Ometi on see leidnud kasutust igapäevaselt tänapäeva kriminaalmenetluses. Arvestades seda, et üha enam leiab kasutust kõikjal digitaalne asjaajamine, info, mille inimesed on igapäevategevusest internetti maha jätavad kasvab iga päevaga, on muutunud tavapäraseks see, et sündmuskoht ei ole enam klassikaline füüsilise ruumi osa vaid võib olla ka virtuaalne.

Näiteks võivad küll küberkurjategijad jätta füüsilisse maailma tõendeid oma tegevuse kohta (DNA jäljed, märkmed paberkandjatel, klassikalised asitõendid, omapoolsed süüteod panevad nad toime füüsilises ruumis), kuid koht, kus kuritegu toime pannakse on küberruum. Selleks, et fikseerida nende poolt seal toimepandut, tuleb vaadelda arvuteid, andmekandjaid, uurida kahtlustatavate küberkäitumist, koguda kokku need jäljed, mille kurjategijad on jätnud küberruumi. Seejuures ei tule menetlejal tegutseda küberkurjategijate tabamiseks ainult Eesti õigusruumis vaid sageli on vajalik ka rahvusvaheline koostöö.

Raske on tänapäeva maailmas ette kujutada riiki, kus arvutialased kuriteod ei ole kriminaalkorras karistatavad. Samuti on raske ette kujutada riiki, kus digitaalsed tõendid ei ole lubatavad. Samas tuleb tõdeda, et erinevates riikides on kehtestatud erinevad korrad küberkuritegude ja digitaalsete tõendite menetlemiseks. Siseriiklikud õigused ei ole kloonid riikideülestest õigusaktidest. Siseriiklik õigus on kujundatud aja poolt ning kujunenud aja jooksul, arvestades valitsejate ja rahva seisukohti. Ning sellest tulenevalt on loogiline, et eri riigid on läinud digitaalsete tõenditega seoses erinevaid teid pidi.

Arvestades tänapäeva ühiskonna arengut, ei ole vaja eriti arutleda selle üle, kas kuritegevus on piiriülene nähtus. Juhani Riekkineni poolt on ajakirjas *Digital Evidence and Electronic Signature Law Review*[4] välja toodud, et küberkuritegevus on olnud alati piiriülene ja rahvusvaheline fenomen. Internet on oma ülesehituselt ja olemuselt selline, et see lubab arvutiandmetel liikuda üle piiri kergelt. Ei eksisteeri ainult ühe riigiga seotud küberkuritegevust. Võimalik digitaalne tõend on sageli laiali teatud geograafilise piirkonna peal

[4] J.Riekkinen. Digital Evidence and Electronic Signature Law Review. 13 (2016).

ja ta asetseb erinevate riikide territooriumitel, on hoiustatud ja kontrollitud erinevate ja sageli ka raskesti tuvastatavate osapoolte poolt nagu näiteks kurjategija ise, ohver, internetiteenuse pakkuja ja veel lisaks erinevad kolmandad osapooled. Selliste digitaalsete tõendite kindlaks tegemine, talletamine küberkuritegude puhul nõuab erinevat taktikat ja meetodeid ning ka vahendeid seaduse täitjate poolt, kui traditsiooniliste kuritegude puhul.

Nii nagu eelpool öeldud, siis sageli iseloomustab küberkäitumist ja digitaalseid tõendeid ning nende asukoha ja kogumisega seotut rahvusvaheline mõõde. Küberruum on oma olemuselt selline, et seda on väga raske piiritleda. Kriminaalmenetluse ruumiline kehtivus põrkub sageli probleemi otsa, kus menetlejal tuleb endalt küsida, kas need andmed, mida ta vajab asuvad just selle riigi territooriumil, mille seadust järgides ta parajasti kriminaalmenetlust toimetab või esineb kriminaalmenetluses rahvusvaheline element ning ta peaks kaaluma rahvusvahelise koostöö instrumentide kasutamist.

Lihtsaimaks näiteks siinkohal on küberrünnakud. Neid saab üheaegselt toime panna erinevatest riikidest, küberkurjategijad tegutsevad sageli globaalselt. Seega on väga oluline osa digitaalsete tõenditega seotud menetlustes rahvusvahelisel koostööl ja sellel, millised rahvusvahelise koostöö instrumendid on menetlejale antud.

On ilmselge, et vastava ettevalmistuseta menetlejal on väga raske, kui mitte võimatu uurida küberkuritegusid, tegeleda digitaalsete tõendite kogumise ja talletamisega.
Seoses muutunud maailmaga on üha rohkem on vaja eriteadmistega menetlejaid (uurimisasutuste teenistujaid, prokuröre, kohtunikke), kes esmalt suudaksid leida ja talletada kriminaalmenetluse reegleid järgides digitaalsed tõendid, mille kurjategijad oma tegevusel maha jätavad ning seejärel ka neid võistlevas menetluses või lühimenetluses kohtus esitada suudaks ning lõpetuseks on vaja kohtunike, kes nende kriminaalmenetluses kogutud (digitaalsete) tõendite pinnalt oleksid pädevad kohtuotsuseid tegema.

Samas on vaja ka eriteadmistega kaitsjaid, et tagada professionaalne õigusabi.

Riik on pidevalt teinud samme, et astuda vastu küberkurjategijatele, kuna ideaalis peaks olema politseinik alati sammu võrra eespool kurjategijast oma teadmiste ja oskuste poolest.

Nii nagu tavakurjategijad, muutuvad ka küberkurjategijad aja jooksul osavamaks. Nende oskused arenevad , tõuseb võimekus erinevate rünnete, kuritegude toimepanemiseks.

Näiteks saab siin välja tuua Eesti küberkurjategija Vladimir Tsaštšini, kes mõisteti möödunud aastal USA-s süüdi arvutisse sissetungi kavandamises ja elektroonilise pettuse kavandamises[5]: „Tšaštšini kuritegelik minevik sisaldab Eestis krediitkaardipettust, rahapesu ja võltsimist. Kuritegelikus skeemis kasutatud pahavara puudutas USA-s vähemalt 500 000 kasutajat, kelle hulgas olid ka USA kosmoseagentuur NASA ja teised valitsusasutused, teatas prokuratuur. Nakatatud arvuti kasutaja, kes klikkis lingile Apple'i iTunesi ametlikul veebilehel, suunati Apple'ile mittekuuluvale veebilehele, mis käivitas reklaamimaksed häkkeritele. Reklaamijad, kes maksid oma lehtede külastamise eest, ei teadnud, et osa klikke oli kaaperdatud. Skeemi teine komponent asendas reklaamid veebilehtedel häkkerite oma reklaamidega. Häkkerid teenisid sellega raha, samas kui veebilehtede seaduslikud operaatorid ja reklaamijad jäid tulust ilma. Tšaštšin ja tema grupp teenis vähemalt 14 miljonit dollarit. Süüdistus esitati kuuele Eesti ja ühele Venemaa kodanikule. Kõik on ennast süüdi tunnistanud peale ühe, keda pole kätte saadud."

Vladimir Tšaštšini kuritegelikku karjääri ja selle arengut aitab aga iseloomustada Tartu Maakohtu kohtuotsus nr 1-06-14599[6]. Nimelt süüdistati teda nimetatud kohtuasjas varalise kasu saamises andmete ebaseadusliku sisestamisega andmetöötlusprotsessi sekkumise teel. Tema ja tema kaasosalised kasutasid väga lihtsat ja levinud skeemi, kus paluti teatud isikutel vormistada arveldusarved, deebetkaardid, U-Neti liitumislepingud, paroolide kaardid, seejärel vormistas Tšaštšin virtuaalsed pangakaardid. Kogu andmed edastas Tšaštšin elektrooniliselt kaugsuhtlusprogrammi ICQ kaudu oma kuriteokaaslasele, seejärel pandi toime kaardipettused erinevate USA internetikauplustega seoses. Kohtuotsuse kohaselt sai Vladimir Tšaštšin koos Mihhaili-nimelise isikuga varalist kasu kokku 1 351 966 krooni ja 40 senti ning tekitas samas summas kahju USA internetikauplustele ja neid teenindavatele USA pankadele.

Tšaštšini näide on välja toodud selleks, et iseloomustada isiku kuritegelikku karjääri, tema oskuste ja teadmiste arengut aastate jooksul. Samuti näitavad need otsused seda, kui palju kriminaaltulu on võimalik küberkuritegevusega teenida.

[5] Eesti küberkurjategija Vladimir Tšaštin mõisteti USA-s seitsmeks aastaks vangi - http://www.delfi.ee/news/paevauudised/krimi/eesti-kuberkurjategija-vladimir-tsastsin-moisteti-usa-s-seitsmeks-aastaks-vangi?id=74355403

[6] Tartu MK Tartu kohtumaja otsus - 1-06-14599, 14.11.2006

Sellises olukorras nagu ühiskond hetkel on, peab riik jätkuvalt tõstma oma võimekust nii küberkuritegude menetlemisel kui ka tagama selle, et menetlusõiguslikud mehhanismid vastaksid kaasaja nõuetele ja võimaldaksid kiiret ja efektiivset rahvusvahelist koostööd.

Eesti küberjulgeoleku strateegiast 2014-2017[7] nähtub, et menetlemise võimekuse tõstmisel on Eestis tehtud pidevalt vastavaid samme. Nimelt koondati 2012. aastal Politsei- ja Piirivalveameti (edaspidi *PPA*) küberkuritegude uurimise võimekus ühte talitusse. Lisaks asutati 2013. aastal prefektuurides küberkuritegude ja digitaaltõendite teenistused, kuhu koondati prefektuuride erinevates üksustes paiknenud küberkuritegude menetluse ja digitaaltõendite haldamisega tegelevad ametnikud. Samuti tegeleb PPA küberkuritegevuse ohtude teadlikkuse tõstmisega, mille käigus on muu hulgas loodud veebikonstaabli[8] ametikohad.

Kaitsepolitseiamet on oma 2016.a. aastaraamatus[9] välja toonud, et küberjulgeoleku tagamine ei seisa lahus füüsilise maailma ohtudest ja kuritegudest ning nende uurimisest, mistõttu on julgeolekuasutusel vajalik omada suutlikkust ka kübervaldkonnas. Kaitsepolitsei ülesanne on tuvastada ja tõkestada riigi julgeoleku vastane kuritegelik tegevus küberruumis. Aastaraamatust nähtub, et nende uurimisvaldkonnaks on riigi olulise taristu vastaseid küberründed ning infohanked. Aastaraamatus on välja toodud, et üheks suureks ohuks on mõne ebasõbraliku riigi eriteenistuste ja küberkurjategijate vaheline sümbioos, mis on mõnel juhul omandanud kuritegeliku ühenduse iseloomu. Konkreetsemalt öeldes kujutab Venemaa eriteenistuste ja küberkurjategijate kohatine eristamatus endast suhteliselt unikaalset kriminaalsete ja riiklike struktuuride põimumist. Nii kasutavad Vene eriteenistused ja Vene küberkurjategijad tihti sama pahavara ning töötavad teineteise huvides. Tegelikult on eeltoodut ilmestav näide nii Eestis aastal 2007 ja Gruusias aastal 2008 toimunu, kus küberrünnakute tõttu halvati mitmeid olulisi infosüsteeme. Seejuures viisid rünnakute uurimisel jäljed Vene Föderatsioonini, kuid loomulikult eitas Venemaa sellist tegevust[10].

[7] Küberjulgeoleku strateegia 2014 – 2017 - https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
[8] Veebikonstaabli ülesanne on tõsta inimeste teadlikkust Interneti turvalisusest ning kaitsta lapsi ja noori Internetis.
[9] Kaitsepolitsei aastaraamat 2016, lk 20 - https://www.kapo.ee/et/content/aastaraamatu-v%c3%a4ljaandmise-traditsiooni-ajalugu-ja-eesm%c3%a4rk-0.html
[10] Küberrünnakud Eesti vastu - http://www.vm.ee/sites/default/files/content-editors/web-static/115/cyber_attacks.pdf

Veel üks näide, mis ilmestab küberkurjategijate ja eriteenistuste seotust on hiljutine Peter Yuryevich Levashovi kinnipidamine Hispaanias[11]. Tegemist on vene päritolu häkkeriga, kes oli ajakirjanduses avaldatud andmetel seotud vene eriteenistustega. Seejuures on meedias välja toodud, et Levashovi kinnipidamine on üks esimesi kordi, kus ameeriklased võtsid kasutusele USA föderaalse kriminaalmenetluse koodeksi § 41 lg 6, mis andis neile võimaluse uurida küberkuritegusid ükskõik kus kohas nakatatud arvutid füüsiliselt asuvad.[12]

Nimetatud reegli kohta kõrvalepõiget tehes, saab öelda, et tegemist on palju arutelu tekitanud muudatusega USA õiguskorras, mis annab kohtutele teatud jutudel võimaluse väljastada läbiotsimis ja vaatlusordereid juhtudel, kui arvuti füüsiline asukoht on teadmata[13].

Digitaalseid tõendeid võib leida kõikjalt – arvuti kõvakettalt, mobiiltelefonist, digitaalkaameratest, mälukaartidelt ja mujalt. Digitaalsed tõendid on sageli seostatavad arvutikuritegudega, kuid praktikas on kinnitust leidnud, et digitaalsed tõendid võivad olla ja on sageli abiks ka mitteküberkuritegude lahendamisel. Näiteks on väärtuslikuks tõendiallikaks salvestised, kuriteo toimepannud isikute poolt kasutatavate andmekandjatele talletatud info nii tekstisõnumite kui ka fotode näol.

Nii näiteks aitasid digitaalsed tõendid tabada Ameerika sarimõrvar Dennis Lynn Raderi[14] ja seda juba aastal 2004. Rader oli ajavahemikul 1974 – 1991 mõrvanud Kansases 10 inimest. Raderi viga oli see, et ta saatis politseile ja ajakirjanikele kirju, kus olid sees detailid tema tegudest. Kirju saatis ta kuni 90ndate aastateni, peale pausi jätkas ta kirjade saatmist 2004.a ja see viis tema arreteerimiseni 2005.a. Nimelt uuris Rader oma kirjades, kas andmeid, mis on flopi-ketastel saab jälitada või mitte. Politsei vastas Raderile ajalehe vahendusel, et ei, et sinna andmete salvestamine on turvaline. 2005.a. veebruaris saatis Rader Fox Tv-le flopi ketta.

[11] G.M.Graff. How FBI took down russias spam king – and his massive botnet. 11.04.2017 https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/

[12] Federal Rules of Criminal Procedure, TITLE VIII. SUPPLEMENTARY AND SPECIAL PROCEEDINGS Rule 41. Search and Seizure - *„(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:*
(A) the district where the media or information is located has been concealed through technological means; or
(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.“ Kättesaadav arvutivõrgus: http://uscode.house.gov/view.xhtml;jsessionid=95CAE72D0C7BE1D2CDBC29BE875A31E3?req=49&f=treesort&fq=true&num=1452&hl=true&edition=prelim&granuleId=USC-prelim-title18a-node35-title8-rule41

[13] Rule 41 Coalition Letter – kättesaadav veebis -https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf

[14] Dennis Radder - https://en.wikipedia.org/wiki/Dennis_Rader

Politsei leidis kettalt metadata, mida sai seostada Raderiga ja edasine viis juba Dennis Raderi vahistamise ja lõpuks ka süüdimõistmiseni.
Seega – võivad digitaalsed tõendid olla abiks ka näiteks isikuvastaste kuritegude uurimisel.

1.2 Digitaalne tõend kui tõendi eriliik

Tõendi mõiste KrMSi mõttes on välja toodud KrMS § 63 lg 1, mille kohaselt selleks on kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või videosalvestis, samuti muu dokument ning foto või film või muu teabetalletus.

Sama paragrahvi lõike 2 kohasel on seadusandja kirjutanud KrMSi sisse, et kriminaalmenetluse asjaolude tõendamiseks võib kasutada ka käesoleva paragrahvi lõikes 1 loetlemata tõendeid, välja arvatud juhul, kui on tegemist kuriteo või põhiõiguse rikkumise teel saadud tõendiga.

Vaadates eeltoodud loetelu, tekib küsimus, kuhu alla paigutada digitaalne tõend, kui tõendi eriliik ja samuti see, et millistel juhtudel võib digitaalne tõend olla saadud põhiõiguste rikkumisega.

Justiitsministeeriumi kriminaalmenetluse revisjoni töörühma liige J.Tehver on digitaalsete tõendite kasutamise võimaldamist käsitlevas kokkuvõttes[15] välja toonud järgmist: „Kehtiv KrMS, praktiliselt ei sisalda erisätteid digitaalsete tõendite kohta. See iseenesest ei välista digitaalsete tõendite kasutamist tõendamiseseme asjaolude tuvastamisel, kuivõrd KrMS § 63 lg 1 loetletud tõendite liigid on piisavalt üldised hõlmamaks ka vähemalt valdavat enamikku digitaalseid tõendid.“ Tehver on samas dokumendis lisaks veel välja toonud järgmist: „Teadaolevalt ei ole praktikas seni tekkinud olukorda, kus mõni digitaalne tõend oleks osutunud kriminaalmenetluses lubamatuks sel põhjusel, et see ei vasta KrMS § 63 lg 1 sätestatud tõendi tunnustele. Samal ajal tuleb nentida, et juba aastaid on praktikas segadus erinevate digitaalsete tõendite kvalifitseerimisel KrMS § 63 lg 1 sätestatud tõendi liikide alla (asitõend, muu dokument, muu teabetalletus). Lisaks sellele võib olla problemaatiline teatud spetsiifiliste ja

[15] J.Tehver, Digitaalsete tõendite kasutamise võimaldamine, mai 2016, lk 2- http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf

praktikas harva vahetult kasutatavate tõendi vormide lugemine tõendiks KrMS § 63 lg 1 järgi -- nimelt näivad antud normis loetletud relevantsed tõendi liigid ehk asitõend, muu dokument ja muu teabetalletus osutavat eelkõige mingisugusele andmekandjale *salvestatud* (ingl k *stored*) teabele, samal ajal kui tõendusteavet võib omada ka erinevate seadmete vahel *liikuv* (ingl k *transmitted*) digitaalne teave, mida kogutakse reaalajas".[16]

Seega – meie kriminaalmenetluse seadustik on piisavalt üldine (nii nagu heale seadusele omane), et see reguleeriks erinevaid asjaolusid, kuid samas võib selline üldisus tekitada segadust selles osas, millise tõendi liigiga konkreetsel juhul tegemist on. Töö hilisemas osas tuleb vaatluse alla KrMSi muudatuste väljatöötamiskavatsus, millele on käesoleva töö kirjutamise ajal arvamuse esitanud Riigikohus, Siseministeerium. Etteruttavalt saab öelda, et käesoleva töö kirjutamise ajal on huvipakkuv, et kohus ja ministeerium on eriarvamusel selles osas, milline peaks olema KrMSi tulevikuregulatsioon.

Käesoleva töö autor on siiski seisukohal, et see, millise tõendi liigi alla üks või teine digitaalne tõend liigitatakse ei ole kõige suurem probleem, mis selliste tõenditega seoses esineb. Palju suuremad väljakutsed on seotud rahvusvahelise koostööga ja piiriüleste kriminaalmenetlusega seoses.

Digitaalse tõendi definitsioone on valdkonna spetsialistid, eksperdid välja töötanud mitmeid. Tähelepanuväärne on see, et sageli kasutatakse sõnu elektrooniline tõend ja digitaalne tõend sünonüümina. Järgnevalt toob käesoleva töö autor välja mõned levinumad definitsioonid:

Stephen Mason on defineerinud digitaalset tõendit näiteks järgnevalt : „ Elektrooniline tõend: andmed, mis on loodud, muundatud, salvestatud või kommunikeeritud igasuguse seadme poolt, arvuti või arvutisüsteemi või edastatud üle kommunikatsioonisüsteemi, mis on asjasse puutuvad õigusemõistmise protsessis." [17]
Digitaalse tõendi definitsioonina on kasutusel ka järgnev : digitaalne tõend on informatsioon , mis on salvestatud või edastatud elektroonilises formaadis, kasutades selleks kahendsüsteemi arve ja mida saab kasutada kohtus[18].

[16] J.Tehver, Digitaalsete tõendite kasutamise võimaldamine, mai 2016, lk 2- http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf
[17] S.Mason.International electronic evidence, xxxv
[18] Digital evidence and forensics - https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx

Digitaalne tõend on info ja andmed, mis omavad tähtsust uurimises ja mis on salvestatud, vastu võetud või edastatud elektroonilise seadme abil[19].

Arvestades seda, et edaspidi käsitlusele tulevas KrMSi seaduseelnõus kasutatakse terminit digitaalne tõend, kasutab ka käesoleva töö autor töös selguse huvides terminit digitaalne tõend elektroonilise tõendi asemel.

Selleks, et mõista, mida tähendab digitaalne tõend, tuleb vaadelda, kust selliseid tõendeid üldse leida võib.

Digitaalseid tõendeid võib leida kõikjalt. Näiteks on digitaalsed tõendid ajatemplid, samuti on digitaalsed tõendid elektroonsete dokumentide metaandmed, mis näitavad selle loomise aega, kohta, looja võimalikku isikut.

Fotode puhul on vahel metaandmetes ka kirjas see, millise fotoaparaadiga on nimetatud foto tehtud. Nii on heal juhul võimalik näiteks tuginedes metaandmetele kokku viia foto selle tegemisel kasutatud kaameraga. Samas näiteks andmekandjalt fotot välja printides ei säili metaandmed reeglina paberdokumendil.

Ajatemplid võimaldavad näiteks tuvastada dokumendi loomise aega, kohta, selle loojat. Digitaalallkirjastatud dokumendi puhul on väga raske vaielda vastu sellele, et nimetatud dokument ei ole loodud digitaalallkirjastaja poolt. See on näiteks selle erinevus klassikalisest allkirjastatud dokumendist, mille puhul ei ole üldjuhul võimalik ilma ekspertiisita tuvastada kindlalt seda, millal nimetatud dokument on loodud ja allkirjastatud.

1.3 Digitaalsete tõendite erinevus klassikalistest tõenditest ja praeguse KrMSi regulatsiooni probleemid

Järgnevalt vaatleb autor seda, mille poolest ja kas erinevad digitaalsed tõendid klassikalistest tõenditest. Lisaks analüüsib käesoleva töö autor seda, kas digitaalse tõendi usaldusväärsuse tõendamisel on mingisuguseid erinevusi võrreldes klassikaliste tõenditega.

[19] Electronic CSI, A Guide for First Responders, 2nd edition, National Institute of Justice, April 2008, ix

Kuigi töö autor tõi eelmises alapeatükis välja, et sageli (näiteks digitaalselt allkirjastatud dokumentide puhul) on digitaalse tõendi puhul väga raske vastu vaielda sellele, et dokument on koostatud kindlal ajal ja kindla isiku poolt, siis on käesoleva töö autor sellest hoolimata seisukohal, et digitaalse tõendi usaldusväärsust on selle iseloomust tulenevalt mõnedel juhtudel kohtus raskem tõendada. Digitaalne tõend on sageli tehniline materjal ja omamata arusaama selle sisust, olemusest, tekkimise põhjustest ja viisidest on üsna keeruline kui isegi mitte võimatu selle usaldusväärsust kohtus tõendada.

Üheks kõige olulisemaks momendiks kriminaalmenetluses on see, kas see tõend, mida kohtus uuritakse, on usaldusväärne ja kas sellele saab tugineda kohtuotsuse tegemisel. Seejuures ei ole ühelgi tõendil ettemääratud jõudu. Riigikohus on lahendi 3-1-1-89-12[20] p 14 välja toonud , et tõendi usaldusväärsuse küsimus tõusetub kohtus üldjuhul alles tõendite hindamisel (KrMS § 61) - seega pärast seda, kui kohus on tõendi vastu võtnud ja selle avaldanud ning see tõend on edukalt läbinud asjakohasuse ning lubatavuse testi.

Kriminaalmenetluse seadustiku kommentaarides[21] on välja toodud, et tõendi usaldusväärseks tunnistamine tähendab kohtuniku veendumust, et see tõend on esiteks adekvaatselt kajastanud mingi uuritava kuriteo tunnust ja teiseks, et seda kajastust on võimalik adekvaatselt kriminaalmenetluses ka reprodutseerida.

Tõendite kogumisel tuleb seda teha järgides tingimusi, mis on KrMSis sätestatud.
KrMS § 64-s on välja toodud tõendite kogumise üldtingimused. KrMS § 64 lg 1 järgselt tõendeid kogutakse viisil, mis ei riiva kogumises osaleja au ja väärikust, ei ohusta tema elu või tervist ega tekita põhjendamatult varalist kahju. Keelatud on tõendeid koguda isikut piinates või tema kallal muul viisil vägivalda kasutades või isiku mäluvõimet mõjutavaid vahendeid ja inimväärikust alandavaid viise kasutades.

Kui tõendeid kogudes kasutatakse tehnikavahendeid, teatatakse sellest eelnevalt menetlustoimingus osalejatele ja neile selgitatakse tehnikavahendite kasutamise eesmärki.

[20] RKKm , 3-1-1-89-12/ p 14, 18.02.2013
[21] E. Kergandberg, P. Pikamäe. KrMS § 61/9. Kriminaalmenetluse seadustik. Komm vlj. Tallinn: Kirjastus Juura 2012, lk 209.

Jälitustoiminguga tõendite kogumine on reguleeritud KrMS-is eraldi peatükis. Käesolevas magistritöös jälitustoimingutega tõendite kogumisi eraldi ei käsitleta.

Ühelgi tõendil ei ole kriminaalmenetluses ette kindlaksmääratud jõudu, nagu eelnevast näha, siis tuleb ühe või teise tõendi lubatavus välja selle kontrolli käigus kohtus.

Selles osas saab väita, et, digitaalsed tõendid ei erine traditsioonilistest tõenditest – ka nende puhul on poolel vaja ära näidata tõendi usaldusväärsus ehk see, et kuidas neid on kogutud ja see, et selle saamisel ei ole rikutud kehtestatud reegleid ja et tõendit ei ole lubamatult muudetud.

Nagu eelpool välja toodud, siis KrMSis puuduvad sätted, mis reguleeriks digitaalsete tõendite kogumist ja esitamist.
Näiteks ei ole üheselt selge, millistel juhtudel seoses digitaalsetelt andmekandjatelt kogutud/kogutava teabega seoses tuleks määrata ekspertiis ja millal mitte.

Riigikohus on lahendis 3-1-1-55-14[22] välja toonud, et ekspertiis on nõutav olukorras, kui tõendamiseseme asjaolu tuvastamiseks on vaja vastata küsimusele, mille lahendamine on usaldusväärselt võimalik üksnes mitteõiguslike eriteadmiste alusel.

Reeglistiku puudumine digitaalsete tõenditega seoses jätab lahtiseks selle, millised on need asjaolud seoses digitaalsete tõenditega, kui ekspertiis ei ole vajalik ja millal ekspertiis on vajalik. On üldteada asjaolu, et oma iseloomult on digitaalsed tõendid vahel väga tehniline materjal, mille mõistmine vajab eriteadmisi.

Esmalt peab teatud digitaalsete tõendite kogumisel kaasama menetlusse juba varajasel staadiumil eriteadmistega menetleja, teiseks peavad ka prokuröril, kelle lauale selline digitaalne tõend jõuab olema eriteadmised. Kriminaalmenetlus ei lõppe üldjuhul prokuratuuris vaid riiklik süüdistaja peab kriminaalmenetluses kogutud tõenditega ka kohtu ette astuma. Ka kaitsjal peavad olema sellised teadmised, et sellisest vahel äärmiselt tehnilisest materjalist aru saada.
Praktikas on prokuröril vahel raske digitaalset tõendit arusaadaval moel kohtule esitada. Mitmetes kohtumenetlustes on toodud riikliku süüdistaja poolt sellisel juhul kohtusse ekspert või asjatundja, kes siis segaseks jäävad kohad arusaadaval viisil ära seletab.

[22] RKKm, 3-1-1-55-14/ p 172, 4.detsember 2014

Näiteks seadsid kohtumenetluse raames kaitsjad korduvalt kahtluse alla erinevate elektrooniliste tõendite usaldusväärsuse kohtuasjas nr 1-12-12478[23], viidates võimalikele puudustele tõendite kogumisel ja fikseerimisel. Samuti viitas kaitsja vajadusele kontrollida kõikide asitõendina äravõetud elektroonilistest andmekandjatest tehtud tõmmiste ning varukoopiate (mida kasutati vaatlusel) räsiväärtusi.

Olukorra lahendamiseks – s.o elektrooniliste tõendite kogumisel rakendatud metoodika ning kasutatud riist-ja tarkvara osas selgituste andmiseks kuulati kohtus asjatundjana üle X. Kuulates ära asjatundja, võttis kohus seisukoha, et arvestades X töökogemust ning haridust, samuti istungil antud selgitusi, hindas kohus kõigepealt seda, kas on tegemist pädeva isikuga, selgitamaks menetluslikke küsimusi, mis jäävad infotehnoloogia valdkonda. Seega hindas kohus tegelikult esmalt isiku pädevust – kas on üldse võimeline digitaalsete tõendite kohta selgitusi andma.

Jaatades seda, jätkati asjatundja selgituste kuulamisega sellest, kuidas tehakse elektroonilisest andmekandjast tõmmiseid (mis kujutavad endast kinniseid konteinereid ning milles olevate andmete muutmine ei ole võimalik), kuidas toimub nendest vaatluse läbiviimiseks vajalike koopiate tegemine ning kuidas neid toiminguid protokollitakse. Kohtuotsusest ilmneb, et sealjuures demonstreeris X nii riist- kui ka tarkvara, mida selle protsessi käigus kasutatakse. Samuti selgitas asjatundja kaitsjatele, mis on räsiväärtus ja kuidas toimub selle arvutamine ja kuidas on selle väärtuse kontrollimine võimalik.

Kohtu palvel kontrollis asjatundja X elukohast leitud mälupulgal olnud andmetest tehtud tõmmise ja tõmmise koopia räsiväärtusi ja võrdles ka neil olevaid andmeid. Kõigil saalisviibijail oli võimalik seda protsessi jälgida ning kontrolli tulemusel tuvastati, et tõmmisel ja koopial olevad andmed on vaatlusprotokollidesse korrektselt kantud.
Lisaks selgitas asjatundja erinevate tõenditena esitatud failide metaandmete võimalikke allikaid ning nende andmete usaldusväärsuse küsimusi (nt mil viisil saab andmekandja kasutaja ise neid andmeid muuta või neid manipuleerida).

[23] Viru Maakohus, Narva kohtumaja kohtuotsus nr 1-12-12478, 28.10.2015

Seega nähtub eeltoodust, et seoses digitaalsete tõenditega tuleb ette olukordi, kus kohtunikud tahavad digitaalsete tõendite osas suuremaid usaldusväärsuse garantiisid ja ei piisa vaid riikliku süüdistaja selgitustest.

Teise näitena esitas kaitsja kohtuasjas nr 1-15-509 [24] maakohtu otsuse peale apellatsiooni, milles tõi välja vajaduse määrata teadud asjaoludega seoses IT – ekspertiis. Apellant väljendas seisukohta, et kriminaalasja ei ole võimalik lahendada eriteadmistele tuginemata ning seetõttu tuleb määrata infotehnoloogiaekspertiis. Ringkonnakohus uuendas määrusega kohtuliku uurimise ja määras kohtuistungi. Ringkonnakohus leidis pärast taotluse kui kriminaalasja materjalidega tutvumist, et kriminaalasja objektiivse lahendamise seisukohalt on vajalik infotehnoloogiaekspertiisi määramine. Küsimus oli nimelt TOR-võrgu kasutamisega seoses süüdistatava poolt.

Kohtukolleegium leidis, et ekspertiisi määramiseks on vajalik kohtumenetluse poolte seisukohtade ära kuulamine eksperdile esitatavate küsimuste osas, mistõttu tuleb korraldada kohtuistung. Määratud eksperdiarvamus, kohtuistungil antud ütlused jätsid üles kõrvaldamata kahtlused süüdistatava osas ning seetõttu tuli isik õigeks mõista.
Nimetatud kohtuasja otsusest nähtub, et teatud digitaalsete tõendite puhul ei ole käesoleval ajal veel võimalik usaldusväärselt siduda tegu süüdistatavaga.[25]

Eeltoodud kaks näidet ilmestavad seda, kui erinevad on digitaalsed tõendid klassikalistest tõenditest. Samas kajastavad nad võimalusi, kuidas siiski tõendada digitaalse tõendi usaldusväärsust kohtus.

Lisaks eeltoodule ei ole probleemne vaid digitaalsete tõendite usaldusväärseks tunnistamine. Probleemid algavad sageli juba varem – näiteks olukorras, kus andmed, mida on tarvis menetlejal saada asuvad elektroonses/digitaalses vormis kellegi valduses olevas sidevahendis, arvutis. Samuti võib menetleja läbiotsimisel silmitsi seista probleemiga, kus andmed on krüpteeritud ja nendele ligipääsemiseks on vaja vastavat teavet, mida aga harilikult kahtlustatav jagama ei ole nõus.

[24] Tallinna Ringkonnakohtu kriminaalkolleegium, 1-15-509, 15.aprill 2016
[25] TORis tuleb käesolevas töös hiljem juttu.

Sellisel juhul tuleb pöörduda sellise menetlustoimingu nagu läbiotsimine (KrMS § 91) juurde. Kõrvalepõikena toob käesoleva töö autor välja, et ebaseadusliku läbiotsimise juhul on võimalik menetlejat kriminaalkorras vastutusele võtta. Nimelt sätestab KarS § 314 lg 1, et ebaseadusliku läbiotsimise või eluruumist väljatõstmise eest karistatakse rahalise karistusega. Seega peab läbiotsimist toimetades järgima seadust. Karistusseadustiku kommentaarides peetakse läbiotsimist ebaseaduslikuks, kui selleks puudub õiguslik alus. [26]

Juhul, kui isik vabatahtlikult annab välja või temalt võetakse ära näiteks kahtlustatava kinnipidamisel mingi sidevahend/andmekandja, siis saab teabe kätte praktika kohaselt ka vaatlusega. Läbiotsitav koht ei ole enamasti avalik koht, selleks on harilikult kahtlustatava elukoht, sõiduk, ruum, mida kahtlustatav kasutas jne. Vaatlus on KrMS § 83 lg 1 kohaselt menetlustoiming, mille eesmärk on koguda kriminaalasja lahendamiseks vajalikke andmeid, avastada kuriteojäljed ja võtta asitõenditena kasutatavad objektid ära. Vaatlus ja läbiotsimine on seega oma sisult erinevad KrMSis sätestatud menetlustoimingud. Ühe eesmärgiks on teostada otsinguid, teise eesmärgiks on koguda vaatlemise teel kokku kriminaalasja lahendamiseks vajalikud andmed.

Kui isik annab vabatahtlikult välja sidevahendi/andmekandja ja annab ka andmed ja loa seadmesse sisenemiseks, ei ole kehtiva praktika kohaselt vaja küsida kohtult luba ära võetud seadme läbiotsimiseks vaid võib arvestades kehtivat praktikat piirduda vaatlusega. Samas juhul, kui ilmneb, et isiku sidevahendi puhul on andmed, millele menetleja ligi pääseb on salvestatud pilveteenusesse, tõusetuvad pilveproblemaatika küsimused, millel käesoleva töö autor peatub hiljem. Etteruttavalt võib öelda, et sellisel juhul tekib küsimus, kas menetlejal on õigus ilma loata vaadelda teise riigi territooriumil asuvaid andmeid. Ja tekib ka teine küsimus – kes peaks sellisele tegevusele loa andma.

Vaatluse puhul probleemiks see, et peaaegu alati on sidevahendites/andmekandjatel kriminaalasjas tähtsust mitteomavad andmed, mille vaatlus enam proportsionaalsuse põhimõttega kooskõlas pole. Sidevahendis võivad olla kolmandate isikute kontod, fotod, muud kolmandatele isikutele kuuluvad andmed, mis ei oma tähtsust kriminaalasjas. Selle juures on probleemiks see, et tegemist on vaatluse käigus andmekandja läbiotsimisega, sest et praktikas tähendab andmekandja/sidevahendi vaatlus enamasti sisuliselt selles otsingute teostamist. Otsingute teostamine on aga oma olemuselt juba läbiotsimine.

[26] J.Sootak. jt. (koost). Karistusseadustik. Kommenteeritud väljaanne. Tallinn: Juura 2008, pt 18/3,4.

Kriminaalmenetluse seadustiku kommentaarides on välja toodud, et oluliseks erinevuseks läbiotsimise ja vaatluse puhul on see, et läbiotsimisel võib menetleja otsitaval alal teostada otsinguid ning leitud objektid ka ära võtta, ent vaatlusega saab fikseerida üksnes nende objektide üleandmist, mida isik annab menetlejale vabatahtlikult[27]. Seega võib arvestades kehtivat seadusandlust olla vahel välistatud vaatluse tegemine, kuna plaanitav menetlustoiming ei ole sisuliselt vaatlus ning selle asemel tuleks teha hoopis läbiotsimine. Samas puudub Eestis kehtivas KrMSis regulatsioon sidevahendite/andmekandjate läbiotsimiseks.

Läbiotsimiseks endaks tuleb saada kohtult üldjuhul luba. Saades läbiotsimisel kätte sidevahendi/andmekandja/arvuti, tuleb teostada nii nagu eelnevalt välja toodud üldjuhul kehtiva praktika kohaselt selle vaatlus või siis saata seade ekspertiisi. Seejuures on tavapärane see, et vaatlusel kasutatakse koopiat (*forensic copy*), kuna on üldteada asjaolu, et digitaalsed andmed on oma iseloomult kergelt hävinevad/hävitatavad, manipuleeritavad.

Käesoleva töö autori arvates on küsitav, kas arvuti vaatluse praktika, mis tegelikult sisuliselt kujutab endast arvuti läbiotsimist on õnnestunud õiguslik lahendus või tuleks kehtivat seadust ja seejärel ka kehtivat praktikat selles osas muuta. Sidevahendite/andmekandjate läbiotsimine ja vaatlus on tegelikult kaks erinevat toimingut. Kohtulikule kontrollile on allutatud vaid esimene neist, vaatluseks ei ole vaja menetlejal eraldi luba küsida. Andmekandja/sidevahendi vaatlus on oma olemuselt samuti otsing ja otsingu käigus leitud info talletamine vaatlusprotokolli. Läbiotsimise ja vaatluse vahele jääb tegelikult veel sidevahendist/andmekandjast koopia tegemine, mille protsess ei ole samuti käesoleval ajal Eestis seaduse tasandil reguleeritud.

Kriminaalmenetluse seadustiku kommentaarides[28] on välja toodud, et kehtiva KrMSi sõnastus ei võimalda käsitleda arvutit (arvutikeskkonda) läbiotsimise objektina. E.Kergandbergi hinnangul asendab sellistel juhtudel läbiotsimist arvuti vaatlus või jälitustoiming[29].

[27] Kergandberg/Pikamäe § 83/ 2.4, lk 252
[28] Kergandberg/Pikamäe § 91/4, lk 269
[29] Jälitustoiminguid reguleerib KrMSis eraldi peatükk. KrMS § 126[1] lg 1 kohaselt on jälitustoiming isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest[29]. Riigikohus on lahendis RKKKo 3-1-1-5-09 välja toonud, et jälitustoiminguga kogutakse ja töödeldakse salaja või varjatult isikuandmeid, mille käigus sekkutakse isikute põhiseaduslikult kaitstavate õiguste sfääri.

Nimetatud KrMSi sätet on hiljuti muudetud, kuid ka kehtiv KrMS ei nimeta läbiotsimise objektina näiteks arvutit. Samas on KrMSi muutmise seletuskirjas[30] välja toodud, et menetlejal tuleb läbiotsimismäärusesse sisse kirjutada, millisel kujul on alust arvata, et ostitu esineb: „Keerukam võib olla dokumentide otsinguga, mis võivad esineda elektroonilisel kujul ka väga väikestel andmekandjatel (mälupulk, mälukaart). Sellisel juhul tuleks juba läbiotsimismääruses märkida, millisel kujul on alust arvata, et need esinevad; kui läbiotsimismääruses ei ole ainsatki viidet sellele, et otsitakse dokumente ka elektroonilisel kujul, ei saa pidada enesestmõistetavaks, et nende leidmiseks läbiviidavad mõistlikud otsingud ulatuvad ka lauaarvuti kõvakettani."

Praktikas tuuaksegi seejuures välja, et on alust arvata, et isiku poolt/isiku valduses olevates sidevahendites/arvutis/andmekandjatel on elektroonilises/digitaalses vormis kuriteoga puutumuses olev teave (seejuures võimalusel lisatakse täpsustus selle kohta, milline teave), mille kättesaamiseks on vajalik teha läbiotsimine.

Varasem KrMS sätestas, et läbiotsimine võib toimuda prokuratuuri loal, edasilükkamatul juhul ka uurimisasutuse määruse alusel, mille siis hiljem prokurör lubatavaks tunnistas. Vaid teatud juhtudel oli vajalik kohtu luba. Alates 01.09.2016 on läbiotsimine allutatud üldreeglina kohtulikule eelkontrollile. Täpsemalt tuleb eeluurimiskohtunikult saada selleks luba. Käesoleva töö autori seisukoht on, et selline kohtulikule kontrollile allutatud läbiotsimine tagab paremini isikute põhiõiguseid. Samas tuleb nentida, et sellega on suurenenud eeluurimiskohtunike töökoormus.

KrMS § 91 sätestab, et läbiotsimise eesmärk on leida hoonest, ruumist, sõidukist või piirdega alalt asitõendina kasutatav või konfiskeeritav objekt, kriminaalasja lahendamiseks vajalik dokument, asi või isik või kriminaalmenetluses arestitav vara või laip või tabada tagaotsitav. Läbiotsimist võib toimetada, kui esineb põhjendatud kahtlus, et otsitav asub läbiotsimiskohas. Käesoleval ajal on läbiotsimine allutatud üldjuhul kohtulikule eelkontrollile, mõningatel juhtudel on siiski võimalik ka kohtulik järelkontroll, kus kohus tunnistab läbiotsimise lubatavaks või mitte.

[30] Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seadus 770 SE, seletuskiri - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d5492f26-424d-42ad-83e4-cce202a5524d

Peale läbiotsimist tuleb menetlejal ära võetud arvutisüsteemides ja andmekandjatel leiduvad vajalikud andmed üldjuhul kopeerida ja teostada nende vaatlus. Saadud andmekandja/arvuti/sidevahendi vaatlusel võib menetleja põrkuda aga probleemiga, kus ta seisab silmitsi teadmisega, et andmed, mida ta vajab on küll kättesaadavad läbi seadme, kuid nad asuvad näiteks pilves, mida hallatakse teises riigis, läbiotsimisluba aga kehtib ainult Eesti territooriumil.

A.M.Osula on artiklis „*Remote search and seizure in domestic criminal procedure: Estonian case study*[31] välja toonud järgmist: "Rahvusvahelise õiguse kohaselt ei saa riik koguda tõendeid teise riigi territooriumilt, kohaldades iseenda kodumaist õigust välja arvatud juhul, kui see toimub lepingu sätteid järgides või selleks on antud nõusolek."

Pilveproblemaatika on üks olulisemaid probleeme, mille üle arutletakse käesoleval ajal maailmas. Ühest lahendust ei ole aga leitud, hoolimata aastatepikkustest aruteludest. Praktikas on tekkinud vajadus nimetatud valdkonna paremaks reguleerimiseks, kuid reaalselt ei ole riigid aktsepteerita lahenduseni jõudnud.

Probleemne seoses pilves asuvate andmetega on ka asjaolu, et KrMS § 3 sätestab, et kriminaalmenetlusõigus kehtib Eesti Vabariigi territooriumil. Samas nimetatud sätte teine lause ütleb, et kriminaalmenetlusõigus kehtib ka väljaspool Eesti Vabariigi territooriumi, kui see tuleneb välislepingust.

Ühest vastust sellele, kas Eesti eeluurimiskohtunikul on võimalik anda Eesti kohtul luba ka välisriigis olevas pilves asuvate andmete saamiseks läbiotsimise käigus ei ole. Puudub sellekohane praktika, Riigikohus ei ole sellekohast küsimust vaaginud. Arvutikuritegevusvastase konventsiooni[32] artikkel 32 b-s, mis reguleerib piiriülest ligipääsu andmetele on sätestatud, et konventsiooniosaline võib teise konventsiooniosalise loata saada juurdepääsu või oma territooriumil paikneva arvutisüsteemi kaudu teises konventsiooniosalises riigis asuvaid salvestatud arvutiandmeid, kui ta saab selleks seadusliku ja vabatahtliku nõusoleku isikult, kellel on seaduslik volitus avalikustada andmeid nimetatud arvutisüsteemi

[31] Osula A-M, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (2016) 24 (4) International Journal of Law and Information, lk 346.

[32] Arvutikuritegevusvastane konventsioon - RT II 2003, 9, 32

kaudu. Põhiseaduse[33] § 14 sätestab, et õiguste ja vabaduste tagamine on seadusandliku, täidesaatva ja kohtuvõimu ning kohalike omavalitsuste kohustus. Põhiseaduse § 26 kohaselt on **i**gaühel õigus perekonna- ja eraelu puutumatusele. Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. Põhiseaduse § 43 kohaselt on **i**gaühel õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Erandeid võib kohtu loal teha kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras. Kui vaadata neid kolme Põhiseaduse sätet ja Arvutikuritegevusvastase konventsiooni artikkel 32 b-d ja ka artiklit 19 nimetatud konventsioonist koos, siis peaks teoorias olemas olema esiteks selline selgelt sõnastatud seadus, mis reguleeriks käitumisjuhiseid seesuguses olukorras kus on vaja teostada pilves olevate andmete läbiotsimist ja teiseks peaks olema sätestatud selgesõnaliselt, et asutus, kes peaks andma nimetatud andmete läbiotsimiseks loa võiks olla kohus. Siinkohal tuleb tõdeda, et rahvusvahelises õiguses puudub selline säte, mis lubaks ühemõtteliselt Eesti täitevvõimul toimetada kohtu loal välisriigis asuvates serverites kriminaalmenetluse raames. Ligipääsuluba on avalikele andmetele (Arvutikuritegevusevastase konventsiooni artikkel 32 a kohaselt) ja territooriumil paikneva arvutisüsteemi kaudu teises konventsiooniosalises riigis asuvatele salvestatud arvutiandmetele, kui riik saab selleks seadusliku ja vabatahtliku nõusoleku isikult, kellel on seaduslik volitus avalikustada andmeid nimetatud arvutisüsteemi kaudu (Arvutikuritegevusevastase konventsiooni artikkel 32 b).

Samas võib konstrueerida järgneva arutelu. Sisuliseks põhjenduseks võib olla see, et menetleja, kes füüsiliselt sellist läbiotsimist toimetab asub üldjuhul Eestis. Samuti on isik, kelle suhtes läbiotsimist toimetatakse Eestis. Loa annaks Eestis asuv eeluurimiskohtunik. Samuti peab olema õigus, mis isikule kohaldub ettenähtav. Põhiseaduse kommenteeritud väljaandes[34] on selle § 13 kommentaari punktis 5.2 välja toodud, et õigusselguse põhimõte tähendab, et põhiõigust riivav seadus peab olema piisavalt määratud. Käesoleval juhul seda meie KrMS pilves asuvate andmete läbiotsimise ja vaatluse osas ei ole, kuid sellest hoolimata saab väita, et isik, kes on füüsiliselt Eestis ja tegutseb Eesti õiguskorras saab harilikult kõige ettenähtavamaks pidada meie õiguskorras kehtivaid seaduseid. Samas võib see kaasa tuua probleeme seoses teise

[33] Põhiseadus - RT I, 15.05.2015, 2

[34] Toimetuskolleegium: prof. Ülle Madise, mag. iur. Berit Aaviksoo, LL.M. Hent Kalmo, prof. Lauri Mälksoo, prof. Raul Narits, PhD (õigus) Peep Pruks, Priit Vinkel. Põhiseaduse kommenteeritud väljaanne, § 13/p 5.2. Juura, 2012.

riigi suveräänsuse riivega ja territoriaalsusprintsiibi riivega, millel peatutakse käesolevas töös hiljem.

Käesoleva töö autori hinnangul tuleb aga sellise teoreetilise põhjendusega ettevaatlik olla. Kui sellist käsitlust aktsepteeritaks kogu maailmas, siis tõusetuvad sellisel juhul julgeolekuprobleemid. Seda võidakse hakata ära kasutama ebasõbralike riikide eriteenistuste poolt. Riikide julgeoleku seisukohast oleks lubamatu, kui mõne sellise riigi täitevvõim, kes võib olla põimunud oma tegevuses eriteenistusega, hakkab toimetama kriminaalmenetluse raames läbiotsimist ja seejärel ka näiteks andmete arestimist Eestis asuvas serveris.

Kohtuniku loa alusel pääseks ta ligi teabele, mis on elektroonilises vormis salvestatud väljaspool Eestit, vahel isegi täpselt tuvastamata riigis. Sellises olukorras võib kriminaalmenetluses leida ennast kahesuguses situatsioonis – teave asub kas Arvutikuritegevusvastase konventsiooniga[35] liitunud riigis või sellega mitte liitunud välisriigis.

Arvutikuritegevusvastase konventsiooni[36] artikkel 32, mis käsitleb piiriülest juurdepääsu avalikele arvutiandmetele ja muudele arvutiandmetele, sätestab, et konventsiooniosaline võib teise konventsiooniosalise loata saada juurdepääsu kahel juhul :
a) avalikele arvutiandmetele nende asukohast sõltumata;
b) või saada oma territooriumil paikneva arvutisüsteemi kaudu teises konventsiooniosalises riigis asuvaid salvestatud arvutiandmeid, kui ta saab selleks seadusliku ja vabatahtliku nõusoleku isikult, kellel on seaduslik volitus avalikustada andmeid nimetatud arvutisüsteemi kaudu.

Seega ei ole probleemne avalikele andmetele ligipääsemine, kui need asuvad teises riigis. Keeruline on aga määratleda, kuidas peaks läbiotsimist toimetama juhul, kui ilmneb, et mitteavalikud andmed, mida kriminaalmenetluses vajatakse on salvestatud teises konventsiooniosalises riigis.

Juhul, kui kahtlustatav annab andmete kättesaamiseks seadusliku ja vabatahtliku nõusoleku, ei ole taas probleemi – kõik vajamineva saab kätte. Kui ta aga seda ei tee, tekib küsimus, kuidas menetleja edasi peaks käituma.

[35] Nimetatud konventsiooni on käsitletud põhjalikult järgnevates peatükkides.
[36] Arvutikuritegevusvastane konventsioon - RT II 2003, 9, 32

Nimetatud küsimuses ei ole ühest arusaama käesoleval ajal Euroopas ega ka maailmas laiemalt. Riigid on läinud praktika kohaldamisel eri teed.

Eeltoodud küsimusega on tegelenud aktiivselt küberkuritegevusevastase konventsiooni rakendamise ja kaasajastamise eest vastutav komisjon *T-CY (Cybercrime Convention Committee)*. Nimelt on nende poolt arutletud, seda, kas ja mil viisil on vajalik art 32(b) täiendamine või täiendav selgitamine, arvestades eeskätt pilvetehnoloogia arengut ja levikut, mis muudab teabe füüsilise paiknemisega seotud jurisdiktsiooni praktiliselt määratlematuks. Oma 2014.a. raportis[37] tõid nad välja, et teatud juhtudel artikkel 32 b töötab. Ka 2016.a. raportis on sellel probleemil peatutud.

Raportis on toodud näide, et juhul, kui narkoäris kahtlustatav peetakse seaduslikul alusel kinni ning samal ajal on tema e-postkast – mis võib sisaldada tõendeid kuriteo kohta – on avatud tema tahvelarvutis, nutitelefonis või muus seadmes. Seega on isiku kinnipidamistaktikal oluline roll. Teisisõnu juhul, kui soovitakse isiku poolt kasutatavate sidevahenditele ligi pääseda, tuleb taktika valida selline, mis võimaldab isikut tabada avatud sidevahendiga. Samas tuleks sellisel juhul siiski saada nõusolek, et isik lubab anda ligipääsu enda andmetele.

Seega juhul, kui kahtlustatav on vabatahtlikult nõus andma politseile juurdepääsu oma kontole ning politsei on veendunud, et e-post asub teises liikmesriigis, siis on alus andmetele juurdepääsuks artikli 32b kohaselt. Selliseid juhtumeid praktikas ilmselt väga palju ette ei tule.

1.4 Kurjategijate anonümiseerumisega seotud probleemid

Kurjategijate tehnilised oskused seavad menetlejatele pidevalt väljakutseid. Praktikas kasutavad nad sageli enda jälgede peitmiseks erinevaid võimalusi. Küberkurjategijad tegutsevad piiriüleselt, peitudes variisikute taha, kasutavad anonüümsust võimaldavaid veebikeskkondi.

Tavakasutajad aga ei pane enamasti väga suurt rõhku sellele, et jääda veebis anonüümseks. Ja ka turvalise netikasutuse puhul ei olda nii nõudlikud kui seda on näiteks küberkurjategijad.

[37] T-CY, Criminal justice access to data in the cloud: challenges. Discussion paper prepared by the T-CY Cloud Evidence Group , 26 May 2015

Lisaks tavapäraselt kasutatavale internetile on olemas nö *Darknet*[38]. *Darknet*-i kasutavad oma tegevuseks näiteks kriminaalsed jõugud. *Darknet*-i eeliseks kriminaalide silmis on see, et politseiuurijad ei suuda kuigi sügavale süvaveebi saladustesse tungida. Otsingumootorid blokeeritakse ning infot kaitstakse kiivalt. [39]

Arengud internetiturul, sealhulgas *darknet*, anonüümust võimaldav tarkvara ja krüptoraha, loovad uusi võrgupõhiseid võimalusi uimastite levitamiseks. Seda on välja toodud näiteks Euroopa Narkootikumide ja Narkomaania Seirekeskuse ning Europoli 2016.a aprillis avaldatud Euroopa Liidu uimastiturgu käsitlevas aruandes.[40]

Nimetatud aruandes on välja toodud, et internetist narkootikumide hankimine *darknet*-i vahendusel on viimastel aastatel suurenenud. Seda peetakse ohtlikuks, kuna on leitud võimalus varjuda nii õiguskaitseorganite eest kui ka hoiduda vahetult kokku puutumast kurjategijate endaga. Sisenetakse sinna *darknet*-i kaudu, makstakse krüptorahaga ja aine tuuakse tellijani postiteenuse vahendusel.

Osad küberkurjategijad kasutavad Tori[41], mis on tarkvara, mis pakub võimalust anonüümseks veebi kasutamiseks. Tori poolt pakutav teenus pole tsentraliseeritud ja Tor võrgu toimimisele saab igaüks kaasa aidata määrates oma arvuti päringute vahendajaks (*relay*). Tor-i kasutades suunatakse kasutaja päring läbi mitme suvaliselt valitud vahendaja (vahendajateks on teised Tor-i kasutajate arvutid), kusjuures iga kahe punkti vaheline ühendus on eraldi võtmega krüpteeritud. Nii teab iga vahendaja selles ahelas ainult endale eelnevat ja järgnevat lüli. Kuna Tor suunab liikluse läbi suvaliste kasutajate arvutite, siis sõltub ühenduse kiirus sellest, kuidas liiklust kasutajate vahel edasi suunatakse. Tor kasutab nn. Onion ruutimist, mis tähendab seda, et saadetav sõnum on mitmekordselt krüpteeritud ja ainult viimane ruuter saab sõnumi sisu lugeda.

Kui aastaid sai Tori kasutada vaid arvutis, siis nüüdseks on turul olemas ka Orbot[42], mis on Tori sarnane tarkvara, mis on mõeldud kasutamiseks Android operatsioonisüsteemidel.

---

[38] Darknet on internetivõrk, ei ole avalikult kättesaadav, sinna pääseb ligi autoriseerides ennast, kasutades spetsiaalset tarkvara ja arvutisätteid - https://www.techopedia.com/definition/2395/darknet

[39] P.Hõbemägi. Interneti pimedam pool – Eesti Ekspress 05.12.2009 http://ekspress.delfi.ee/kuum/interneti-pimedam-pool?id=27693601

[40] Euroopa Liidu infokeskus. EL-i aruanne: uimastiturg ja terrorism on omavahel tugevalt seotud – 05.05.2016 http://elik.nlib.ee/el-i-aruanne-uimastiturg-ja-terrorism-on-omavahel-tugevalt-seotud/

[41] Tor Project - https://www.torproject.org/

[42] Guardian Project. What is Orbot - https://guardianproject.info/apps/orbot/

Uued võimalused tähendavad menetlejate jaoks aga uusi väljakutseid. Sellistes kriminaalmenetlustes, kus isikud tellivad *darknet*-ist relvaosi ja narkootilisi aineid, ei jõuta küll tavaliselt nende müüjateni, samas aga ollakse võitluses ostjatega küllaltki edukad.
Nimelt on viimastel aastatel süüdi mõistetud mitmeid isikuid, kes on enesele *darknet*-i vahendusel narkootilisi aineid tellinud. Näiteks mõisteti kohtuasjas 1-14-3221[43] kolm noormeest süüdi selles, et nad olid endale *darknet*-ist tellinud erinevaid narkootilisi aineid. Tasusid nad seejuures nende eest *bitcoin*-idega. Pakend marihuaanaga peeti aga riiki sisenemisel tollikontrolli käigus kinni, mistõttu jäi kuritegu lõpule viimata.

1.5 Rahvusvahelise koostöö võimalused digitaalsete tõenditega seoses

Rahvusvahelise koostöö instrumendid, mis võimaldavad digitaalsete tõendite seadustatud viisil saamist on samad, kui füüsiliste tõenditega seoses.

Raul Narits on juba 1999.a. ajakirjas Juridica ilmunud artiklis „Ühest tänapäevasest põhiseaduse mõttest arusaamise viisist“[44] välja toonud järgmise mõtte: „ Kõrvuti põhiseadusega mängivad riigi avanemisel väljapoole suurt rolli rahvusvahelised lepingud. Minemata konkreetseks, võib väita, et konstitutsiooniline riik peab rahvusvahelisi lepinguid kasutama minimaalselt niivõrd, kuivõrd nendega on kaitstud inimõigused“.

Ehk siis kui rahvusvaheliste lepingutega antakse riigile võimalused võidelda kuritegevusega parimal moel, siis see tegelikult tähendab ka teisipidi seda, et oma lepingupartneritega lepitakse ka kriminaalmenetluse valdkonnas kokku sellised efektiivsed koostöömehhanismid, mis võimaldavad vajaminevaid andmeid kiiresti kätte saada.

Järgnevalt vaatleb töö autor seda, millised rahvusvahelised instrumendid on olemas, et käesoleval ajal saaks toimida efektiivne koostöö tõendite kogumisel rahvusvahelist elementi omavates kriminaalmenetlustes.

Kriminaalasjades vastastikuse abistamise Euroopa konventsiooni[45] artikli 1 kohaselt kohustuvad lepingupooled võimaldama üksteisele ulatuslikku vastastikust abi

[43] Harju Maakohtu otsus nr 1-14-3221
[44] R.Narits. Ühest tänapäevasest põhiseaduse mõttest arusaamise viisist. Juridica X 1999. lk 466-472
[45] Kriminaalasjades vastastikuse abistamise Euroopa konventsioon - RT II 1997, 7, 36

kriminaalasjades, milles karistamine kuulub taotleva poole õigusasutuste pädevusse abi taotlemise ajal.

Kriminaalmenetluse ülevõtmise Euroopa konventsiooni[46] reguleerib üldistatult kriminaalmenetluste ülevõtmise ja kriminaalmenetluste paljususega seotut.

Lisaks sellele on Eesti Vabariigil olemas riikidevahelised õiguskoostöö lepingud. Neid on oma olemuselt kahte liiki. Ühed on riiklikud õiguskoostöö lepingud kriminaalasjades – Eesti ja Soome ning Eesti ja USA vahel.
Teised on aga õigusabilepingud, mis reguleerivad rahvusvahelist suhtlemist nii kriminaal- kui ka tsiviilõiguse valdkonnas. Sellised on Eesti – Venemaa[47], Eesti – Läti ja Leedu[48] vahel sõlmitud, Eesti ja Ukraina[49] ning Eesti ja Poola[50] vahel sõlmitud õigusabilepingud.

Üheks olulisimaks rahvusvaheliseks konventsiooniks, mis reguleerib riikidevahelisi suhteid digitaalsete või siis elektrooniliste tõenditega seoses on eelpool välja toodud Arvutikuritegevusvastane konventsioon[51]. Nimetatud konventsiooni puhul on tähelepanu vääriv fakt see, et Eesti oli 2004. aastal jõustunud konventsiooni ja selle lisaprotokolli väljatöötamist algatanud riikide hulgas.

Arvutikuritegevusvastane konventsioon (*Convention on Cybercrime* – RT II 2003, 9, 32), mis on koostatud 23. novembril 2001. aastal Budapestis, jõustus Eesti Vabariigi suhtes 1. juulil 2004. aastal.

Nimetatud konventsioon on oma olemuselt esimene niivõrd laiaulatuslik rahvusvaheline kokkulepe valdkonnas, mis puudutab kuritegusid, mis on Internetis toime pandud ja teistes arvutivõrkudes. Konventsiooni esimeses osas on keskendutud materiaalõiguslikele probleemidele ja sellele, millised teod peaksid olema materiaalõiguses määratletud.

[46] Kriminaalmenetluse ülevõtmise Euroopa konventsioon- RT II 1997, 8, 37
[47] Eesti Vabariigi ja Vene Föderatsiooni leping õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades - RT II 1993, 16, 27
[48] Eesti Vabariigi, Leedu Vabariigi ja Läti Vabariigi õigusabi ja õigussuhete leping - RT II 1993, 6, 5
[49] Eesti Vabariigi ja Ukraina leping õigusabi ja õigussuhete kohta tsiviil- ning kriminaalasjades - RT II 1995, 13, 63
[50] Eesti Vabariigi ja Poola Vabariigi vaheline leping õigusabi osutamise ja õigussuhete kohta tsiviil-, töö- ning kriminaalasjades - RT II 1999, 4, 22
[51] Convention on Cybercrime – RT II 2003, 9, 32

Konventsiooni teises osas on sätestatud reeglid menetlusõigusele, et tagada selliste kuritegude efektiivne ja tulemuslik menetlus. Käesolevas töös käsitletakse konventsiooni teist peatükki. Tähelepanuväärne on see, et nimetatud konventsiooniga on lisaks Euroopa Liidu liikmesriikidele liitunud Austraalia, Kanada, Jaapan, Iisrael, Sri Lanka, USA[52].

Ehk siis tegelikult saab väita, et nimetatud konventsiooni on aktsepteeritud tõe poolest juba laia ringi riikide seas. Mis aga ei tähenda seda, et riigid ei ole siseriikliku õiguse arendamisel läinud siiski ise teed[53]. Nimetatu ongi põhjus, miks peaks võimalikult palju riike liituma nimetatud konventsiooniga. Koostöö ongi võimalik ainult seal ja siis, kui on vastavad kokkulepped sõlmitud ja neid aktsepteeritakse ning neid ka järgitakse.
Juhul, kui kuritegu pannakse toime riigis, mis ei ole konventsiooniosaline ja mis ei ole ka valmis rahvusvaheliseks koostööks, on küberkurjategija tabamine keerukam. Näiteks võib ta hävitada tema poolt talletatud andmed, teda ennast ei pruugita füüsiliselt tabada. Juhul, kui ta varjab end riigis, kus tegu, mida talle ette heidetakse ei ole kuritegu, siis ongi sellises konventsiooniga mitteliitunud riigis olemine talle nagu nö seaduslik vihmavari.
Nimetatud konventsiooni olulisust on avalikult tunnustanud ka mitmed suurettevõtted.
Näiteks 2016, kui täitus 15 aastat konventsioonist, tuli Microsoft oma blogis[54] välja järgneva teatega: „Budapesti konventsioon on oma 15ndal aastapäeval saavutanud nö kuldstandardi rahvusvaheliste konventsioonide seas, mis reguleerib küberkuritegevuse valdkonda. See on kriitiline vahend, mis aitab kaitsta ja turvata meie kliente küberkuritegevuse vastu. Samuti avaldab hiid lootust, et üha rohkem riike ühineb nimetatud konventsiooniga."

Seega on nimetatud konventsiooni, kui rahvusvahelise „relva" tähtsust võitluses kuritegevusega tunnustanud ka eraettevõtted.

Nimetatud konventsiooni preambula kohaselt selle üheks väga oluliseks eesmärgiks on ka täiendada rahvusvahelisel tasandil riikidevahelist koostööd reguleerivaid Euroopa Nõukogu konventsioone ning Euroopa Nõukogu liikmesriikide ja teiste riikide vahelisi sama laadi lepinguid. Nimetatud konventsiooni eesmärk on arvutisüsteemide või -andmetega seotud

[52] Council of Europe. Chart of signatures and ratifications of Treaty 185. Status as of 17/04/2017 https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=N1Folg06
[53] Nt USA föderaalse kriminaalmenetluse reegel nr 41
[54] Microsoft Secure staff blog - The Budapest Convention on Cybercrime – 15th Anniversary , 16-17.november 2017

kuriteo eeluurimise ja menetlemise tõhustamine ning kuriteo elektrooniliste tõendite kogumise võimaldamise huvides olemasolevate konventsioonide täiendamine.

Käesoleva töö jaoks oluliseks valdkonnaks on konventsiooni II peatüki 2. jagu, kus on sätestatud menetlusõigusesse puutuv.
Nimetatud jaos on välja toodud meetmed, mida konventsiooniga liitunud riigid peavad tarvitusele võtma.
Artikkel 14 lg 1-s on kirjas, et konventsiooniosaline võtab seadusandlikke ja muid meetmeid, et kehtestada selles jaos käsitletud eeluurimise ja menetluse kord ning et anda asja eeluurimiseks või menetlemiseks vajalikud volitused. Sisuliselt tähendab nimetatud säte seda, et konventsioonis sätestatud nõudmiste ja eeskirjade siseriiklikku õigusesse üle võtmine tuleb tagada ja konventsiooni ratifitseerinud riigid on kohustatud viima riigisisese õiguse vastavusse konventsiooniga.

Olulised põhimõtted on välja toodud artiklis 15, mille lõike 1 kohaselt konventsiooniosaline tagab, et selles jaos käsitletud volitusi andes ja kasutades ning selles jaos sätestatud korda kehtestades ja kohaldades järgitakse tema seadustes ettenähtud proportsionaalsuspõhimõtet ja asjaomaseid kaitsenõudeid ning inimõiguste kaitse neid sätteid, mis on tema seadustesse võetud Euroopa Nõukogu 1950. aasta inimõiguste ja põhivabaduste kaitse konventsiooni ja ÜRO 1966. aasta kodaniku- ja poliitiliste õiguste rahvusvahelise pakti ning inimõigusi käsitlevate muude rahvusvaheliste õigusaktide alusel ettenähtud kohustustest tulenevalt.

Teiseks kaitsenõudeks, mis on konventsioonis välja toodud on see, et asjaomase volituse või korra laadi arvestades nähakse kaitsenõuetes vajaduse korral *inter alia* ette kohtuliku või muu sõltumatu järelevalve kohaldamine ja esitatakse kohaldamise põhjendus ning kehtestatakse volituse või korra ulatuse ja kestuse piirangud.

Artikkel 15 lõike 3 kohaselt - õiglase õigusemõistmise põhimõtet ja üldhuvi arvestades kaalub konventsiooniosaline võimalust kohaldada selles jaos volitusi ja korda reguleerivaid sätteid kolmanda isiku õigustele, vastutusele ja õigustatud huvile.

Arvutikuritegevusvastane konventsioon kohustab ka internetiteenusepakkujaid (*Internet Service Provider, ISP*) säilitama nende käsutuses olevaid andmeid (sealhulgas kasutaja isikuandmeid) ja need teatud tingimustel uurimisorganitele üle andma. Konventsiooniga

kehtestatakse seega teenuse pakkujaile hulgaliselt lisakohustusi. Näiteks on sätestatud kiirsäilituse ajad (artikkel 16).

Siinkohal vaatleb käesoleva töö autor kõrvalepõikena järgnevalt seda, millised probleemid on tekkinud praktikas seoses teenuse pakkujate käsutuses olevate andmetega.

Nimelt on kriminaalmenetluses alati olulist rolli mänginud sideettevõtjatelt saadud andmed, mille pinnalt saab olulist informatsiooni kuritegude toimepanemise kohta. Viimastel aastatel on Euroopa kohus teinud nimetatud valdkonnas ehk kommunikatsiooni liiklus ja asukohaandmete säilitamisega seoses teinud mitu olulist otsust, mis tulevikus kohustavad riike muutma siseriiklikke seadusi ja olenevalt muudatusest võivad kriminaalmenetlusi mõjutada palju.
Selliste andmete säilitamist reguleeris 2006. aasta 15. märtsil vastu võetud direktiiv 2006/24/EÜ[55], mis käsitleb elektrooniliste sideteenuste ja sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist. Nimetatud direktiivi kohaselt tuli säilitada elektroonilise side teenuste ja sidevõrkude pakkujatel säilitada mitte vähem kui kuue kuu ja kõige rohkem kahe aasta jooksul alates side toimumise päevast kommunikatsiooni liiklus- ja asukohaandmed.
Eestis kehtiva Elektroonilise side seaduse[56] § 111^1 lg 4 kohaselt on teenusepakkujal kohustus säilitada nimetatud andmeid üks aasta, alates side toimumise ajast, kui need sideteenuse osutamise käigus on loodud või neid on töödeldud. Nimetatud olukord võib aga tulevikus muutuda.
Euroopa Kohtu suurkoja 8. aprilli 2014. a otsuse kohaselt kohtuasjades *Digital Rights Ireland.*[57]Euroopa Kohus otsustas, et direktiiviga pandud kommunikatsiooni liiklus- ja asukohaandmete säilitamise kohustus piirab ebaproportsionaalselt Euroopa Liidu põhiõiguste harta artiklites 7 ja 8 sätestatud eraelu ja isikuandmete kaitse õigust. Kohus sedastas, et direktiiv toob liidu õiguskorras kaasa nende põhiõiguste ulatusliku ja väga raske riive, ilma et see riive oleks täpselt piiritletud sätetega, mis võimaldaksid tagada, et riive piirdub tõepoolest vaid vältimatult vajalikuga. Kohus möönis, et kuigi tegemist on eraelu ja isikuandmete kaitse õiguse raske riivega, ei kahjusta see põhiõiguse olemust.

[55] Euroopa Parlamendi ja Nõukogu direktiiv 2006/24/EÜ,15. märts 2006 ELT L 105, 13.04.2006, lk 54–63
[56] Elektroonilise side seadus (lühend - ESS) - RT I, 17.05.2016, 2
[57] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, Digital Rights Ireland Ltd

21.12.2016 otsuses tegi Euroopa Kohtu suurkoda järjekordse otsuse seoses liiklus ja asukohaandmete säilitamise kohustusega. Kohtuotsuses[58] oli välja toodud järgmised asjaolud:
Rootsis asuv elektroonilise side teenuste osutaja Tele2 Sverige teatas 9. aprillil 2014 PTSile, et pärast direktiivi 2006/24 kehtetuks tunnistamist 8. aprilli 2014. aasta kohtuotsusega *Digital Rights Ireland* jt (C-293/12 ja C-594/12, EU:C:2014:238; edaspidi „kohtuotsus Digital Rights"), lõpetab ta alates 14. aprillist 2014 LEKs ette nähtud elektroonilise side andmete säilitamise ja kustutab sideandmed, mida ta kuni nimetatud kuupäevani on säilitanud.
Rootsi Politseiamet esitas 15. aprillil 2014 PTSile kaebuse selle peale, et Tele2 Sverige lõpetas talle kõnealuste sideandmete edastamise.

Nimelt otsustas kohus liidetud kohtuasjades C-203/15 ja C-698/15 (Tele2 Sverige AB jt[59]), et kuritegevuse vastu võitlemise eesmärk iseenesest ei ole piisav, et põhjendada kõikide isikute elektroonilise side andmete kogumist ja säilitamist. Kohus leidis, et riigisisesed meetmed toovad kaasa eraelu puutumatuse ja isikuandmete kaitse (EL põhiõiguste harta[60] art 7 ja 8) ulatusliku riive, mida tuleb pidada eriti raskeks. Kokkuvõtlikult leidis kohus, et Euroopa Liidu õigust tuleb tõlgendada kitsendavalt ning andmete säilitamist ja ligipääsu andmetele saab lubada ainult ja üksnes juhul, kui võideldakse raskete kuritegudega.

Nimetatud kohtuasja p 22- 25 oli välja toodud käesoleva aja regulatsioon Rootsis. Selle kohaselt võivad teabe kogumise raames Rootsi politsei, Rootsi kaitsepolitsei ja Rootsi toll seaduse 2012:278 § 1 alusel selles seaduses ette nähtud tingimustel ja LEK põhjal väljastatud loa alusel tegutseva elektroonilise side võrgu või elektroonilise side teenuste osutaja teadmata koguda andmeid elektroonilise side võrgus edastatud sõnumite kohta, teatavas geograafilises piirkonnas asuvate elektroonilise side seadmete kohta või nende geograafiliste asukohtade kohta, kus elektroonilise side seade asub või asus.
Kohtuotsuse punktist 22 nähtub, et seaduse 2012:278 §-de 2 ja 3 kohaselt võib andmeid põhimõtteliselt koguda siis, kui asjaolud on sellised, et meede on eriti tähtis, selleks et hoida ära, ennetada või avastada kuritegevust, mis hõlmab ühte või mitut kuritegu, mille eest on karistuseks ette nähtud vähemalt kaheaastane vangistus või mis on loetletud selle seaduse §-s 3 ja mille eest on karistuseks ette nähtud vähem kui kaheaastane vangistus. Niisuguse meetme võtmist õigustavad põhjendused peavad üles kaaluma kaalutlused, mis on seotud riive või

[58] EKo. 21. detsember 2016, liidetud kohtuasjad C-203/15 ja C-698/15 (Tele2 Sverige AB)
[59] EKo. 21. detsember 2016, liidetud kohtuasjad C-203/15 ja C-698/15 (Tele2 Sverige AB)
[60] Euroopa Liidu Põhiõiguste harta - Euroopa Liidu Teataja 2012/C 326/02

kahjuga, mille meede toob kaasa isikule, kes on meetme objekt, või vastanduvale huvile. Kõnealuse seaduse § 5 kohaselt ei tohi niisugune meede kesta kauem kui üks kuu.

Kõnealuse meetme võtmise otsuse teeb pädeva asutuse juht või selleks volitatud töötaja. Meetme võtmiseks ei ole vaja kohtu või sõltumatu haldusasutuse eelnevat luba.

Seaduse 2012:278 §-s 6 on sätestatud, et igast andmete kogumise otsusest tuleb teatada Rootsi julgeoleku- ja terviklikkuse kaitse komisjoni. Õiguskaitseasutuste repressiivtegevuse üle järelevalve teostamise seaduse (2007:980) § 1 näeb ette, et see komisjon kontrollib seaduse täitmist õiguskaitseasutuste poolt.

RB reguleerib säilitatavate andmete edastamist siseriiklikele ametiasutustele eeluurimistegevuse raames. RB 27. peatüki § 19 kohaselt on isiku teadmata „elektroonilise side jälgimise alla võtmine“ põhimõtteliselt lubatud eeluurimises, mis muu hulgas puudutab kuritegusid, mille eest on karistusena ette nähtud vähemalt kuuekuuline vangistus. „Elektroonilise side jälgimise alla võtmise“ all tuleb vastavalt RB 27. peatüki §-le 19 mõista isiku teadmata niisuguste andmete omandamist, mis puudutavad elektroonilise side võrgu teel edastatud sõnumit, konkreetses geograafilises asukohas kasutatavaid või kasutatud elektroonilise side seadmeid või geograafilist asukohta või asukohti, kus teatavad elektroonilise side seadmed asuvad või asusid.

Neil asjaoludel otsustas eelotsusetaotluse esitanud kohus menetluse peatada ja esitada Euroopa Kohtule järgmised eelotsuse küsimused:

„1. Kas üldine kohustus säilitada kuritegevuse vastu võitlemise eesmärgil andmeliiklusandmeid, mis hõlmavad ilma igasuguste eristuste, piirangute või eranditeta kõiki isikuid, kõiki elektroonilise side seadmeid ja kõiki andmeid […], on kooskõlas direktiivi 2002/58 artikli 15 lõikega 1, võttes arvesse harta artikleid 7 ja 8 ning artikli 52 lõiget 1?

2. Kas juhul, kui vastus esimesele küsimusele on eitav, võib niisugune säilitamiskohustus siiski olla lubatav, kui:

a) siseriiklike asutuste juurdepääs säilitatavatele andmetele on kindlaks määratud nii, nagu on kirjeldatud [eelotsusetaotluse] punktides 19–36, ning

b) andmete kaitset ja turvet käsitlevad nõuded on reguleeritud nii, nagu kirjeldatud [eelotsusetaotluse] punktides 38–43, ja

c) kõiki andmeid tuleb säilitada kuus kuud alates päevast, mil asjaomane sideseanss lõppes, ning pärast seda kustutada, [nagu kirjeldatud eelotsusetaotluse] punktis 37?“

Sama kohtuasjaga oli liidetud kohtuasi nr C-698/15[61]. Kohtuasja kohaselt nimetatud asjas T. Watson, P. Brice ja G. Lewis esitasid kohtule *High Court of Justice* kaebused, milles nad palusid kontrollida DRIPA[62] § 1 õiguspärasust, viidates muu hulgas selle paragrahvi vastuolule harta artiklitega 7 ja 8 ning EIÕK[63] artikliga 8.

DRIPA § 1 annab siseministrile õiguse võtta ilma kohtu või sõltumatu haldusasutuse eelneva loata vastu üldise korra, mis paneb üldkasutatava telekommunikatsiooniteenuse operaatoritele kohustuse säilitada maksimaalselt 12 kuu jooksul kõiki andmeid postiteenuse või telekommunikatsiooniteenuse kohta, juhul kui siseminister leiab, et niisugune nõue on vajalik ja proportsionaalne Ühendkuningriigi õigusaktides seatud eesmärkide saavutamiseks. Ehkki need andmed ei hõlma sideseansi sisu, võivad need olulisel määral sekkuda sideteenuste kasutajate eraellu.

Court of Appeal (England & Wales) (Civil Division) (apellatsioonikohus (Inglismaa ja Wales) (tsiviilasjade koda)) peatas siseriikliku menetluse ja esitas Euroopa Kohtule järgmised eelotsuse küsimused:

„1. Kas kohtuotsuses *Digital Rights* (sh eelkõige selle punktides 60–62) on sedastatud Euroopa Liidu õiguses valitsevad imperatiivsed nõuded, mida kohaldatakse liikmesriigi korra suhtes, mis reguleerib juurdepääsu vastavalt siseriiklikele õigusaktidele säilitatavatele andmetele, et järgida harta artikleid 7 ja 8?

2. Kas kohtuotsusega *Digital Rights* on harta artikli 7 ja/või 8 kohaldamisala laiendatud üle EIÕK artikli 8 kohaldamisala, nagu selle on kindlaks määranud Euroopa Inimõiguste Kohus oma kohtupraktikas?“

Euroopa kohus leidis kokkuvõttes, et Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiivi 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv), muudetud Euroopa Parlamendi ja nõukogu 25. novembri 2009. aasta direktiiviga 2009/136/EÜ, artikli 15 lõiget 1 tuleb Euroopa Liidu põhiõiguste harta artikleid 7, 8 ja 11 ning artikli 52 lõiget 1 arvesse võttes tõlgendada nii, et sellega on vastuolus liikmesriigi õigusnormid, mis näevad kuritegevuse vastu võitlemise eesmärgil ette kõiki elektroonilise side

[61] Tegemist on kohtuasjas Secretary of State for the Home Department (C-698/15) vs T.Watson, P.Brice, G.Lewis tõusetunud küsimusega.

[62] Data Retention and Investigatory Powers Act 2014 - https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014

[63] Euroopa Inimõiguste ja Põhivabaduste Kaitse Konventsioon – RT II 2010, 14, 54.

vahendeid puudutava kohustuse säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik liiklusandmed ja asukohaandmed.

Direktiivi 2002/58 (direktiiviga 2009/136 muudetud redaktsioonis) artikli 15 lõiget 1 tuleb harta artikleid 7, 8 ja 11 ning artikli 52 lõiget 1 arvesse võttes tõlgendada nii, et sellega on vastuolus liikmesriigi õigusnormid, mis reguleerivad liiklusandmete ja asukohaandmete kaitset ja turvalisust ning eelkõige pädevate ametiasutuste juurdepääsu säilitatavatele andmetele, piiramata seda juurdepääsu kuritegevuse vastu võitlemise raames üksnes raske kuritegevuse vastu võitlemisega; nägemata ette, et andmetele juurdepääsu saamise eeltingimuseks on kohtu või sõltumatu haldusasutuse eelnev kontroll; ning nõudmata, et kõnealuseid andmeid säilitataks liidu territooriumil.

Sisuliselt leidis Euroopa Kohus, et kommunikatsiooni liiklus- ja asukohaandmete säilitamine on vajalik, kuid üldine, kõikide abonentide ja registreeritud kasutajate andmete säilitamine rikub õigust eraelu puutumatusele ja isikuandmete kaitsele. Ehk siis ei tohiks olla andmete mass salvestamist nagu see toimib praegusel hetkel. Juhisena toodi otsuses välja, et riigid peaksid paika panema isikute ringi, kelle andmeid talletatakse, mis on ilmselt keeruline ülesanne, sest et vahel ei vajata kriminaalmenetluses vaid kahtlustatava kohta käivaid andmeid vaid ka kannatanu kohta käivaid andmeid.

Teiseks tuleb täpsemalt määratleda ära kuritegude ring, kus selliseid päringuid teha saab. Eelpool toodu on kindlasti väljakutse, mis on seotud Euroopa tasandil digitaalsete tõendite kättesaadavusega seoses.

Seejuures peaks jällegi sellekohane üldregulatsioon olema Euroopa Liidus ja tegelikult võimalikult laias ulatuses maailmas olema ühtne. Riikide ühtlane regulatsioon tagab selle, et andmed, mida vajab näiteks Eesti, on salvestatud ka USAs ühe pika ajavahemiku jooksul. Samas nimetatud kohtulahendiga seati kahtluse alla Budapesti konventsiooni artikkel 16 kehtivus. Andmete mass salvestamine ei ole kohtuotsuse kohaselt lubatav.

Käesoleva töö autori seisukoht on, et kuni ei ole leitud ühist arusaama selle kohta, milliseid andmeid ja kelle omasid võib salvestada, kaitseb mass salvestamine avalikku korda ja rahu paremini kui see, kui seda ei tehta.

Lisaks on Arvutikuritegevusvastases konventsioonis sätestatud ka rahvusvahelise koostöö üldpõhimõtted, andmete edastamise õigus omal algatusel, väljaandmismenetluse põhimõtted. Abitaotlused esitatakse Interpoli vahendusel.

Seega on kokkuvõttes Arvutikuritegevusvastases konventsioonis sätestatud üldised põhimõtted, mida tuleks konventsiooniosalistel jälgida ja millele peaks vastama liitunud riikide siseriiklik materiaalõigus ja menetluskord.

Järgnevalt toob käesoleva töö autor välja selle, millised on praktikas enim kasutatavad rahvusvahelise koostöö instrumendid.

Üheks võimaluseks, kuidas saada andmeid, mis asuvad teises riigis on rahvusvaheline koostöö eelkõige õigusabitaotluste tegemise näol.

Prokuratuuri aastaraamatu[64] kohaselt lahendas Riigiprokuratuur 2016. aastal kokku 627 välisriigi taotlust seoses rahvusvahelise koostööga kriminaalasjades. Vastastikune koostöö seisnes aastaraamatu kohaselt nii välisriikide õigusabitaotluste täitmises kui ka rahvusvaheliselt tagaotsitavate isikute loovutamises ja väljaandmises välisriikidele ning välisriikides tehtud kohtuotsuste tunnustamises. Kõige tihedam koostöö kriminaalasjades toimub naaberriikide Soome, Läti ja Leeduga.

Aastaraamatu kohaselt esitasid Eesti prokurörid välisriikidele 2016. aastal kokku 343 õigusabitaotlust, nendest 42 koostas Riigiprokuratuur. Euroopa vahistamismääruseid koostasid riigiprokurörid 7, ühes kriminaalasjas taotleti menetluse ülevõtmist ning 11 kuriteoteadet edastati spontaanse informatsioonina välisriigile menetluse alustamise otsustamiseks.

Teise võimalusena on rahvusvahelise koostöö hea näide ühistes uurimisrühmades osalemine.

Prokuratuuri aastaraamatu kohaselt osales Eesti 2016. aastal 9 ühise uurimisrühma (i.k *joint investigation team*) tegevuses. Uurimisrühmade raames menetleti piiriüleste pettuste ja rahepesu kuritegusid, maksukuritegusid, narkokuritegusid, relvadega seotud kuritegusid ning asja hävitamise ja mõrvaga seotud kuritegu. Aastaraamatus on välja toodud, et sageli kestab uurimisrühma töö mitu aastat. Uusi lepinguid ühistööks sõlmiti 2016. aastal 4 (2015: 2 uut lepingut).

Prokuratuuri aastaraamatus tuuakse välja, et ühise uurimisrühma loomine ja selle tegevuses osalemine tähendab prokuröri jaoks väga tihedat rahvusvahelist koostööd ning igapäevast suhtlemist ja infovahetust välisriikide menetlejatega. Piiriüleste kuritegude puhul, kus kuritegusid pannakse samaaegselt toime mitme erineva riigi territooriumil, kahtlustatavad tegutsevad ning tõendid asuvad erinevates riikides, annab ühine uurimisrühm võimaluse väga

[64] Prokuratuuri aastaraamat 2016 – kättesaadav veebis: http://www.prokuratuur.ee/et/prokuratuuri-aastaraamat-2016/rahvusvaheline-koostoo

kiiresti infot ja tõendeid vahetada ilma täiendavate formaalsuste ja õigusbaitaotluste esitamiseta. Prokurörile annab ühises uurimisrühmas osalemine suure rahvusvahelise koostöö kogemuse, sest menetluse planeerimisel ja otsuste vastuvõtmisel tuleb kooskõlastada oma tegevused teiste riikide menetlejatega, s.h arvestada riikide erinevat õiguskorda, kohtupraktikat jms.

Arvutikuritegevusvastase konventsiooni rakendamise ja kaasajastamise eest vastutava komisjoni *T-CY* (*Cybercrime Convention Committee*) raportites on siiski välja toodud, et klassikaline õigusabitaotluste süsteem ei ole piisavalt efektiivne. Nimelt on nad oma 2016.a. raportis[65] esile toonud, et praegused rahvusvahelise õigusabitaotluse menetlusprotseduuris on liiga keerukad, aega ja ressurssi nõudvad ning seetõttu liiga ebatõhusad.
Vastamise ajad ulatuvad keskmiselt kuuest 24 kuuni. Seetõttu hüljatakse paljud taotlused ja ka menetlused.

Kokkuvõttes on nimetatud komisjon leidnud, et klassikalised rahvusvahelise koostöö instrumendid nagu õigusabipalvete esitamine ei tööta sellistel kiiretel juhtudel nagu sageli on vaja menetlejal lahendada seoses digitaalsete tõenditega ja vaja on kiiremaid vahendeid, mis tagaksid võimalikult kiire ja asjakohase tegutsemise võimaluse õiguskaitseasutustele.

Seega on vähemalt nende riikide ringis, kes on ühinenud Arvutikuritegevusvastase konventsiooniga ühene arusaam sellest, et tänapäeval on vaja teistsuguseid ühisreegleid, kui aastal 2004.

Käesoleva töö autor on seisukohal, et see, milline saab tulevikus olema seisukoht digitaalsete tõendite rahvusvahelise kogumise võimalikkusega seoses, sõltub sellest, kuidas ja milliste ühiskonna liikmetena inimesed ennast positsioneerivad. Samuti sõltub see kindlasti ka poliitilistest otsustest nii riikide kui Euroopa Liidu tasandil. Oluline on see, kuidas tulevad teised riigid Euroopa praktika ja kokkulepetega kaasa.

Käesoleval ajal ei ole veel üldiselt selliseid instrumente õiguskordadesse sisse viidud, kuid kui tulevikus tugevneb positsioon, kus seostatakse end väga tugevasti näiteks Euroopa Liidu

[65] Cybercrime Convention Committee (T-CY) . Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group, 16 September 2016

kodanikena või siis mõne teise üleriigilise koosluse liikmena, on võimalik teoorias ka näiteks digitaalsete tõendite puhul see, et neid on võimalik hankida ilma teise riigi õiguskaitseorgani abita, tehes otsinguid ise või nõudes andmeid välja otse teenusepakkujatelt.

Käesoleva töö autori hinnangul on hetkeolukord maailmas siiski selline, et näiteks on küsitav, milline on Euroopa Liit tulevikus (arvestades nt Brexitit). Kas ja kui mõistlik oleks näiteks Arvutikuritegevusvastase konventsiooniga liitunud riikide vahelise koostöö põhimõtted sättida selliseks, et need võimaldaksid saada arvestades üha enam rahvusvahelist keskkonda ka teatud tõendeid ilma lepingupartneri poolsete reaalsete sammudeta – sellele hetkel vastata ei ole üheselt võimalik. Samas on ilmselt rahvusvahelise eraõiguse näitel võimalikud kokkulepped teatud riikide ringi vahel.

Ära ei saa seejuures unustada seda, et Arvutikuritegevusvastase konventsiooniga ei ole käesolevaks ajaks liitunud kõik riigid maailmas. Seega, kui rahvusvahelisel tasandil saavutatakse kokkulepe, mille kohaselt on võimalik kohtu loal näiteks teises riigis pilves asuvate andmeteni jõuda, siis kehtib see kokkulepe siiski vaid nende riikide vahel, kes on konventsiooniosalised.

Lisaks on olemas ka kolmandad riigid – näiteks Venemaa ja Hiina. Venemaaga on Eestil kehtiv õigusabileping, kuid nagu näitas 2007.a. aprillisündmuste praktika, siis ilmselt ei ole Venemaa valmis selliseks koostööks. Suhetes selle riigiga kaalub ilmselt poliitiline olukord üle koostöösoovi kriminaalasjades.

Kõrvalepõikena toob käesoleva töö autor välja selle, et seoses „aprillirahutustega“ alustati kümneid kriminaalasju, millest lahendi said enamasti sellised juhtumid, kus tänavatel märatseti ja korda rikuti. Riigiprokuratuur alustas ka toimunud küberrünnakute uurimiseks kriminaalasja[66], mille raames koostati rünnakute taga olevate isikute tuvastamiseks ka õigusabipalve Vene Föderatsioonile.
Kriminaalmenetlust alustati karistusseadustiku paragrahvide, mis käsitlevad arvutikahjurlust ja arvutivõrgu ühenduse kahjustamist tunnustel. Süüdimõistmisel oleks saanud nimetatud kuritegude eest raskeima karistusena mõista kuni kolm aastat vangistust.

[66] K.Masing. Riigiprokuratuur alustas küberrünnakute uurimiseks kriminaalasja – Eesti Päevaleht 02.05.2007

Eesti riigiprokuratuur saatis Venemaa peaprokuratuurile 10. mail 2007 õigusabipalve, milles palus kaasabi aprilli lõpus alguse saanud Eesti vastaste küberrünnakute taga olevate isikute leidmiseks, kes võivad asuda Venemaal. 28. juunil saabunud vastuses keeldus Vene peaprokuratuur Eesti palvet täitmast. Keeldumise põhjusena tõi Venemaa välja, et Eesti soovitud menetlustoimingute läbiviimine ei ole riikide vahelises õigusabilepingus kajastatud. Käesoleva töö autori arvates oleksid võimaldanud õigusabilepingu sätted siiski rahvusvahelist koostööd. Nimelt hõlmab õigusabileping selle artikli 3 kohaselt järelepärimise saanud lepingupoole seadusandlusega ettenähtud protsessuaaltoimingute sooritamist, nagu poolte, süüdistatavate ja kohtualuste, tunnistajate ja ekspertide ülekuulamist, ekspertiisi tegemist, kohtulikku vaatlust, asitõendite üleandmist, kuriteo toime pannud isikute kriminaaljälitamise algatamist ja väljaandmist, tsiviilasjades langetatud kohtuotsuste tunnistamist ja täitmist, dokumentide kätteandmist ja edasisaatmist ning teise poole palvel süüdistatavate karistatuse kohta andmete esitamist. [67]

[67] Eesti Vabariigi ja Vene Föderatsiooni leping õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades - RT II 1993, 16, 27

2. PILVEANDMETÖÖTLUS, TERRITORIAALSUSPRINTSIIP JA JURISDIKTSIOONIPROBLEEMID

2.1 Pilveandmete omapärad

Suur osa digitaalsete tõenditega kokku puutunud menetlejatest on ilmselt praktikas kokku puutunud ka olukorraga, kus tema ees töölaual on sidevahend või arvuti, mille kaudu on ligipääs selle omaniku või selle kasutajate mõnes teises serveris asuvatele sõnumitele, fotodele, salvestatud paroolidega kontodele, kasutaja käsutuses olevale pilveruumile. Seejuures võib arvata, et nii mõnigi menetleja on vahel ka tahtmatult menetlustoimingu käigus kokku puutunud olukorraga, kus tema kasutuses on andmed, millele kohalduv õigus ei ole üldse see, mis on menetleja asukohariigi õigus. Veel keerulisemaks teeb olukorra see, et menetleja ei pruugi isegi aru saada, et ta sellistele ehk teise riigi õigusega reguleeritud andmetele ligi pääses.

Pilveandmetöötlus tähendab laias laastus seda, et üha vähem on olukordi, kus andmed on ühes kindlas seadmes või siis suletud võrgus. Seejuures kasutavad pilveteenuseid igapäevaselt ka paljud füüsilised isikud. Pilveandmetöötlus on kaasaegse maailma igapäevaosa, tehnoloogia, mis üha enam ületab riikide vahelisi piire. Hoolimata piiridest lubab pilveandmetöötlus olla väga efektiivne ja tagab kasutajatele ka parema teeninduse. Siiski on selle iseloomust tulenevalt kerkinud küsimus – mis saab siis, kui erinevad riigid näevad ette nendele andmetele juurdepääsuks erinevad reeglid?[68]

Ühest küljest annavad andmete pilve talletamise võimalused seega võimaluse hoida kokku kõvaketaste ruumi, mis kuuluvad andmete omanikule ja võimaluse andmetele pääseda ligi maailma eri punktidest. See tekitab aga küsimusi, millist õigust tuleb kohaldada seoses pilveteenusesse salvestatud andmetega. Samuti tekivad selle käigus küsimused, kas ja kelle loal on täitevvõimul luba ligi pääseda teise riigi serverites asuvatele andmetele.

Üha enam on tavapärane see, et andmed on erinevate teenusepakkujate valduses, erinevates asukohtades, erinevates jurisdiktsioonides laiali. Selline andmete hajasus on tingitud pilveteenuse pakkujate organisatsioonilisest ülesehitusest, kus peakorter on ühes riigis, kuid organisatsiooni harud on erinevates riikides.

[68] M.McKenna, Up in the Cloud: Finding Common Ground in Providing for Law Enforcement Access to Data Held by Cloud Computing Service Providers

Pilveandmete töötlust iseloomustab ka see, et sageli ei tea ei andmete omanik ega ka õiguskaitseorganid seda, kus täpselt asuvad andmed, mida ühes või teises kriminaalmenetluses vajatakse. Nimetatud probleem on välja toodud ka varem nimetatud küberkuritegevusevastase konventsiooni rakendamise ja kaasajastamise eest vastutava komisjoni T-CY raportites[69].

Näiteks kui uurimisasutus peab kinni kahtlustatava ning saab tema käest kätte sidevahendi ja sidevahend on seadistatud nii, selles olevad andmed salvestatakse aeg ajalt pilveteenuse abil, et säästa ruumi isiku valduses olevas seadmes, siis ei pruugi ka kahtlustatav ise teada, millise riigi seadustega reguleeritud pilves näiteks tema tehtud fotod on. Menetlusasutuse poole pealt on oluline seejuures vajalikud andmed kätte saada ja sellisel juhul on see ka võimalik, kui seade on avatud ja isik annab nõusoleku andmete vaatlemiseks. Kuid isikul on ka õigus privaatsusele. Lisaks tuleb mängu ka veel usaldus teenusepakkuja vastu – ei ole ju välistatud, et teatud juhtudel võib teenusepakkuja väljastada tema valduses olevad andmed õiguskaitseorganile isiku loata. Käesoleva töö autori hinnangul juhul, kui teenusepakkuja väljastab tema valduses olevaid andmeid õiguskaitseorganile, peab selleks olema seaduslik alus. Praktikas on ilmsiks tulnud aga mitmeid näiteid, kus koostöö teenusepakkuja ja õiguskaitseorganite vahel ei toimi.

Siinkohal peatub käesoleva töö autor 2016.a. kohtuasjal, kus FBI soovis ligi pääseda terrorist Syed Rizwan Farooki telefoni iPhone 5C sisule. Apple teatas, et nad FBI-d aidata ei plaani, kuna see rikub nende privaatsuspõhimõtteid.[70] Nimetatud kohtuasjas oli seega küsimuseks, mis tuli kohtul lahendada õigus privaatsusele versus turvalisus. Ehk teisisõnu - kus läheb piir selle vahel, kas avalik huvi kaalub üles üksikisiku õiguste kaitse.

Nimetatud kohtuasjas pöördus FBI kohtusse ja kohus otsustas, et Apple peab ligipääsemiseks vajaliku tarkvara ikkagi valmis tegema. Operatsioonisüsteemi seda versiooni, mis on terroristi telefonis, ei suuda enda väitel lahti muukida ka Apple ise. Möödunud aasta märtsis teatas FBI aga, et nad ei vaja Apple abi, kuna on suudavad kolmanda osapoole abil ise andmetele ligi pääseda.

[69] T-CY 2014, 2016 raportid
[70] DigitalTrends. Apple vs. the FBI: A complete timeline of the war over tech encryption. 03.04.2016 http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/

Eeltoodud näide annab aimu sellest, et tegelikkuses põrkuvad õiguskaitseorganid sagedasti andmekaitsereeglitega. Samas ei saa ka andmete valdajad endale lubada seda, et nad muutuks klientide jaoks ebausaldusväärseks, kuna privaatsus ja andmekaitse on need valdkonnas, mida enamus inimesi hindab.

Põhiseaduse[71] § 26-s on välja toodud, et sätestab, et igaühel on õigus perekonna- ja eraelu puutumatusele. Riigiasutused, kohalikud omavalitsused ja nende ametiisikud ei tohi kellegi perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks.

Põhiseaduse[72] § 33 on välja toodud, et kodu on puutumatu. Ei tohi tungida kellegi eluruumi, valdusse ega töökohta ega neid ka läbi otsida, välja arvatud seadusega sätestatud juhtudel ja korras avaliku korra, tervise või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks, kurjategija tabamiseks või tõe välja selgitamiseks kriminaalmenetluses.

Põhiseaduse § 43[73] toob välja selle, et igaühel on õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele. Erandeid võib kohtu loal teha kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras.

Põhiseaduse kommenteeritud väljaandes[74] on välja toodud, et suhtlemine ja vaba teabevahetus on osa isikuvabadusest, mistõttu on õigusriigis igaühel põhjust eeldada oma suhtluse privaatsust ning seda, et sõnumite saladuse õigust ei riivata ilma seaduses ette nähtud mõjuvate kaalutlusteta. Kommentaari kohaselt hõlmab sõnumite saladuse õiguse kaitseala sõnumite vahetamist posti teel ja mitmesuguste tehniliste vahendite abil. Sõnum sisaldab teavet inimese mõtete, veendumuste, arvamuste, kavatsuste, sündmuste kirjelduste ja muu kohta, mida inimene sageli soovib jagada vaid valitud suhtluskaaslasega. Avalikult edastatavad sõnumid (nende sisu) kaitset ei vaja. Õigus sõnumite saladusele ajalooliselt kujunenud vajaduse tõttu tagada puutumatus vahendaja kaudu liikuvatele kirjadele ja luua usaldust teenuseosutaja suhtes.

[71] Põhiseadus - RT I, 15.05.2015, 2
[72] Vt viide 71
[73] Vt viide 71
[74] Põhiseaduse kommenteeritud väljaanne, pt 2, § 43

Kehtiv KrMS ei anna vastust sellele, mil määral võib ilma läbiotsimisloata isiku käest saadud sidevahendisse siseneda ja kuidas peaks toimima, kui läbi õiguskaitseorganite valduses oleva seadme ei ole võimalik ligi pääseda kriminaalmenetluses olulisele informatsioonile.

Käesoleva töö autori hinnangul on tegemist probleemiga, mis võib omakorda tuua kaasa probleeme kohtumenetluses, kui võib tõusetuda küsimus, kas tõend on saadud seaduslikul teel.

Selle probleemi üle käib käesoleval ajal aktuaalne diskussioon nii Euroopa Liidu kui ka maailma tasandil üldse.

Küberkuritegevusevastase konventsiooni rakendamise ja kaasajastamise eest vastutav komisjon *T-CY* (*Cybercrime Convention Committee*) on oma 2016.a raportis[75] välja toonud järgmist:

1. Sageli ei ole kriminaalmenetlust toimetavatele õiguskaitseorganitele selge see, millise jurisdiktsiooni alluvuses on salvestatud andmed ja milline õiguslik režiim neile kohaldub. Teenusepakkujatel võib olla peakorter ühes riigis, samas kohaldub teise riigi õigus ja samas on andmed üldse salvestatud kolmandas riigis. Andmed võivad peegelduda ja liikuda erinevate jurisdiktsioonide vahel. Samuti peetakse võimalikuks seda, et teenusepakkuja, see tähendab andmete hoidja võib andmeid liigutada ühest riigist teise, et vältida neile ligipääsu andmist kriminaalmenetluses. On võimalik ka see, et teenusepakkuja ise ei tea täpselt seda, kus ühed või teised andmed parajasti asuvad.

2. Isegi juhul, kui teoreetiliselt on teada see, kus andmed on, siis on vaidlus selle üle, millise riigi õigust kohaldada tuleks, et neile seadusekohaselt ligi pääseda. Vaidlus võib tekkida selle üle, kas kohaldada tuleks teenusepakkuja peakorteri asukohajärgset õigust, selle haru/osakonna asukohajärgset õigust, õigust, mis kohaldub kohas, kus on andmed ja server on või siis hoopis selle koha õigust, kus on teenuse ostja liitunud teenusega. Samuti võib tulla kõne alla hoopis kahtlustatava kodakondsuse või elukohajärgse õiguse kohaldamine.

3. Alati ei ole selge see, kas pilveteenuse pakkuja on vastutav töötleja või volitatud töötleja kasutaja andmete suhtes ja seega on küsimus, millised reeglid kohalduvad.

[75] T-CY (Cybercrime Convention Committee) 2016.a raport - https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

4. Lisaks sellele tõusetuvad jurisdiktsiooni küsimused, kui andmete omanik ei ole teada või kui andmed on salvestatud läbi rahvusvahelise kaashaldamise lahenduse.

Lisaks on problemaatiline see, et teenuse pakkuja võib olla seotud erinevatel tasanditel erinevate jurisdiktsioonidega, mis kohalduvad tema teenusele samal ajal.

Digitaalsete tõendite olemusest lähtudes võib digitaalselt talletatud andmetele ligipääsemise vajaduse tõusetumisel tekkida probleemid isegi siis, kui vajaminevale ligi pääsetakse.

Eelnimetatud raportis on välja toodud kolm eri probleemi, mis võivad tõusetuda seoses pilveandmete saamise vajadusega:

1. Isegi kui serverid on mingi kindla riigi territooriumil, ei saa kindlad olla, et andmed, mida vajatakse asuvad just selle riigi territooriumil. Juhul, kui läbiotsimisluba saadakse, võivad andmed olla krüpteeritud ja krüpteeringu avamiseks vaja minevaid andmeid hoitakse hoopis teises riigis, kus on kohalduv teise riigi õigus. See probleem tekib jällegi tingituna pilveteenuse pakkujate organisatsioonilisest ülesehitusest.

2. Küberründe toimumisel võidakse jõuda valedele jälgedele. On üldteada asjaolu, et küberkurjategijad on osavad ja suudavad oma jälgi varjata.

3. Töötava seadme vaatlusel otse sündmuskohal võidakse saada ligi küll andmetele, mida vajatakse (ka neile, mis on talletatud pilveteenuses), kuid ei saada sageli teada seda, millise õiguskorraga riigis on server, kus andmed on talletatud.

Seega, kui füüsiliste tõendite puhul ei ole enamasti kahtlust tõendile kohalduva õiguse osas, siis digitaalsete tõendite puhul ei ole sageli isegi selge, kus see tõend on ja millist õigust kohaldada tuleks.

2.2 Territoriaalsuspõhimõte ja jurisdiktsioon

Artiklis „*Global Views on Internet Jurisdiction and Trans-Border Access*“[76] on välja toodud järgmist: „Väljendil jurisdiktsioon on erinevad tähendused, sõltuvalt siis sellest, millises kontekstis seda kasutatakse – kas rahvuvahelise õiguse, rahvusvahelise eraõiguse, kriminaalõiguse. Samuti sõltub see sellest, milline on riigi õigussüsteem ja traditsioon riigis. Seejuures on artiklis välja toodud, et selle ulatus võib erineda riigiti, kuna mõiste jurisdiktsioon on sisustatud kahe aspektiga. See on seotud riigi suveräänsusega ja teiseks tähistab riigi võimu selle territoorumil, riigis, regioonis või provintsis.“

Riiklik enesemääramine on rahvusvahelise õiguse põhimõte, mis lähtub rahvaste suveräänsusest ja võrdõiguslikkusest. Sellest tulenevalt on igal rahval õigus omariiklusele, õigus vastu võtta põhiseadus, ise määrata oma riigikord, riigiorganite struktuur ja majandussüsteem ning ise juhtida ja korraldada kogu riigi- ja ühiskonnaelu.[77]

Iga riik määrab kindlaks ise selle, millised seadused kehtivad riigis, kellel on täidesaatev võim jne. Juhul, kui teine riik hakkab toimetama teise riigi õiguskorra alla käivas ruumis kriminaalmenetlust, võib olla tegu ründega suveräänsuse vastu, sest et toimetatakse enda riigi reeglite järgi. Teisel riigil on pädevus ja õigus teise riigi õiguskorra alla käivas ruumis tegutseda ainult omavahelise kokkuleppe või rahvusvahelisi reegleid järgides.

Aga millised reeglid kehtivad internetis ? Eelminematud artiklis on välja toodud, et interneti jurisdiktsioon on kõige vastuolulisemaid valdkondi, mis on seotud interneti valitsemisega. Ei ole ühte arusaama, mis sobiks kõikidele juhtumitele, mis tuleks lahendada piiriüleste probleemide ilmnemisel. On teada, et internetis ei ole selliseid geograafilisi piire nagu on füüsilises maailmas.

Territoriaalsuspõhimõte on üks fundamentaalpõhimõtteid rahvusvahelises õiguses. Selle kohaselt on ka õiguskaitseorganitel pädevus tegutseda oma riigi territooriumil. Arutluse all on õigusteadlaste seas olnud see, mida tähendab tänapäeva internetiühiskonnas territoriaalsuseprintsiip. Näiteks tekib territoriaalsusega seotud küsimus koheselt, kui õiguskaitseorganitel on vaja pääseda ligi teabele, mis on talletatud ekstraterritoriaalselt[78].

[76] C.Velasco,A-M.Osula,J.Hörnle. Global Views on Internet Jurisdiction and Trans-Border Access. Volume 24 of the series Law, Governance and Technology Series , lk 465-476
[77] Põhiseadus - RT I, 15.05.2015, 2
[78] C.Velasco,A-M.Osula,J.Hörnle. Global Views on Internet Jurisdiction and Trans-Border Access. Volume 24 of the series Law, Governance and Technology Series, lk 465-476

Käesoleva töö autor nõustub A.M.Osulaga selles, et ilma rahvusvahelise õiguse põhimõtete järgimiseta ei saa tänapäeval ükski tsiviliseeritud maailma kuuluda sooviv riik hakkama. Samas on riigiti nende põhimõtete järgimine ja arusaam neist erinev. Raske, kui mitte võimatu on nimetada valdkond, kus valitseb absoluutne üksmeel ühe või teise ülemaailmse asjaoluga seoses.

Nii nagu enamuse riikide põhiseadustes, on ka Eesti Vabariigi põhiseadusesse sisse kirjutatud suveräänsus ja territoriaalsuspõhimõte. Põhiseaduse § 1 sätestab, et Eesti on iseseisev ja sõltumatu demokraatlik vabariik, kus kõrgeima riigivõimu kandja on rahvas. Eesti iseseisvus ja sõltumatus on aegumatu ja võõrandamatu. Riigisisestes suhetes tähendab suveräänsus avaliku võimu teostamise monopoli. Kui riigisiseselt suhtleb riik teiste subjektidega ülemvõimu positsioonilt, siis rahvusvahelistes suhetes piirab riigivõimu teostamist teiste riikide suveräänsus, mida iga riik peab austama. Rahvusvahelisel tasandil tähendab riigi suveräänsus riigi vahetut allumist üksnes rahvusvahelisele õigusele ja mitte mõnele muule rahvusvahelise õiguse subjektile.[79]

Põhiseaduse §-s 2 on sätestatud, et Eesti riigi maa-ala, territoriaalveed ja õhuruum on lahutamatu ja jagamatu tervik. Põhiseaduse kommentaarides on välja toodud järgmist: „Et tänapäeval rajaneb riigivõimu teostamine territoriaalprintsiibil, on Eesti territoorium, mis koosneb maismaast, veealadest ja nende kohal olevast õhuruumist, ruumiks, kus asuvad isikud alluvad Eesti riigivõimule (välja arvatud isikud, kellele rahvusvaheline õigus tagab immuniteedi asukohariigi jurisdiktsiooni suhtes, nt teiste riikide riigipead ja diplomaatilised esindajad). Eesti territooriumi piiride kindlaksmääramist reguleerib PS § 122.“[80]
Kommentaari kohaselt rahvusvaheline õigus seob riigi territoriaalse terviklikkuse printsiibi tihedalt riigi poliitilise sõltumatusega. [81]

ÜRO põhikirja[82] art 2(4) sätestab, et liikmesriigid hoiduvad oma rahvusvahelistes suhetes jõu kasutamisest riigi territoriaalse terviklikkuse ja poliitilise sõltumatuse suhtes või sellega ähvardamisest.

[79] Põhiseaduse kommenteeritud väljaanne, § 1 kommentaar p 2.2
[80] Põhiseaduse kommenteeritud väljaanne, § 2 kommentaar p 1
[81] Põhiseaduse kommenteeritud väljaanne, § 2 kommentaar p 2
[82] Ühinenud Rahvaste Organisatsiooni põhikiri ning Rahvusvahelise Kohtu statuut, RT II 1996, 24, 95

Rahvusvahelises praktikas väljendub territoriaalse terviklikkuse rikkumine selles, et riik kaotab täielikult või osaliselt kontrolli ja valduse enda territooriumi üle. Territoriaalse terviklikkuse rikkumine võib seisneda nii riigi territooriumi okupeerimises kui ka tema siseasjadesse sekkumises, kui aidatakse riigivõimu vastu ülestõusnutel mingi maa-ala üle kontrolli saavutada.[83]

Sekkumisena riigi suveräänsusesse võib aga vaadelda ka näidet, kus üks riik otsustab oma kriminaalmenetlust toimetades teha seda ka teise riigi territooriumil. Füüsilises ruumis toime pandud kuritegude puhul on see ilma teise riigi loata peaaegu mõeldamatu.[84] Rahvusvahelise koostöö reeglid on paika pandud erinevate rahvusvaheliste kokkulepetega. Samuti on see reeglistik sätestatud KrMSi rahvusvahelise koostöö peatükis.

Eeltoodud problemaatikaga seotu on olnud arutluse all mitmetes kohtuasjades. Näiteks kestis aastaid Belgias Yahoo kohtuasi, kus USA ettevõte keeldus väljastamast meiliteenuse kasutajate andmeid Belgia prokurörile[85]. Nimetatud kohtuasja valguses oli arutlusel see, kas tegevus prokuröri poolt ei olnud mitte riive teise riigi suveräänsusele.[86]

Belgia kriminaalmenetluse seadustikus on artikkel 88ter, mis puudutab arvutisüsteemide läbiotsimisega seotut. Nimelt lubab see säte kohtunikul, kui ta on andnud loa arvutisüsteemi läbiotsimiseks, laiendada otsinguid ka teise riigi territooriumil asuvasse arvutisüsteemi või selle osasse. Kohtunikul on õigus sellisel viisil lubada läbiotsimist laiendada juhul, kui see on tõe väljaselgitamise huvides vajalik ja kui teised võimalikud uurimis– ja menetlustoimingud ei ole saavutatava eesmärgi suhtes proportsionaalsed või kui on selge oht tõendite hävimiseks. Kohtunik saab lubada ülal kirjeldatud viisil arvutisüsteemi läbiotsimist vaid selliste arvutisüsteemide puhul, kuhu esialgse arvutisüsteemi kasutajatel on ligipääs. Pärast sellist

[83] Põhiseaduse kommenteeritud väljaanne, § 2 kommentaar p 2

[84] Teatud juhtudel on see siiski võimalik – nimelt on Prümi lepinguga kokku lepitud võimalused tabamusepõhiseks juurdepääsuks DNA, FP (sõrmejälgede) ja VRD (sõidukite registreerimisandmed) registritele. Nimetatud lepingus käsitletakse meetmeid terrorismikuritegude ennetamiseks ning muid koostöövorme nagu nt ühispatrullid ja ühisoperatsioonid, abi seoses suursündmustega jms. Lepinguga on kaetud ka meetmed ebaseadusliku rände vastaseks võitluseks

[85] S. De Schrijver, T.Daenens. The Yahoo! Case: The End of International Legal Assistance In Criminal Matters – Who`sWhoLegal, september 2013 - http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters

[86] Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), lk 32. Arvutivõrgus: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8

laiendatud läbiotsimist peab kohtunik teavitama seda isikut, kes vastutab konkreetse arvutisüsteemi eest, kui selline isik on mõistlikul viisil tuvastatav.[87]

Sarnaselt Belgiale ei vaeva ennast eriti suveräänsuse ja territoriaalsusprintsiibi võimaliku rikkumisega Portugal. Nimelt on Portugali küberkuritegevust reguleerivas seaduses (*The Portuguese Law on Cybercrime (Law nº 109/2009, from 15 September 2009*)) reeglid, mis kirjeldavad seda, kuidas käituda digitaalsete tõenditega. [88]
Piiriülene ligipääs andmetele on lubatud nimetatud seaduse alusel arvutiandmete otsimise mõttes. Reeglid, mis on paika pandud on ajendatud nii Portugali kriminaalmenetlust reguleerivast seadustikust kui ka Budapesti konventsioonist. Nimetatud seaduse artikkel 15.1 lubab teha arvutisüsteemis otsinguid, kui menetluse käigus on tekkinud vajadus tõe väljaselgitamise huvides koguda tõenditena andmeid, mis on selliselt salvestatud. Artikli 15.5 kohaselt juhul, kui arvutisüsteemi läbiotsimisel, mis on alanud Portugali territooriumilt, ilmneb, et teave, mida otsitakse, on talletatud teise riigi territooriumil olevasse arvutisüsteemi, kuid neile andmetele saab seaduslikult ligipääsu esialgsest süsteemist, siis võib läbiotsimist laiendada pädeva asutuse volitusel. Selline laiendamise õigus kehtib nii teistele arvutisüsteemidele, mis on Portugali enda territooriumil kui ka väljaspool seda, eeldusel et algsele süsteemile on ligipääs saadud seaduslikult. Lisaks on Portugali küberkuritegude seaduses kirjas, et juhul, kui teise riigi õiguskaitseasutused saavad Portugali võimude eelneva heakskiiduta juurdepääsu andmetele, mis füüsiliselt asuvad Portugalis, siis on neil õigus neid andmeid ka saada (artiklid 25 a ja 25b).[89]

A.M.Osula on artiklis „*Remote search and seizure in domestic criminal procedure: Estonian case study*[90]" välja toonud järgmist: "Rahvusvahelise õiguse kohaselt ei saa riik koguda tõendeid teise riigi territooriumilt, kohaldades iseenda kodumaist õigust välja arvatud juhul, kui see toimub lepingu sätteid järgides või selleks on antud nõusolek. Olukorras, kus tõendi asukoht on teadmata, maadlevad riigid territoriaalsuse põhimõtte tõlgendamisega, et võta seisukoht, millist õigust tuleb kohaldada. Kuigi territoriaalsete piiride tähtsus on järk järgult vähenenud ja väheneb ka edaspidi tänu tehnika kiirele arengule ja vajadusele arvesse võtta keerulisi rahvusüleseid kuritegusid, enamus riike ei pea siiski lubatavaks, et nende

[87] Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), lk 32–33.
[88] vt viide 46, lk 37.
[89] Vt viide 46, lk 38
[90] Osula A-M, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian Case Study' (2016) 24 (4) International Journal of Law and Information

arvutisüsteemidesse või arvutiandmetesse tungitaks teise riigi läbiotsimisorderitega. Seetõttu, õiguskaitseorganite kaugligipääs andmetele, mis on salvestatud teise riigi territooriumil võib olla tõlgendatav, kui teise riigi suveräänsuse riive. Veel enam – ühise arusaama puudumine aksepteeritud praktikast kaugläbiotsimisega seoses tõusetab rahvuste/riikide vahel usaldamatust ja võib viia privaatsusõiguse ja teiste põhiõiguste rikkumiseni. “

Käesoleva töö autor nõustub A.M.Osula poolt väljatooduga, et territoriaalsete piiride tähtsus on järk järgult vähenenud ja väheneb ka edaspidi tänu tehnika kiirele arengule ja vajadusele arvesse võtta keerulisi rahvusüleseid kuritegusid. Territoriaalsete piiride tähtsus on järk järgult vähenenud ka muude riikidevaheliste eluliste olukordadega seoses [91]. Samas saab väita, et nendes valdkondades on siiski olemas riikideülesed selgesõnalised kokkulepped. Kaugläbiotsimiste puhul aga käesoleval ajal sellised kokkulepped puuduvad. Vajadus selleks on olemas, arvestades tehnika kiiret arengut ja küberkurjategijate osavust olemasolevat süsteemi vihmavarjuna ära kasutada.

Seega kokkuvõttes oleks siiski vajalik kujundada seisukoht, kas see, kui menetleja toimetab näiteks teise riigi pilves ilma teist riiki teavitamata on tungimine teise riigi siseellu või on see käesoleval ajal aksepteeritav. Käesoleva töö autori hinnangul ei ole selline tegutsemine teise riigi küberruumis ilma selgete reegliteta lubatav. Käesoleval ajal kehtivas õigusloomes puuduvad garantiid, mis välistaks selle, et juhul, kui riigiülene läbiotsimine oleks lubatud tegevus, selle, et sellist võimalust ei hakataks ära kasutama näiteks teise riigi julgeoleku õõnestamiseks, küberspionaažiks.

Kuni ei ole tehtud riikideüleseid kokkuleppeid, tuleb siiski kasutada olemasolevaid meetodeid ning tegutseda hästi läbimõeldud menetlustaktika aluse.

Arusaamade lahususel ja usaldamatusel on ka otsene mõju riikide rahvuslikule julgeolekule. Ei saa välistada et teoorias võib selline tõlgenduste erinevus kaasa tuua ühel hetkel mõne rahulolematu riigi reaktsiooni teise riigi vastu, mis võib väljenduda kas siis leebemal juhul koostöö tegemise lõpetamisega või halvimal juhul ka jõu kasutamisega. Igas riigis kehtivad siseriiklikud reeglid ja seadused ning neid tuleb teisel riigil austada.

[91] näiteks on Schengeni leppe alusel on kaotatud riikidevaheline piirikontroll.

2.3 Digitaalsete tõendite valdkonna rahvusvahelise koostöö aktuaalsed probleemid ja võimalikud lahendused

Kuigi eelmises peatükis käsitleti juba põgusalt eri riigikordades kehtestatud piiriülese situatsiooniga kehtestatud reegleid, siis on käesolev peatükk pühendatud rahvusvahelise koostöö problemaatikale.

Kuna küberkuritegevus on oma iseloomult rahvusvaheline, siis on ilmselge, et selleks, et selle vastu efektiivselt ja tulemuslikult võidelda, peaksid olema nii rahvusvahelised kui siseriiklikud vahendid sellised, mis võimaldaksid reageerida ja kurjategijad tabada kiired, ökonoomsed ja efektiivsed. Seejuures ei ole oluline ainult mõista seda, et küberkuritegevus on rahvusvaheline aga ka seda, et küberkuritegevuse vastu võitlemine eeldab rahvusvahelist koostööd. Siseriiklikult võib kehtestada küll kindlad reeglid, kuid juhul, kui need ei haaku või on vastuolus riigiüleste kokkulepetega, siis tekib siiski küsimus nende seaduslikkusest. Isegi kui siseriiklik kohus nimetatud reeglid kohtuvaidlustes lubatavaks ja seaduslikuks tunnistab, ei tähenda see seda, et teiste riikide arvates on nad aktsepteeritavad.

*United Nations Offic*e on *Drugs and Crime* 2016.a. raportis[92] on välja toodud, et seadusandlus, tehniline tugi ning võimekuse tõstmine on võtmesõnad, et hakkama saada *darkneti* üha suurema tähtsusega. Õiguskaitseorganid ja kriminaalõiguse süsteem ei ole veel paljudes riikides sellises seisus, et nad oleks võimelised efektiivselt võitlema anonüümsete kaubitsemisplatvormidega nagu seda on *darknet*. See on praktiline probleem, kuid sellest eraldi on veel mitmeid õiguslikke küsimusi, mis tuleb lahendada. Selleks on kohalduva õiguse probleem olukorras, kus andmed liiguvad omasoodu – riigist riiki, eriti olukorras, kus ei ole teada, kus müüja füüsiliselt asub. Lisaks politseiagentide kasutamine, kes võiksid imbuda sellistesse süsteemidesse nii internetis kui ka füüsiliselt, et koguda tõendeid ja õõnestada selliseid võrgustikke. Samuti on lahendamata krüpteerimisega seotu – raporti kohaselt tuleks luua ja ellu viia seadusandlus, mis kohustaks kahtlustatavaid avaldama paroole/krüptovõtmeid. Ja kõige olulisemaks peetakse seda, et riigid suurendaksid oma võimekust digitaalsete tõendite kogumisel.

[92]United Nations Office on Drugs and Crime, „World drug report 2016“ https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf, XXV

17.02.2016 avaldati Justiitsministeeriumi poolt ülevaade[93], kus hinnati majanduskuritegude menetluspraktikat, sealhulgas on eesmärgiks anda ülevaade menetlusaja pikkusest, koormusest ning ressursside paiknemisest. Ülevaates toodi välja, et tulenevalt antud valdkonna spetsiifikast ning ressursimahukusest on põhjendatult ette nähtud eraldi ametnikud, kes tegelevad kriminaaltulu ja varajälitusega. Lisaks spetsiaalsele oskusteabele omab kriminaaltulu tuvastamisele ning varajälitusele spetsialiseerunud ametnik rahvusvaheliste võrgustike kaudu kontakte, mille kaudu võib olla võimalik saada välisriigilt vajalikku informatsiooni oluliselt kiiremini kui aeganõudvate õigusabipalvete kaudu. Näiteks on ülevaates välja toodud, et Eesti Maksu- ja tolliametis on eraldi rahvusvahelise koostöö talitus, kelle ülesandeks on korraldada EMTA-le vajalikku rahvusvahelist koostööd ja vastata õigusabipalvetele. Seetõttu ei pea menetlejad EMTA-s tegelema õigusabipalvetega ning nad saavad keskenduda kuriteo uurimisele.

Õigusabipalveid on peetud Küberkuritegevusevastase konventsiooni rakendamise ja kaasajastamise eest vastutav komisjon *T-CY* (*Cybercrime Convention Committee*) hinnangul äärmiselt aeglaseks ja aeganõudvaks meetodiks rahvusvahelise elemendiga kriminaalmenetluste puhul[94].

Käesoleva töö autori hinnangul ei ole õigusabipalved efektiivsed just nende menetlusaja tõttu, mis varieerub kuudest aastateni. Arvestades aga näiteks Eesti Vabariigis kehtivat KrMSi ja selle kasvõi näiteks vahistuse kestust kohtueelses menetluses reguleerivaid sätteid, tuleb tõdeda, et paljudel juhtudel on enne, kui vastus õigusabipalvele saadakse kriminaalasjas otsustus vastu võtta. Samas on aga teisest küljest õigusabipalved jällegi sellised mehhanismid, mille reeglite osas on riigid jõudnud kokkuleppele ja mis välistavad siiski küsimused territoriaalsuspõhimõtte riivega seoses või siis suveräänsusega seoses. Sellisel viisil saadud tõendite usaldusväärsuse tõendamisel kohtus ei tõusetu ilmselt selliseid küsimusi nagu võiks tõusetuda seoses piiriüleste läbiotsimistega, mis on tehtud teise riigi teadmata.

[93] K-C.Kruusmaa, M.Kärner. Majanduskuritegude menetluspraktika analüüs. Kriminaalpoliitika analüüs nr 5/2015 - http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/majanduskuritegude_menetluspraktika_analuus.pdf

[94] Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY.16.09.2016 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e

Alternatiiv õigusabipalvetele on otse andmete nõudmine näiteks teenuseosutajatelt, kelle valduses on näiteks teave mingi seadme kohta – olgu selliseks teabeks siis andmed, mis võimaldavad krüpteeringut avada või muu kasutaja kohta käiv teave. Samas nii nagu eelpool välja toodud, siis õigus sõnumite saladusele on ajalooliselt kujunenud vajaduse tõttu tagada puutumatus vahendaja kaudu liikuvatele kirjadele ja luua usaldust teenuseosutaja suhtes. Seetõttu pole ka teenuseosutajad väga koostöövalmid igasugustele infopäringutele vastama. Siseriiklikult päringute süsteem teenuseosutajatele toimib, aga rahvusvahelisel tasandil minnakse sellise käitumisega jällegi mööda teisest riigist kui teenusepakkuja asub teises riigis.

Käesoleva töö kirjutaja hinnangul võib ka see tekitada usaldamatust riikide vahel. Näiteks ei saa olla kindel, et sellisel viisil ei hakataks mittesõbralike riikide eriteenistuste poolt koguma infot varjates end kriminaalmenetluse maski taha. [95]

Mitmed suurettevõtted on avaldanud oma kodulehtedel nii öelda läbipaistvuse raportid (*transparency raport*). Näiteks on Apple välja toonud, et nad suhtuvad väga tõsiselt andmekaitse reeglitesse ka juhul, kui saavad abipalve õiguskaitseorganitelt. Sellisel juhul nad ei avalda nende valduses olevat infot, vaid teevad sellisel juhul siiski kaalutlusotsuse, jättes siiski endale õiguse olukorras, kus näiteks on tõsine oht kas mõnele lapsele või muud tõsine oht avaldada andmeid klienti teavitamata. Lisaks on Apple välja toonud, et iga valitsusasutus, sh ka siis õiguskaitseorganid peavad esitama Apple-le läbiotsimisloa, kui nad tahavad saada kasutajaga seotud andmeid, seejuures reserveerib Apple endale õiguse edastada nii vähe andmeid, võimalik[96]. Raportis on välja toodud ka näiteks see, et möödunud aastal esitasid Eesti õiguskaitseorganid Apple-le2 taotlust.

Seega on ilmselge vajadus, et riigiüleselt kehtestataks uued reeglid, mida aktsepteeriks nii erasektor kui ka avalik sektor. Seejuures tuleb leida tasakaal riigi huvide ja eraisikute/juriidiliste isikute õiguste vahel. Eeltoodust nähtub, et senised seaduslikud meetmed on kas liiga aeglased või ei aktsepteeri neid erasektori esindajad. Seega on vaja esiteks tõsta õigusabitaotluste menetlemise kiirust ja teiseks on vaja tõsta usaldust avaliku sektori ja erasektori organisatsioonide vahel. Ilmselt saab esimese probleemi lahendada sellega, et kehtestada siiski riikide vahelise kokkuleppega tähtajad õigusabitaotluste vastamisele. Teiseks probleemi

[95] Vt viide 9
[96] Apple Inc. Report on Government Information Requests January 1 - June 30, 2016 https://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf

lahendusena võiks kaaluda seda, et koos erasektoriga töötatakse välja teatud reeglid, milliste alusel tehtavatele päringutele on erasektoril kohustus vastata.

Koostöö erasektoriga eeldab seda, et kokkulepped sõlmitakse nii rahvusvahelisel tasandil kui ka siseriiklikult. Eesti kehtivas KrMS § 215-s[97] on sätestatud uurimisasutuse ja prokuratuuri määruste ning nõuete kohustuslikkus. KrMS § 215 lg 1 kohaselt uurimisasutuse ja prokuratuuri määrused ja nõuded nende menetluses olevates kriminaalasjades on kohustuslikud kõigile ning neid täidetakse kogu Eesti Vabariigi territooriumil. Sama paragrahvi kolmanda lõike kohaselt KrMS § 215 paragrahvi lõikes 1 sätestatud kohustuse täitmata jätnud menetlusosalist, kriminaalmenetluses osalevat muud isikut või menetlusvälist isikut võib eeluurimiskohtunik prokuratuuri taotlusel trahvida kohtumääruse alusel. Kahtlustatavat ja süüdistatavat ei trahvita. Käesolevasse töösse ei mahu nimetatud riigipoolse nõude aluse ulatuse analüüs, kuid siiski on see näide, et siseriiklikult on Eestis kehtestatud reeglid, mis nõuavad ka erasektorilt koostööd kriminaalmenetluses.

Arvestades aga rahvusvahelise elemendi esinemist kuritegevusega seoses, tuleks selline reegel kehtestada ka rahvusvaheliselt, kaasates seejuures läbirääkimistele võimalikult palju selliseid partnereid kelle häält ja kelle tegusid ning kelle kokkuleppeid aktsepteeritakse ka teiste poolt ning nendest juhindutakse.

Ehk oleks kasu sellest, et pärast erasektorilt andmete mittesaamist saadetakse vastavasisuline teade asjasse puutuva riigi õiguskaitseorgale, kes saab mingites ajalistes raamides kohustada erasektori organisatsiooni andmeid avaldama.

[97] Kriminaalmenetuse seadustik, RT I, 31.12.2016, 46

3. DIGITAALSETE TÕENDITEGA SEOTUD ERIREGULATSIOONID

3.1 Soome õigus ja Norra õigus

Järgnevalt vaatleb käesoleva töö autor, kuidas on sätestatud digitaalsete tõendite kogumisega seotu Soomes, Norras ja teistes riikides.

Juhani Riekkinen on ajakirjas *Digital Evidence and Electronic Signature Law Review*[98] välja toonud käsitluse digitaalsete tõenditega seotu reguleeritusse Soome kriminaalmenetluse seadustikus. Riekkinen on tõdenud, et küberkuritegevus erineb oluliselt traditsioonilistest kuritegevuse vormidest. Valdavalt eksisteerib see digitaalses ja elektroonses vormis arvutiandmetena, millel on erinevaid karakteristikuid, mis eristab seda traditsioonilistest füüsilistest objektidest ja dokumentidest. Arvutiandmed (ka andmed üldiselt) on sõltuvad riistvarast ja tarkvarast ja on rohkem või vähem haavatavad. Seda saab lihtsalt üle viia, kopeerida, muuta, võltsida, kahjustada või kustutada – isegi ilma füüsilise ligipääsemiseta konkreetsesse seadmesse, kuhu see on salvestatud, tahtlikult või ettevaatamatusest.

Riekkinen on artikli sissejuhatuses välja toonud, et õiguskaitseorganitele antud volitused on olulised vahendid täidesaatva võimu esindajale. Nad tagavad huvide kaitstuse, mis on seotud õigusemõistmisega, teisest küljest nad teevad võimalikuks tõendite erinevad kogumise viisid erinevaid meetodeid kasutades. Samuti mängivad nad olulist rolli peaaegu kõikides kriminaalmenetlustes.

Soome õiguses erisätteid digitaalsete tõenditega seoses ei ole. Nende kriminaalmenetluse seadustik on üldine, digitaalsete tõenditega toimitakse samamoodi nagu füüsiliste tõenditega. Suuremate probleemidena toob Riekkinen nimetatud artiklis välja probleemi, mille kohaselt tekitab menetlejates küsimusi andmetest koopiate tegemine, samuti on probleemsed juhud, kui tuleb tegemist teha krüpteeritud andmetega – puuduvad mehhanismid krüpteeringu avamiseks kohustamiseks. Lisaks toob ta välja, et probleem on ka jälitustegevusega, kuna isikutel on vähe võimalusi selle seaduslikkuse kontrollimiseks.

Norra kriminaalmenetluse seadustikus on reguleeritud üldine tõenditele ligipääsu kord. Sätted on üldsõnalised, digitaalne tõend ei ole reguleeritud eriviisil. Samas on nende elektroonilise side seaduse kohaselt võimalik küsida ilma kohtu loata otse andmeid teenusepakkujatelt. [99]

[98] J.Riekkinen. Digital Evidence and Electronic Signature Law Review. 13 (2016).
[99] Transborder access to data and jurisdiction: Options for further action by the T-CY (2014),lk 36-37

Norra õigusteooria kohaselt võivad Norra õiguskaitseorganid ligi pääseda elektroonilisel viisil salvestatud andmetele sama moodi nagu konto omanik, juhul, kui neil on kehtiv läbiotsimisluba ja juhul, kui kasutajanimi ja ligipääsukoodid on olemas. Samas puudub statistika, kui sageli seda tehtud on. Üldiselt puudutab teises riigis salvestatud andmetele ligipääsemine sellist juhtu, kus on vajalik ligi pääseda e-mailile ja sotsiaalmeediale ja see ligipääs on saadud kooskõlas artikliga 32 Budapesti konventsioonist. [100]

3.2 Horvaatia õigus

Horvaatia kriminaalmenetluse seadustikus[101] on eraldi välja toodud digitaalse tõendi mõiste, kuid see on suuresti ka kõik, mis puudutab digitaalsete tõendite eraldi reguleeritust nimetatud õiguskorras. Horvaatia kriminaalmenetluse seadustiku artiklis 202 lõikes 32 on sätestatud, et digitaalne (elektroonne) tõend on andmed, mis on kogutud tõendida elektroonses (digitaalses) vormis kooskõlas selle seadusega.

Artiklis 331 on välja toodud, et kui seaduses ei ole erisätteid digitaalse tõendi osas, kohaldatakse tavaliste tõendite kogumisele sätestatud reegleid, mis on seaduses välja toodud.

Horvaatia õiguses on huvipakkuv see, et seal on kehtestatud läbiotsimisloale ajaline piirang. Nimelt on sätestatud artiklis 242 lõikes 3, et läbiotsimisorderi alusel tuleks läbiotsimist toimetada kolme päeva jooksul. Peale kolme päeva möödumist ei tohi läbiotsimist toimetada enam selle kohtumääruse alusel. Läbiotsimist lubav määrus tuleb tagastada viivitamatult kohtunikule, kes selle tühistab. Eesti seaduses sellist piirangut ei ole. Autori arvates ei ole õigustatud ka sellise piirangu kehtestamine, kuna see seab olulisi ajalisi piire menetlejatele ja võib takistada kriminaalmenetluse tulemuslikku läbiviimist.

3.3 Sloveenia õigus

Sloveenia on üks riikidest, mille kriminaalmenetluse seadustikus on erisätted digitaalsete tõendite kohta olemas ja seda alates aastast 2009.

Nimelt on selle riigi kriminaalmenetluse seadustiku[102] sisse viidud kaks ulatuslikku erisätet, mis reguleerivad digitaalsete tõendite saamiseks elektrooniliste seadmete arestimist, ära

[100] Transborder access to data and jurisdiction: Options for further action by the T-CY (2014),lk 36-37
[101] Zakon o kaznenom postupku, 3 July 2009

[102] Criminal Procedure Act (official consolidated text) (Slovenia)

võtmist, samuti nendelt saadud andmete säilitamist ja lisaks on üldised juhised, mis kajastavad seda, kuidas neid uurida tuleks.

Sloveenia kriminaalmenetluse seadustiku artiklites 219 ja 223 on kehtestatud üldised juhised elektroonsete tõendite kogumiseks kriminaalmenetluses. Seejuures on lähtutud asjaolust, et paljude kriminaalasjade juures ei ole elektrooniline seade see, mis on ülioluline vaid just need andmed, mis seal sees või sellesse talletatud on. [103]

Ajakirjas *Digital Evidence and Electronic Signature Law Review*, 7 on aastal 2010 Liljana Selinšek avaldanud artikli digitaalsete tõenditega seotust Sloveenia õiguskorras. Ta on välja toonud, et vajadus digitaalsete tõendite osa sisseviimiseks Sloveenia õiguskorda tekkis suuresti 2008.a. Sloveenia konstitutsioonikohtu otsusest[104], mille kohaselt see, kui loetakse sms-de sisu ja otsitakse telefonist andmeid viimaste kõnede kohta on sisu vaatlus ja sekkumine kommunikatsiooniprotsessi. Selliseks tegevuseks peab olema politseil Sloveenia konstitutsioonikohtu otsuse kohaselt kohtu luba.

Uued sätted, mis viidi kriminaalmenetluse seadustikku sisse on oma olemuselt laiad – nad ei reguleeri vaid privaatsusega seotud küsimusi vaid kogu sellise info kogumist, mis on elektroonses vormis ja mis on vajalikud kriminaalmenetluses. Lisaks sellele on artiklis välja toodud, et mõiste „elektrooniline seade“ on Sloveenia õiguse mõistes lai ja seda kasutatakse ka näiteks nende seadmete kohta, mis on ühendatud elektrooniliste seadmetega ja ka elektrooniliste andmekandjate kohta.

Artiklid 219 ja 223 reguleerivad kolme protseduuri, mis on seotud elektrooniliste tõenditega:

1. Elektrooniliste seadmete arestimist, ära võtmist
2. Andmete elektroonilises vormis säilitamist
3. Elektrooniliste seadmete uurimist.

Sloveenia kriminaalmenetluse seadustiku artikli 219 lg 1 kohaselt on lubatud uurida elektroonilisi andmekandjaid ja nendega seotud seadmeid, sh ka telefone, arvuteid jne eesmärgiga saada elektroonilises vormis informatsiooni selle kohta, et rünne toimus ja on tõenäosus, et elektroonilised seadmed sisaldavad elektroonilisi andmeid, mille pinnalt on võimalik tuvastada kahtlustatav või süüdistatav, tuvastada kuriteo jälgi, mida saab kasutada

[103] L.Selinšek. Electronic evidence in the Slovene criminal procedure act. Digital Evidence and Electronic Signature Law Review, Vol 7, lk 77- 86
[104] Vt viide 101, 102

kriminaalmenetluses. Loetelu elektroonilistest andmekandjatest ja seadmetest ei ole seejuures suletud nimekiri.

Sloveenia õiguse kohaselt tuleb prokuröril saada kohtu luba selleks, et otsida läbi digitaalne andmekandja. Seejuures peab ära näitama taotluses selle, milline on nimetatud elektrooniline seade, millelt loodetakse digitaalseid tõendeid leida, teiseks tuleb ära määratleda see, miks on vaja nimetatud seade läbi vaadata, kolmandaks see, millist teavet loodetakse andmekandjalt/elektroonselt seadmelt leida, neljandaks on vaja välja tuua see, miks on vaja just sellist uurimismeetodit kasutada ja miks see on vajalik.

Nii nagu selgub nimetatud artiklist, on võimalik ka Eesti mõistes edasilükkamatu läbiotsimise võimalikkus. Seejuures on oluline see, et suulisele loale tuleb saada 12 tunni jooksul kohtu kirjalik kinnitus läbiotsimise lubatavuse kohta. Juhul, kui seda ei saada, peab politsei hävitama kogutud andmed ja 8 päeva jooksul teavitama ka andmete kustutamisest/hävitamisest kohtunikku, prokuröri ja andmete omanikku.[105]

Järgmine protseduur, peale läbiotsimise teostamise ja andmete saamise on andmete vaatlus. Vaatlus peab olema läbi viidud vastavate eksperditeadmistega isiku poolt. Seejuures ei ole Sloveenia kriminaalmenetlusõiguses määratletud seda, milline peaks olema vastav haridus/väljaõpe – see on jäetud vaidluse korral kohtu otsustada. Andmete vaatlusel tuleb talletada järgnev informatsioon:

1. Tuleb identifitseerida elektroonne seade, mida vaadeldakse.
2. Samuti tuleb ära märkida menetlustoimingu algus ja lõpp, kui uurimistoimingus tehakse pause, tuleb ka need ära märkida.
3. Kirjalikult tuleb fikseerida menetlustoimingul osalejate nimed.
4. Välja tuleb tuua kohtu luba, mille alusel vaatlust toimetatakse.
5. Vaatluse käik.
6. Vaatluse tulemused ja muu oluline ja asjakohane teave.

Sellised nõuded erinevad osaliselt Eestis kehtivast praktikast. Tuleb tõdeda, et pigem sarnanevad sellised nõuded eksperdi poolt koostatud ekspertiisiakti ülesehitusele, kui sidevahendi/andmekandja vaatlusprotokollile.

Lisaks eeltoodule on Sloveenia kriminaalmenetluse seadustiks säte, mis kohustab elektroonilise seadme omanikku abistama ja vajadusel avaldama paroolid, juhul, kui andmed on krüpteeritud

[105] Vt viide 100,101

võtmed, millega saab teavet dekrüpteerida. Juhul, kui abist keeldutakse on menetlusosalist võimalik karistada rahatrahviga või vabaduse kaotusega. Samas ei saa sellist abistamiskohustust nõuda aga kahtlustatavalt/süüdistatavalt ega ka näiteks kaitsjalt. Kahtlustatava puhul kehtib enese mittesüüstamise privileeg.

Veel on huvitav, et erisätted on toodud ka juhuleiu kohta. Nimelt on artiklis 219a sätestatud reeglid selliseks juhuks, kui elektrooniliste tõendite uurimisel avastatakse juhuslikult informatsioon mingi teise kuriteo kohta. Kui selline teave leitakse, tuleb selle leidmine talletada ajaliselt, samuti tuleb sellise info leidmisest koheselt teavitada prokuröri, kes otsustab kriminaalmenetluse alustamise. Juhul, kui prokurör leiab, et kriminaalmenetluse alustamine ei ole otstarbekas ja puuduvad ka muud alused sellise teabe uurimiseks, tuleb see teave hävitada. Sellise teabe hävitamine tuleb samuti ajaliselt fikseerida.

Lisaks sellele – Sloveenia kriminaalmenetluse seadustiku artikli 219 paragrahvis 11 on reguleeritud see, et kui elektroonilist tõendit on uuritud vastuolus kohtu poolt antud loaga, ilma kohtu loata, ilma omaniku kirjaliku nõusolekuta, siis kohus ei saa teha otsust tuginedes sellisel viisil saadud teabele ja sellisel viisil saadud tõend ei ole lubatav.

Kokkuvõttes leiab käesoleva töö autor, et Sloveenia kehtiv õigus, mis puudutab kriminaalmenetluses elektrooniliste tõendite kogumist seab menetlejale mõneti kõrgemad nõudmised, kui Eestis hetkel kehtiv kriminaalmenetluse praktika. Näiteks on läbiotsimistaotluste põhistamise kohustus olemas ka Eesti õiguses, kuid see ei sea nii selgeid kriteeriume selle kohta, mis peab kindlasti olema ära näidatud.

Samuti ei ole Eestis menetlejal kohustust juhuleiu puhul koheselt prokuröri teavitamiseks, kes peab otsustama kriminaalmenetluse alustamise, vastasel juhul leitud teave hävitatakse. Leian, et Sloveenia kriminaalmenetluse seadustiku digitaalseid tõendeid käsitlevad sätted austavad inimeste privaatsust enam, kui meie KrMSi vastav osa, mis ei ole küll spetsiaalselt digitaalsete tõendite kohta käiv, kuid mida järgides nimetatud valdkonnas toimetatakse.

3.4 Digitaalsete tõendite menetlemise juhend prokuratuuris

Alates 24.05.2016 on Prokuratuuris kasutusel IT tõendite menetlemise soovituslik juhend[106]. Nimetatud juhendi preambulas on välja toodud, et käesolev juhend annab edasi prokuratuuride

[106] Prokuratuuri IT- tõendite menetlemise soovituslik juhend, 24.05.2016.

ja erinevate uurimisasutuste kooskõlastatud arusaamu selle kohta, kuidas koguda kohtueelse uurimise käigus IT-tõendeid ja kuidas nendega ümber käia. Sisuliselt on juhendis nii menetlusõiguse kohta käivad selgitused, samas on aga välja toodud ka menetlustaktika põhimõtted, mida võiks järgida.

Juhendi eesmärk on ühtlustada IT-tõendite kogumise praktikat prokuratuurides ja uurimisasutustes. Seega annab juhend edasi üldiseid põhimõtteid, millest praktikud saaksid oma töös juhinduda.

Selliste juhiste loomine näitab käesoleva töö autori arvates seda, et seadusandlik regulatsioon ei ole käesoleval ajal Eesti õiguses piisav, et tagada ühtne praktika digitaalsete tõendite kasutamisel ning selleks, et kriminaalmenetluses toimetataks eri piirkondades ühte moodi, ongi vaja selliste juhiste olemasolu. Üldjuhul ongi juhiste kehtestamine vajalik, kui seadus on üldine, praktika on piirkonniti erinev, kohtupraktika ei ole piisav, et lahendada vajalikke küsimusi.

Autori seisukoht on, et selline juhis kompenseerib hetkel õigusmaastikul olevat olukorda, kus digitaalsete tõendite regulatsioon ei ole piisav, et tagada praktikutele igapäevatöös selged arusaamad selle kohta, kuidas midagi, millal ja ka kelle poolt teha.

Nimetatud juhise kohaselt tuleb kriminaalmenetluses IT-tõendeid koguda ja kasutada nii, et tõendusteabe usaldusväärsus oleks maksimaalselt tagatud. Selleks tuleb järgida kolme põhimõtet, milleks on IT-tõendite identifitseeritavuse, jälgitavuse ja rikkumatuse tagamine.

Samuti tuuakse juhises välja, et üldjuhul toimub IT-tõendite uurimine andmekandjast tehtud koopia käitlemise kaudu. See tähendab, et menetluse käigus on vaja võimalikult täpselt ja kvaliteetselt dokumenteerida ka tõendite uurimisele eelnenud tegevused, mis on seotud tõendite kogumisega, nagu IT-seadmete ja -andmete äravõtmise ning andmetest tõendusväärtusliku koopia tegemisega.

Siinkohal peatub autor andmekandjast tehtud koopial, sest see on just üks aspekt, mis eristab digitaalset tõendit füüsilisest tõendist. Kuigi ka füüsiliste tõendite hulgas on neid, mille koopiaid uuritakse (sõrmejäljed, jalatsijäljed, rehvijäljed jne), siis digitaalsete tõendite puhul võib väita, et peaaegu eranditult uuritakse koopiat, mitte aga originaali, kuna originaali on lihtne kahjustada.

Nii nagu eelpool välja sai toodud, siis on digitaalsed tõendid väga kergesti nii muundatavad kui ka lihtsalt hävitatavad. On üldteada, et nende oskamatust käsitlemisest tingitud tagajärjed võivad olla korvamatud.

Riigikohus on lahendis 3-1-1-46-10[107] välja toonud, et kriminaalmenetluse seadustiku § 123 lg 1 kohaselt võib tõendamisel kasutada dokumenti, mis sisaldab teavet tõendamiseseme asjaolude kohta. Kuigi viidatud säte ei ava dokumendi mõistet, saab selle pinnalt siiski teha järelduse, et KrMS § 123 lg 1 tähenduses on dokumendi kvaliteet ka originaaldokumendi koopial ja ärakirjal, mis sisaldab teavet tõendamiseseme kohta. Samas märgib kolleegium, et kuigi ka originaaldokumendi koopia on kriminaalmenetluses lubatud tõendiks, tuleb selle võltsimiskahtluse korral lahendada küsimus kõnealuse tõendi usaldusväärsusest.
Seega juhul, kui koopia tegemisel järgitakse kehtestatud reegleid, ei tohiks kohtus tõusetuda sellist küsimust nagu eelpool välja toodud kohtuasjas, kus eksperdil tuli kohtus selgitada, kuidas koopia tegemise protsess käib ja ega juhuslikult tegemist ole rikutud koopiaga. Samas ei ole reguleeritud Eestis see, milliseid vahendeid andmekandjast koopia tegemisel kasutada võib. Samuti ei ole Eestis teadaolevalt kehtestatud ühtset-selget reeglistikku selle kohta, millistele tingimustele peab vastama koopia tegemise protsess ja mida selle tegemisel arvestada tuleb.

Koopia alusel vormistatakse harilikult vaatlusprotokoll. Seda nõuab ka KrMS § 86, mis sätestab, et dokumendi või muu objekti vaatlusel selgitatakse kuriteojäljed ja muud tunnused, mis on vajalikud kriminaalasja lahendamiseks ning on aluseks objekti kasutamisel asitõendina ja kui asitõendiks olevat dokumenti, asja või muud objekti on vaja täiendavalt uurida, tehakse asitõendi vaatlus.

Praktikas teevad koopiad andmekandjatest kas eksperdid või vastava väljaõppe saanud menetlejad (IT-haridusega menetlejad) või siis menetlejad ehk uurijad, jälitajad. Andmete kopeerimine on ka üks võimalik infotehnoloogiaekspertiisi ülesanne.

Infotehnoloogiaekspertiisi tegemine tähendabki üldisemas mõistes andmete kopeerimist, märksõnade alusel informatsiooni tuvastamist, kustutatud informatsiooni taastamist, tegevuste

[107] RKKo 3-1-1-46-10/p 8.3.1, 18. juuni 2010

modelleerimist, pahavara analüüsi, mobiilsetest seadmetest andmete kopeerimist, elektroonikaseadmete testimist[108].

Samas ei ole infotehnoloogia eksperdid ainukesed, kellel lasub digitaalsete tõenditega seoses oluline roll. Vahel tuleb kasutada digitaalsete tõendite kohtukõlbulikuks muutmiseks ka kujutiseekspertide abi.

Näiteks tekkis seoses kujutiseeksperdi pädevusega ja tegevusega küsimus kriminaalasjas nr 3-1-1-82 - 16[109]. Nimetatud asjas vaidlustas kaitsja maa ja ringkonnakohtu otsuse riigikohtus ning väitis, et kujutiseekspertiisi käigus parandati algsete videofailide kvaliteeti ja need ühendati, mis kahandab nende failide tõendusväärtust. Tuvastatud ei ole, millises mahus videofaile muudeti, ja seega ei saa ekspertiisiakti lubatava tõendina käsitada.

Riigikohus tõi esmalt nimetatud lahendis välja, mis on kujutiseekspertiis ja mis on selle sisu: „ Kujutiseekspertiisi sisuks on lahendi kohaselt kujutise tehniline uuring. See hõlmab eeskätt kujutava materjali digitaalset töötlust (nt videosalvestise kvaliteedi parandamine, selle kaadrite eraldamine ja liitmine), aga ka kujutise analüüsi, sh erinevate kujutiste töötlemisjärgset võrdlevat uurimist jms. Ekspertiisiobjektide töötlemine ja võrdlemine on vastavate ekspertiisiülesannete püstitamisel kujutiseekspertiisis teineteisega rohkemal või vähemal määral seotud uuringud, mis tagavad võimalikult täpse, põhjaliku ja tulemusliku ekspertiisi tegemise. Nii sõltub kujutiste võrdlemise täielikkus ja tulemuslikkus paljuski kujutava materjali töötlemise mahust ja spetsiifikast (nt videosalvestiste kvaliteedi parandamine, et võrrelda erinevatel salvestistel olevate isikute eritunnuseid). Seepärast ei ole kujutiseeksperdi pädevuses mitte üksnes kujutiste digitaalne töötlus, vaid ka nende võrdlemine ja seeläbi võrdlemist võimaldavate tunnuste väljatoomine. Kuna ekspert töötleb kujutiseekspertiisi käigus enda eriteadmistest lähtuvalt kujutavat materjali ja uurib (nt võrdleb) selle pinnalt kujutisi, võib ta uuringute põhjal anda ka eksperdiarvamuse (vastavasisulise ekspertiisiülesande korral) kujutistel sedastatavate tunnuste samasuse, sarnasuse ja erinevuse kohta. Sellest johtuvalt ei väljunud ekspert arutatavas kriminaalasjas ekspertiisiakti tegemisel temale antud pädevuse piiridest ning kohtud ei eksinud kujutiseeksperdi esitatud eksperdiarvamusele tuginedes.“[110]

Nimetatud kohtuasjas jäi eriarvamusele riigikohtunik E. Kergandberg. Nimelt nentis kohtunik, et jääks mõnevõrra hätta, selgitamaks seda, et millisele teadusvaldkonnale

[108] Kutsestandard, kohtukriminalistikaekspert, tase 7 – leitav veebist: http://www.innove.ee/UserFiles/Kutseharidus/Malle/kohtukriminalistikaekspert-tase-7.3.pdf
[109]RKKKo 3-1-1-82 – 16, 7.november 2016
[110] RKKKo 3-1-1-82 – 16/ p 15, 7.november 2016

tugineb kujutisekspertiis ja kuidas kujutisekspertiisiakti hindamisel kontrollida, kas eksperdiarvamus on ikka teaduslikult põhjendatud. Samuti ei olnud tema hinnangul kujutiseekspertiisi akti põhjendava ja lõpposa (eksperdiarvamuse) võrdlemisel kuidagi võimalik kindlaks määrata seda, et milles siis seisneb selle ekspertiisi puhul eksperdiarvamuse eriteadmistele tuginev järelduslikkus. Eksperdiarvamuses lihtsalt korratakse veelkord üle seda, mis on kirjas juba ka põhistavas osas. Samuti nentis ta seda, et ilmselt vajab kriminaalmenetluses ekspertiisi ja muus vormis eriteadmiste kasutamisega seonduv seadusandja uut sekkumist.[111]

[111] RKKKo 3-1-1-82-16, E.Kergandbergi eriarvamus.

4. DIGITAALSETE TÕENDITE ERIREGULATSIOONI VAJADUS KRIMINAALMENETLUSE SEADUSTIKUS

Nii nagu eelpool välja toodud, on käesoleval ajal käimas maailmas aktiivne diskussioon digitaalsete tõenditega, eriti piiriüleste andmetega seoses. Eestil tuleks teha lähiajal otsustus selle kohta, kas ja kuidas reguleeritakse KrMS-s või mõnes alama astme õigusaktis digitaalsete tõenditega seotut.

Eelpool olevast nähtub, et tegelikult seistakse silmitsi kolme suurema probleemiga:

1. Kas digitaalsete tõenditega seoses peaks olema KrMS-s eriregulatsioon?
2. Kuidas peaks olema reguleeritud rahvusvahelise koostöö vajadusega seotu?
3. Kuidas peaks olema reguleeritud elektrooniliste andmetega seotud läbiotsimised ?

On riike, kes on enda kriminaalmenetlust reguleerivatesse seadustesse sisse kirjutanud digitaalseid tõendeid käsitlevad sätted ja on neid riike, kes seda veel teinud ei ole. Eesti on üks nendest riikidest, kes ei ole veel kriminaalmenetluse seadustikku sisse kirjutanud digitaalsete tõendite kohta käivat eriregulatsiooni, kuid seda ilmselt plaanitakse lähiajal[112].

Käesoleva aasta 9.veebruaril esitas Justiitsministeerium arvamuse avaldamiseks kriminaalmenetluse seadustiku revisjoni väljatöötamiskavatsuse (edaspidi VTK). Väljatöötamiskavatsuse eesmärgiks on süsteemne KrMS analüüs kohtueelse menetluse perspektiivist[113].

Siseriikliku menetlusseadustiku kaasajastamine on iseenesestmõistetav, sest ajaga tuleb kaasas käia. Käesoleva töö autori seisukoht on, et KrMS vajab kaasajastamist ja selle kaasajastamine on vajalik seoses ühiskonnas toimuvate kiirete arengutega tehnoloogia valdkonnas. Üha enam kuritegevust on seotud internetiga. Selleks, et sellega efektiivselt võidelda, on vaja siseriiklikku õiguskorda sisse viia muudatused, mis tagaksid menetlejatele aja- ja asjakohased vahendid võitluses kuritegevusega.

Õiguskantsler on varem samuti juhtinud tähelepanu, et arvestades elektroonilise suhtluse laia kasutusala ning elektroonilistes andmekandjates sisalduva info teatavaks saamisega kaasnevat

[112] VTK-s on ajaliselt ette nähtud, et osaliselt jõustuvad muudatused juunis 2017 (esimese etapi muudatused, kus vaidlust ei ole), teised muudatused pärast 2018. aastat, digitaalse kriminaalmenetluse osas 2023.
[113] Kriminaalmenetluse seadustiku muutmise seaduse eelnõu väljatöötamise kavatsus 09.02.2017 - http://eelnoud.valitsus.ee/main/mount/docList/aca7e3cf-d349-4a40-a700-bbdb2b5a115c#qGL4zV3Q

põhiõiguste riive ulatust, oleks asjakohane kaaluda, kas täpsem regulatsioon (koos vajalike menetlusgarantiidega) aitaks kaasa põhiõiguste ja –vabaduste paremale tagamisele.[114]

Raul Narits on välja toonud järgmist[115] :“ Ühiskondlikke suhteid tuleb reguleerida siis ja niivõrd, kui see on ühiskonna jaoks oluline. Kui ei teki probleeme ühiskonnas ja suhted reguleeritakse muul viisil, ei ole otstarbekas sinna õiguslikult sekkuda. Hea seaduse üheks kvaliteeditunnuseks on tema vajalikkus. Regulatsioonid peavad olema optimaalsed ja menetlus peab olema lihtne.“

Nii on ka KrMSi vaadates ilmselge, et see, mis sai kunagi KrMSi sätestatud, võib olla ajaliselt juba iganenud ja ei sobi kaasaega. Lisaks on ka oluline roll siiski üha enam rahvusvahelisemaks muutuvas keskkonnal, kus menetlejatel tegutseda tuleb. Väljakutsed kurjategijate tabamisel on teistsugused, kui need olid aastaid tagasi.

Näiteks eeldavad rahvusvahelist koostööd organiseeritud kuritegevuse valdkonda kuuluvad kuriteod. Õigusabipalved ning rahvusvahelise koostöö eri vormid kasvõi näiteks uurimisgruppide moodustamise näol on kaasajal paljude suuremate kriminaalasjade lahutamatu osa. Teine näide on eelkirjeldatud pilveproblemaatika, kus on rahvusvaheline moment väga tõsiselt sisse kodeeritud.

Samuti on üha enam kõne all olnud privaatsuse kaitse ajal, kus inimesed enda tegevusest iga päev küberruumi jälgi jätavad. Sageli on kerkinud küsimused, kas ja kui kaugele inimeste privaatsusesse on menetlejal õigus tungida erisuguste kriminaalasjade raames.

Ka Riigikohus on oma viimastes lahendites rõhutanud seda, et jälitustegevuse aluseks saab olla ainult siiski vägagi põhjendatud vajadus, ära tuleb näidata, miks ei saa muud moodi isikute puhul esile kerkinud kahtlustusele kinnitust leida. Näiteks tõi riigikohus lahendis 3-1-1-112-16[116] välja, et jälitustoimingu loa põhjenduses peab sisalduma selge ja arusaadav argumentatsioon mh ka jälitustoimingu vajalikkuse ehk KrMS § 126.1 lg-s 2 sätestatud jälitustoimingu tegemise eelduste kohta. Jälitustoimingu vajalikkuse tuvastamisel kehtib küll lihtsustatud põhjendamisstandard, kuid see ei tähenda, et põhistus võiks rajaneda standardsetel ja deklaratiivsetel formuleeringutel. Määrusest peavad nähtuma konkreetsed kriminaalasja

[114] Õiguskantsleri 05.12.2012.a. arvamus kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõule (295 SE) - http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=52727c38-5c97-433d-bc25-eda7af8db244& , punkt 27

[116] RKKKm 3-1-1-112-16/ p 31, 23.02.2017

tehioludest ja uurimise senisest käigust lähtuvad põhjendused selle kohta, millised asjaolud välistavad tõendite kogumise muude menetlustoimingutega või raskendavad seda oluliselt.

Väljatöötamiskavatsuse on välja toodud vajadus teha KrMSis muudatusi seoses digitaalsete tõenditega seonduva ebaühtlase menetluspraktikaga. Nimelt tuuakse praeguse KrMSi puudusena välja erisätete puudumist, mis reguleeriks digitõendite kogumist, talletamist ja käitlemist. Väljatöötamiskavatsuses on välja toodud, et selleks, et kohaldada digitaalsetele tõenditele kehtivat KrMSi, tuleb tegeleda seaduse tõlgendamisega ja see tõlgendamisviis on küsitav.[117]

Nii nagu eelpool oli välja toodud, siis näiteks Prokuratuur on koostanud digitaalsete tõendite kasutamise juhendi, et ühtlustada menetluspraktikat. Menetluspraktika ebaühtlus on ka üks VTK-s väljatoodud aspekte.

KrMSi revisjoni VTK-s on sätestatud kaks suuremat eesmärki, mida soovitakse revisjoniga saavutada[118] :

Digitaalsete tõendite täpsema regulatsiooni eesmärk on sätestada KrMS-is digitaalseid tõendeid puudutav regulatsioon selliselt, et:

a) ühelt poolt oleks tagatud võimalus koguda ja kasutada kriminaalmenetluses tõendina digitaalseid teabetalletusi nii, et ükski asjakohane ja õiguspäraselt saadud tõend ei jääks menetlusõiguse ebaselguse, vasturääkivuse või lünga tõttu tõe tuvastamisel uurimata ja analüüsimata; ja

b) teiselt poolt oleks kehtiva menetlusõigusega tagatud, et kriminaalmenetluses tõendina kasutatav teave oleks kogutud ja menetluses käideldud tõendusteabe usaldusväärsust tagaval ja selle kontrollimist võimaldaval viisil ning et digitaalsete tõendite kogumisel ja kasutamisel ei riivataks ebaproportsionaalselt teabevaldajate õigusi ja huve.

Tegelikkuses seistakse kahe võimaliku lahenduse ees – kas kehtestada erikord digitaalsete tõendite kogumise ja kasutamise osas või seda mitte teha. VTK autorid on välja toonud, et selline erikord tuleks siiski seaduse tasandil sätestada.

Lisaks on kaalutud, kas sätestada ka seoses teabetalletusest koopia tegemise ja kasutamise osas tõendina eriregulatsioon, sätestades sealhulgas seaduses eraldi digitaalsest teabetalletusest

[117] Vt viide 112
[118] Vt viide 112

tõendusväärtusliku koopia loomine ja vastava menetlustoimingu tegemise nõuded. Teine variant on, et seda mitte teha. Nii nagu nähtub VTK-st, siis on eelistatud hetkel siiski nõuete kirjapanek seadusesse.

Lisaks on kerkinud praktikas küsimus andmekandjalt tõendusteabe otsimise tingimuste osas.

VTK- s on välja toodud järgmist: „Lahendada on vaja küsimus, millise regulatsiooni alusel peaks toimuma digitaalse andmekandja sisu uurimine, kas vaatluse või läbiotsimise regulatsiooni alusel.“[119]

Eneli Laurits on Kohtute aastaraamatus aastal 2015[120] välja toonud järgmist: Seega, kui füüsilise maailma puhul on menetlejal kohustus konkreetselt välja tuua, millise objekti otsimiseks on määrus antud, siis digitaalsete tõendite otsimise puhul see ei kehti. Nii piisab sisuliselt vaid sellest, kui menetleja määrab, et digitaalseid tõendeid on vaja otsida ning läbiotsimiskohast võetakse ära andmekandja(d). Hiljem ei piira vaatluse käiku aga miski ning fikseeritakse vaid leitud tõendamiseseme seisukohast tähtsad esemed. Protokollis kajastatakse küll vaatluse käik, kuid selle täpsusaste on menetleja enda otsustada. Kui füüsiline koht otsitakse läbi, toimub see vähemasti kohaliku omavalitsuse esindaja juuresolekul, siis vaatluse juurde ei ole kohustust menetlejal kedagi kaasata.“

Hetkel on VTK koostajad väljendanud seisukohta, et tuleks kehtestada andmekandjatelt digitaalsete tõendite otsimisele eriregulatsioon, mis on sisult analoogne läbiotsimise regulatsiooniga või mis võiks teatavates olukordades ja võimalusel sisalduda ka tavapärases läbiotsimismääruses.

Praktikas on Riigikohus sellele aspektile ka oma lahendites tähelepanu pööranud: RKKKm 16.05.2012 nr 3-1-1-57-12, p 16[121]: „Arvutiandmete läbiotsimisel ja arestimisel proportsionaalsuse põhimõttega arvestamine tähendab, et ära võtta või arestida võib vaid sellises ulatuses andmeid või andmekandjaid, mis on menetluse läbiviimiseks ja tõendamiseseme asjaolude selgitamiseks vajalikud. Võimaluse korral tuleks asjassepuutuvad andmed kopeerida, kahtlustatava arvutist kustutada või talle kättesaamatuks muuta, mitte aga

[119] Vt viide 112
[120] E.Laurits. Mõned probleemid arvutisüsteemi läbiotsimisel. Kohtute aastaraamat 2015, lk 138
[121] RKKKm nr 3-1-1-57-12/p 16, 16.05.2012

arvutit, arvutisüsteemi või andmekandjat tervikuna ära võtta. [---] Neid põhimõtteid tuleb arvestada ka kohtul asitõenditega toimimise viisi silmas pidades [---].“

Siinjuures tuleks arvestada seda, et juhul, kui eriregulatsioon kehtestada, tuleb arvestada, et näiteks ei ole võimalik see, et seatakse absoluutne piirang ja ajaliselt piiratakse läbiotsimistaotluses ja sellega kaasnevas kohtu loas leitavate andmetega seotut. Näiteks võib isik seadistada oma arvuti kella ja kuupäeva nii, et dokumentidele jääb vale kuupäev ja kellaaeg.

Neljas oluline muudatus, mida kavandatakse on jälitustoimingu dokumenteerimise kohustuse täiendamine – VTK-s on välja toodud, et kehtiv KrMS § 126[10] ei näe ette kohustuslikke nõudeid jälitustoimingute dokumenteerimiseks selles osas, mis puudutab digitaalandmete kogumise protsessi ning andmete autentsuse ja terviklikkuse tagamise meetmete kirjeldamist. Probleemi lahendamiseks tuleks KrMS-i täiendada jälitustoimingute dokumenteerimise nõuetega juhul, kui jälitustoiminguga kogutakse digitaalset teavet[122].

Arvutikuritegevusvastase konventsiooni artikkel 16 näeb ette, et konventsiooniosaline võtab seadusandlikke ja muid meetmeid, et võimaldada oma pädevatel asutustel korraldada liiklusandmete ja muude arvutiandmete kiirsäilitus, kui on alust arvata, et arvutiandmed on kaduma mineku või muutmise suhtes kaitsetud. VTK-s on välja toodud, et käesoleval ajal ei näe KrMS ette alust nõuda teabevaldajalt kaotsiminekule või muutmisele altite andmete säilitamist ja menetlejale üleandmist, mida nõuavad Arvutikuritegevusvastase konventsiooni artiklid 16, 17 ja 18. Ka selle lahenduseks on õigusselguse huvides eelistatud see, et tulevikus on KrMS-is eraldi toiminguna ette nähtud andmete kiirsäilitamise ja üleandmise nõudmine koos asjassepuutuvate menetlust tagavate meetmete ja menetlusgarantiidega.

Käesoleva töö autor leiab, et sellised muudatused nagu on kavandatud KrMSi revisjoniga toovad õigusmaastikule selgust. Mitmeti tõlgendatavad olukorrad reguleeritakse paremini ja ilmselt toob see kaasa olukorra, kus menetluspraktika ühtlustub.

Kavandatavate muudatuste mõju väljendub eelkõige asjassepuutuva regulatsiooni selguse ja arusaadavuse paranemises ning sellest lähtuvalt ka isikute õiguste riive ettenähtavuse nõude paremas täidetuses. Seetõttu mõjutavad planeeritavad muudatused üksnes kriminaalasjades

[122] Vt viide 112

kahtlustatavaid ja süüdistatavaid, kelle põhiõigused on paremini kaitstud ning ka menetlejaid, kelle tegevus on selgemalt seaduses reguleeritud. Selliseid mõjusid on aga võimatu täpsemalt kvantifitseerida. [123]

Käesoleval ajal on VTK-s välja toodud järgmised muudatused, mida plaanitakse seaduse muutmisega teha:

1. Sätestada seaduses erikord digitaalsete tõendite kogumisele ja kasutamisele.
2. Sätestada seaduses eraldi digitaalsest teabetalletusest tõendusväärtusliku koopia loomine ja vastava menetlustoimingu tegemise nõuded. Käesoleva töö autor leiab, et see muudatus on positiivne, sest et see muudab tõendi kogumise tee jälgitavamaks ja seetõttu tõusetub ilmselt vähem küsimusi selle kohta, kas originaalandmetel ja koopial võivad olla erinevusi.
3. Kehtestada andmekandjatelt digitaalsete tõendite otsimisele eriregulatsioon, mis on sisult analoogne läbiotsimise regulatsiooniga või mis võiks teatavates olukordades ja võimalusel sisalduda ka tavapärases läbiotsimismääruses. Ka seda muudatust peab käesoleva töö autor positiivseks. Lisaks tuleks kehtestada eriregulatsioon ka digitaalsete andmekandjate vaatlusele. Nii nagu E.Laurits on välja toonud[124], siis vaatluse käiku ei piira miski ning fikseeritakse vaid leitud tõendamiseseme seisukohast tähtsad esemed.
4. Jälitustoimingu dokumenteerimise kohustuse täiendamine - kehtiva KrMS § 126^{10} ei näe ette kohustuslikke nõudeid jälitustoimingute dokumenteerimiseks selles osas, mis puudutab digitaalandmete kogumise protsessi ning andmete autentsuse ja terviklikkuse tagamise meetmete kirjeldamist. Probleemi lahendamiseks tuleks KrMS-i täiendada jälitustoimingute dokumenteerimise nõuetega juhul, kui jälitustoiminguga kogutakse digitaalset teavet. Täiendustega tuleks sätestada jälitustoimingu käigus saadud digitaalse teabetalletuse kohustuslik lisamine jälitustoimingu protokollile ning kohustus kajastada jälitustoimingu protokollis teabetalletuse terviklikkuse ja autentsuse tagamise meetmed.

   Ilmselt paneb selline muudatus lisakoormuse menetlejatele, hetkel jääb arusaamatuks, mida täpselt peetakse silmas kohustuse all kajastada jälitustoimingu protokollis teabetalletuse terviklikkuse ja autentsuse tagamise meetmed. Üldjuhul lisatakse kriminaalasja materjalidele niikuinii teabetalletus, mida kahtluse korral ka kohtus kuulatakse.

[123] Vt viide 112
[124] Vt viide 119

5. Andmete kiirsäilitamise ja üleandmise nõue - kehtiv KrMS ei näe ette alust nõuda teabevaldajalt kaotsiminekule või muutmisele altite andmete säilitamist ja menetlejale üleandmist, mida nõuavad Arvutikuritegevusvastase konventsiooni artiklid 16, 17 ja 18. Näha KrMS-is eraldi toiminguna ette andmete kiirsäilitamise ja üleandmise nõudmine koos asjassepuutuvate menetlust tagavate meetmete ja menetlusgarantiidega.

6. Arvutiandmete otsingu laiendamine - kehtiv KrMS ei näe ette, et tõendusteabe otsimisel arvutisüsteemist on lubatud koguda teavet ka teistest arvutisüsteemidest või andmekandjatelt, mis on otsingule allutatud arvutisüsteemiga ühendatud tehnilise lahenduse kaudu ja on otsingule allutatud arvutisüsteemi kaudu kättesaadavad (Arvutikuritegevusvastane konventsioon, riigisisese otsingute laiendamise osas artikkel 19 lg 2 ning teiste konventsiooniosaliste arvutisüsteemide osas artikkel 32(b)). Vastava võimaluse sätestamiseks tuleks täiendada KrMS vaatluse või digitaalsete tõendite otsimise eriregulatsiooni. Välisriigis (või teadmata asukohas, nt pilveserveris) asuvatele andmetele ligipääsemise ja sel viisil saadud andmete tõendina kasutamise küsimus on ka rahvusvaheliselt suuresti reguleerimata, samas kui selliste andmete kasutamine muutub kriminaalmenetlustes järjest olulisemaks.

Tegemist on positiivse muudatusettepanekuga, kuna nii muutub siseriiklik õigus täpsemaks ja arvestab rohkem Arvutikuritegevusvastase konventsiooni sätetega. Samas ilma konkreetset seadusemuudatuse teksti nägemata ei saa öelda, kas ja millised rahvusvahelisusega seotud probleemid see lahendab.

Käesoleva töö kirjutamise ajaks on kooskõlastused KrMSi muutmise eelnõu väljatöötamiskavatsusele andnud Rahandusministeerium, Sotsiaalministeerium ja Siseministeerium. Arvamuse on andnud Riigikohus.

Riigikohus väljendas oma arvamuses järgmist: „Leiame, et kehtiva regulatsiooni üle vaatamine ja muutmine digitaalsete tõendite kogumise ja kasutamise eripärast tulenevalt on vajalik. Arvestades igapäevaselt digitaalselt edastatavate, säilitatavate jm viisil töödeldavate andmete mahtu, on vajalik sätestada seaduses nt arvandmete kogumise ja tõendina kasutamise tingimused ning puudutatud isikute menetlusgarantiid (vt ka nt EIKo 14.03.2013 Bernh Larsen Holding AS jt *vs*. Norra; EIKo 03.09.2015 Servulo ja Associados – Sociedade de Advogados, RL *vs*. Portugal).“. Ehk siis ka Riigikohus on leidnud, et üheks kindlasti täpsustamist vajavaks

aspektiks on kõik, mis puudutab igapäevaselt digitaalselt edastatavaid, säilitatavaid ja muul viisil töödeldavaid andmeid.

Esimeses lahendis (EIKo 14.03.2013 Bernh Larsen Holding AS jt *vs*. Norra[125]), millele riigikohus viitas oli arutuse all juhtum, kus kaebajateks on kolm äriühingut. Norra maksuamet viis läbi revisjoni esimese kaebaja suhtes ning soovis enda valdusesse saada arvuti serveris asuva teabe. Kaebaja ei lubanud juurdepääsu kogu serverile põhjendusega, et seda kasutasid ka teised kaebajad oma raamatupidamise andmete hoidmiseks. Seejärel andis maksuamet korralduse ka teiste kaebajate suhtes revisjoni läbiviimiseks. Viimased nõustusid teabe välja andma, kuid esitasid koheselt kaebuse kohtule selle meetme vastu. Maksuamet lõpetas teiste kaebajate suhtes alustatud revisjoni ilma sisuliste toiminguteta. Norra kohtute arvates ei olnud nõue saada juurdepääsu kogu serverile ebaproportsionaalne, sest maksuametil on õigus saada juurdepääs ka paberdokumentide arhiivile vaatamata sellele, et seal hoitakse teiste ettevõtete andmeid. Maksuametil on maksusaladuse hoidmise kohustus. Avaldus EIK-ile oli konventsiooni artikli 8 rikkumise tuvastamiseks.

Euroopa inimõiguste kohus leidis, et kõigile elektroonilistele ühistele andmekandjate juurdepääsu saamine tulenes Norra seadustest ja Norra Ülemkohtu praktikast, mille kohaselt maksuametil on lai diskretsioon saada juurdepääs kõigile dokumentidele, mis võivad omada maksustamise aspektist tähtsust. Ökonoomika põhimõttest tulenevalt ei saa eeldada, et maksuamet selekteerib juba ette välja sellised dokumendid, millega ta soovib lähemalt tutvuda[126]. Seega tulenes meede seadusest. Meetmel oli ka legitiimne eesmärk – s.o riigi majanduslike huvide kaitse. Seega jäi selgitada, kas riive oli vajalik demokraatlikus ühiskonnas. Samuti leidis kohus, et kaebajate huvide kaitseks oli mitmeid tagatisi. Esimesele kaebajale teati revisjonist aasta ette. Kõigil kaebajatel oli võimalus esitada andmete võetuse kohta kaebus, mida nad ka tegid. Seejärel pitseeriti äravõetud andmekandjad kuni kohtuotsuse jõustumiseni. Pärast revisjoni lõpule viimist kuulusid andmekandjad hävitamisele.

Teises kohtuasjas[127] olid kaebajateks Portugalis tegutsev advokaadibüroo ning neli advokaati, sh partner. Kriminaalmenetluse käigus Portugali valitsuse poolt Saksamaa ettevõttelt kahe allveelaeva ostutehingu uurimiseks andis eeluurimiskohtunik loa advokaadibüroo

[125] EIKo 14.03.2013 Bernh Larsen Holding AS jt *vs*. Norra
[126] EIK toetus sellele, et vaidlusaluses arvutis olid andmed segiläbi – ei olnud selget jaotust erinevate andmesubjektide kaupa.

[127] EIKo 03.09.2015 Servulo ja Associados – Sociedade de Advogados, RL *vs*. Portugal

läbiotsimiseks ning arvutite ja dokumentide äravõtmiseks. Kohtunik määratles, et otsida tuleb materjale 35 märksõna alusel. Advokaadibüroo esitas enne läbiotsimise teostamist kaebuse kohtule, märkides, et märksõnad on määratletud laialt ning võivad tuua kaasa asjasse puutumatu teabe saamise. Kohus ei rahuldanud kaebust. Läbiotsimise juures viibisid eeluurimiskohtunik, büroo esindajad ja advokatuuri esindaja. Materjalide esialgsel läbivaatamisel otsustas eeluurimiskohtunik määrata 850 andmekandja hävitamise. Kaebajate avaldus EIK-ile oli konventsiooni artikli 8 rikkumise tuvastamiseks.

Euroopa inimõiguste kohus leidis lahendis, et kuigi eeluurimiskohtuniku määruses oli läbiotsimise ese määratletud laialt, tagati kaebajatele kõik seadusest tulenevad tagatised omavoli vastu. Eeluurmiskohtunik tagas põhiseaduslike õiguste kaitse enne menetlustoimingu läbiviimist, selle läbiviimise ajal ning pärast selle toimumist. EIK-il puudus alus kahelda kohtuniku otsustuses seoses materjalide esialgse läbivaatamisega. EIK leidis, et kaebajate professionaalsesse tegevusse sekkumine ei olnud ebaproportsionaalne, lähtuvalt selle legitiimsest eesmärgist.

Kohtuotsusele esitatud eriarvamuse kohaselt oli vaatamata kohaldatud garantiidele oli läbiotsimise määruse sõnastuses läbiotsmise ese määratletud liiga üldiselt.

Siseministeerium leidis VTK kohta arvamust avaldades, et erikorda digitaalsete tõendite kogumisele ja kasutamisele ei tuleks kehtestada vaid tuleks säilitada selles osas senine olukord, kus eriregulatsioon puudub, tehes seaduses minimaalseid täiendusi ja muudatusi praktikas ilmnenud vastuolude ja lünkade kõrvaldamiseks[128].

Lisaks sellele tõi Siseministeerium välja, et infotehnoloogia areng on ja jääb seadusandluses tehtavatest muudatustest kiiremaks, mistõttu on kiirelt vananeva erikorra sätestamise asemel sobiv lahendus jätta kõnealused küsimused praktikute lahendada. Samas on nad oma arvamuses seisukohal, et kindlasti peaks kaasajastama KrMS-i selle osas, et oleks arvestatud digitaalsete andmete eripäraga.

Siseministeerium ei näe vajadust reguleerida tõendite kogumise eripära, argumenteerides seda kokkuvõtlikult sellega, et teiste eriliigiliste tõendite puhul seda tehtud ei ole.

[128] Siseministeeriumi 13.03.2017 arvamus VTK kohta, leitav veebis: http://eelnoud.valitsus.ee/main#AWTTk3L0

Lisaks on Siseministeeriumi arvamuses välja toodud, et digitaalsetele tõenditele rakenduvad samad üldnõuded nagu usaldusväärsuse ja kontrollitavuse tagamine (*chain of custody*), mis muudele tõenditele. Vastavalt kriminalistika nõuetele toimub üldnõuete tagamine eriliigilise tõendi spetsiifikast lähtuvalt nii, nagu seda tehakse teistegi tõendite osas.

Käesoleva töö autori hinnangul on siiski eriregulatsioon vajalik. Tavaliste tõendite puhul ei ole kerkinud selliseid küsimusi nagu on see, millist õigust peaks kohaldama ja kas Eesti eeluurimiskohtunik on pädev tunnistama lubatavaks sellise läbiotsimistaotluse, mille puhul on alust arvata, et menetleja ei piirdu vaid Eesti õiguskorraga seotud andmetega.

Käesoleva töö autori seisukoht on, et juhul, kui KrMSi muudatused vastu võetakse, peavad nad olema vastu võetud selliselt, et õiguslik reguleeritus oleks tabav. Õigusnorm peab oma iseloomult olema võimalikult täpne. Seega tuleks eelnevalt kaardistada võimalikult täpselt praegu olemasolev olukord. Eelnõu koostamisel tuleks võimalikult täpselt selgitada välja see, milliseid õiguslikke tagajärgi tulevikuregulatsioon kaasa tuua võiks. Samuti tuleks hea õigusloome juures võtta aega ja mõelda. Täpselt nii nagu Eesti vanasõna – 7 korda mõõda, 1 kord lõika.

Kui praegusel ajal ei ole KrMSis eraldi digitaalsete tõendite kohta käivat regulatsiooni, ei tohiks ka tulevikus kehtima hakkav regulatsioon olla selline, mis on oma olemuselt selline, mis väga kiiresti ajale jalgu jääb või ei vasta tegeliku elu ootustele. Samas peab kehtestatav regulatsioon olla selline, mille pinnalt saavad menetlejad oma käitumist kujundada ja mis on arusaadav normi adressaatidele.

Samuti ei plaanita ühemõtteliselt sätestada regulatsiooni piiriüleste läbiotsimiste jaoks. See jäetakse siiski selliseks uduseks alaks, kus õiguse kohaldajatel tuleb ise praktikas rakendatav välja kujundada. Ilmselt ei ole Eesti valmis minema USA teed pidi ja kehtestama seale kriminaalmenetluse reeglistikuga sarnast reeglit nagu on reegel 41[129]. See ei oleks käesoleval ajal veel ka kooskõlas Arvutikuritegevusvastase konventsiooniga.

[129] Vt viide 12

KOKKUVÕTE

Probleemid tõusetuvad praktikas, kokkulepped sõlmitakse riikide tasandil. Siseriiklikud ja riikide-ülesed kohtud lahendavad küll vaidlused, kuid vaidlustes ei selgu alati tõde. Ilma küsimusi esitamata ei saa tekkida ka vastuseid. Seega loodetavasti saab lugeda veel palju kohtulahendeid, milles tuuakse välja argumente seoses digitaalsete tõendite erisustega. 7 korda mõõda, 1 kord lõika. Nii tuleks toimida ka käesoleva töö autori hinnangul uue siseriikliku kriminaalmenetluse seadustiku regulatsiooni kehtestamisel. Seejuures tuleks arvestada nii rahvusvahelisi parimaid praktikaid kui ka seda, millised probleemid on siseriikliku õiguse kohaldamisel tekkinud.

Käesolevas töös on välja toodud küberkäitumise omapärad, see, et digitaalseid tõendeid ning nende asukoha ja kogumisega seotut iseloomustab rahvusvaheline mõõde. Küberruum on oma olemuselt selline, et seda on väga raske piiritleda. Kriminaalmenetluse ruumiline kehtivus põrkub sageli probleemi otsa, kus menetlejal tuleb endalt küsida, kas need andmed, mida ta vajab asuvad just selle riigi territooriumil, mille seadust järgides ta parajasti kriminaalmenetlust toimetab või esineb kriminaalmenetluses rahvusvaheline element ning ta peaks vaatama rahvusvahelise koostöö instrumentide poole. Küberrünnakute uurimine ei ole üldjuhul võimalik ilma rahvusvahelise koostööta. Kuigi siseriiklikult on kehtestatud juba osades maailma riikides sellised reeglid, mille abil saaks ka ilma teiste riikide loata teises riigis asuvast serverist tõendeid koguda. Kuid ka sellisel juhul on siiski vaja teha mingil hetkel teise riigiga koostööd. Näiteks ei oleks Peter Yuryevich Levashovi kinnipidamine Hispaanias ilmselt aset leidnud, kui koostööd ei oleks teinud ka hispaanlased.

Digitaalsed tõendid erinevad klassikalistest tõenditest. Digitaalsete tõendite kogumine, talletamine ja kohtus esitamine erineb teiste tõendite samasisulisest menetlemisest oluliselt.

Nii nagu õiguspraktika on näidanud, siis digitaalse tõendi usaldusväärsust on kohtus raskem tõendada selle iseloomust tulenevalt. Materjal on sageli tehniline ja uurija, prokurör ja ka kohus vajab sellest aru saamiseks vahel eksperdi, asjatundja või eriteadmistega menetleja abi.

Probleemid seoses digitaalse tõendi usaldusväärsusega jäävad üldjuhul juba kriminaalasja kohtuliku uurimise staadiumisse. Probleemid saavad alguse juba varem - rahvusvahelise koostöö instrumendid, mis võimaldavad digitaalsete tõendite seadustatud viisil saamist on samad, kui füüsiliste tõenditega seoses ja see on probleem. Üheks võimaluseks, kuidas saada andmeid, mis asuvad teises riigis on rahvusvaheline koostöö eelkõige õigusabitaotluste

tegemise näol. Teiseks võimaluseks on ise teise riigi territooriumil talletatud infole ligi pääsemine. Kolmas võimalus on otse teenusepakkujate poole pöörduda, kuid see on keeruline, kuna teenusepakkujad on kohustatud olema diskreetsed ja kaitsma nende valduses olevat.

Eraldi on käesolevas töös peatutud pilveandmetöötlusel. Pilveandmetöötlus on kaasaegse maailma igapäevaosa, tehnoloogia, mis üha enam ületab rahvuste vahelisi piire.

Üha enam on tavapärane see, et andmed on erinevate teenusepakkujate valduses, erinevates asukohtades, erinevates jurisdiktsioonides laiali. Selline andmete hajasus on tingitud pilveteenuse pakkujate organisatsioonilisest ülesehitusest, kus peakorter on ühes riigis, kuid organisatsiooni harud on erinevates riikides. Pilveandmetega seoses põrkuvad menetleja ja teenuseosutaja huvid. Menetlusasutuse poole pealt on oluline vajalikud andmed kätte saada ja teatud juhtudel on see ka võimalik, kui seade on näiteks avatud ja isik annab nõusoleku andmete vaatlemiseks. Kuid isikul on ka õigus privaatsusele. Lisaks tuleb mängu ka veel usaldus teenusepakkuja vastu – ei ole ju välistatud, et teatud juhtudel võib teenusepakkuja väljastada tema valduses olevad andmed õiguskaitseorganile isiku loata.

Igal iseseisval riigil on õigus omariiklusele, õigus vastu võtta põhiseadus, ise määrata oma riigikord, riigiorganite struktuur ja majandussüsteem ning ise juhtida ja korraldada kogu riigi- ja ühiskonnaelu. Seesugune õigus on aga piiratud rahvusvaheliste kokkulepetega, millega riigid ühinevad. Seejuures on selliseid kokkuleppeid vastu võetud ka menetlusõiguse valdkonnas. Nii nagu käesolevas töös on välja toodud, on riigid piiriülest andmete saamist käsitlevate probleemide lahendamisel läinud aga eri teed. Suurriikidest on näiteks USA , Belgia ja Portugal võtnud vastu korrad, mis annab neile õiguse, mille kohaselt on kohtutele teatud jutudel võimalus väljastada läbiotsimis ja vaatlusordereid juhtudel, kui arvuti füüsiline asukoht on teadmata. On riike, kes suhtuvad liberaalselt andmete otsimisele teise riigi serveritest (nt Portugal) ja on riike, kus seda valdkonda ei ole üldse seaduses reguleeritud, v.a üldklausliga, et kriminaalmenetlust võib toimetada oma riigi territooriumil.

Käesolevas töös on esitatud seisukoht, et arusaamade lahususel ja usaldamatusel on otsene mõju riikide rahvuslikule julgeolekule. Ei saa välistada et teoorias võib selline tõlgenduste erinevus kaasa tuua ühel hetkel mõne rahulolematu riigi reaktsiooni teise riigi vastu, mis võib väljenduda kas siis leebemal juhul koostöö tegemise lõpetamises või halvimal juhul ka jõu kasutamises.

Käesoleval ajal kokku lepitud rahvusvahelise koostöö instrumendid ei ole enam kaasaega sobivad. Maailmal on vaja kiiremaid lahendusi. Lahendused peavad olema sellised, mida

aktsepteeriks nii erasektor kui ka avalik sektor ja mis austaks ka inimeste põhiõiguseid ja andmekaitsereegleid.

Tõsta on vaja õigusabitaotluste menetlemise kiirust ja teiseks on vaja tõsta usaldust avaliku sektori ja erasektori organisatsioonide vahel. Ilmselt saab esimese probleemi lahendada sellega, et kehtestada näiteks riikide vahelise kokkuleppega tähtajad õigusabitaotluste vastamisele. Teiseks probleemi lahendusena võiks kaaluda seda, et koos erasektoriga töötatakse välja teatud reeglid, milliste alusel tehtavatele päringutele on erasektoril kohustus vastata. Ehk oleks kasu sellest, et erasektorilt andmete mittesaamisel saadetakse vastavasisuline teade asjasse puutuva riigi õiguskaitseorganile, kes saab mingites ajalistes raamides kohustada erasektori organisatsiooni andmeid avaldama.

Peagi ootavad Eestis kehtivat kriminaalmenetluse seadustikku muudatused.

Käesoleva aasta 9.veebruaril esitas Justiitsministeerium arvamuse avaldamiseks kriminaalmenetlusseadustiku revisjoni väljatöötamiskavatsuse (edaspidi VTK). Väljatöötamiskavatsuse eesmärgiks on süsteemne KrMS analüüs kohtueelse menetluse perspektiivist.

Erinevad osapooled on avaldanud arvamust selles osas, kas kehtestada või mitte kehtestada erikorda seoses digitaalsete tõenditega ning käesoleval ajal kaldub kaalukeel siiski eriregulatsiooni kehtestamise poole.

See on vajalik, et tagada ühtne praktika digitaalsete tõendite kasutamisel. Täpsema regulatsiooni vajadust on kinnitanud nii õiguskantsler, justiitsministeerium, Riigikohus.

Milline see erikord olema saab, seda näitavad edasised arengud õigusloomes.

Käesolevas töö kirjutamise käigus sai kinnitust püstitatud hüpotees, et digitaalsed tõendid ja nende erinevus klassikalistest tõenditest on selline, mis vajab eriregilatsiooni. Digitaalsete tõendite leidmine, kasutatavus ja säilitamine, digitaalsete tõendite lubatavus, olulisemad küberkriminalistika omapärad, kohtumenetlus seoses digitaalsete tõenditega on oskused, mille omandamine on kaasaja kriminaalmenetluse lahutamatu osa.

РЕЗЮМЕ

Тема настоящей магистерской работы: «Особенности использования цифровых доказательств».

В настоящей работе выведены некоторые особенности поведения в киберпространстве, в том числе то, что цифровые доказательства и связанное с их местоположением и сбором, характеризуется международным масштабом. Кибернетическое пространство по своему существу таково, что его очень трудно разграничить. Пространственное действие полномочий производства по уголовным делам часто сталкивается с проблемой, когда лицо, ведущее производство должно задать себе вопрос, находятся ли данные, в которых он нуждается, на территории этого государства, соблюдая закон которого, он в настоящий момент ведет уголовное производство или в уголовном производстве присутствует международный элемент, и он должен смотреть в сторону инструментов международного сотрудничества. Расследование кибер-атак по большей части невозможно без международного сотрудничества. Хотя внутри государства уже в некоторых странах установлены правила, с помощью которых можно без разрешения других стран собирать доказательства, находящиеся на серверах других государств. Однако и в этом случае следует в какой-то момент сотрудничать с другим государством. Например, задержание в Испании Петра Юрьевича Левашова не состоялось бы, если испанцы не сотрудничали бы.

Цифровые доказательства отличаются от обычных классических доказательств. Сбор цифровых доказательств, их сохранение и представление в суде существенно отличается от производства других подобных доказательств.

Как показывает правовая практика, достоверность цифрового доказательства сложнее доказать в суде по причине его характера. Часто материал является техническим и следователь, прокурор, а также суд для его понимания нуждаются в помощи эксперта, знатока или специализированного следователя.

Проблемы, связанные с достоверностью цифрового доказательства, остаются как правило на стадии судебного разбирательства. Однако проблемы возникают раньше – инструменты международного сотрудничества, которые позволяют получение цифровых доказательств законным способом такие же, как и в связи с физическими доказательствами, а это уже и есть проблема.

Одной из возможностей для получения данных, которые находятся в другой стране, является международное сотрудничество, прежде всего в виде ходатайства о правовой помощи. Второй возможностью является личный доступ к хранимой в другой стране информации. Третьей возможностью является прямое обращение к представителю услуги, однако это сложно, поскольку представители услуг должны быть тактичными и защищать имеющееся у них во владении.

Отдельно в данной работе рассматривается обработка данных в облаке. Обработка данных в облаке является ежедневной частью современного мира, это технология, которая все больше преодолевает межнациональные границы.

Все больше становится обыденным то, что данные находятся во владении различных представителей услуг и в различных местах и в различных юрисдикциях. Такая разбросанность данных обусловлена с организационным построением представителей облачной услуги, когда главная контора находится в одном государстве, а ветви организации в других странах. В связи с данными в облаке сталкиваются интересы лица, ведущего производство и лица, оказывающего услуги. Для учреждения, ведущего производство, важно получить необходимые данные и в некоторых случаях, это возможно, если, например, устройство открыто и лицо дает соглашение на просмотр данных. Однако у лица есть право на приватность. В добавок в игру вступает и доверие в отношении представителя услуги – не исключено, что в некоторых случаях представитель услуги может выдать правоохранительным органам, имеющиеся у него во владении данные, без разрешения лица.

У каждого независимого государства есть право на независимость, право принимать конституцию, самому назначать свой государственный строй, структуру государственных органов и экономическую систему, а также руководить и организовать жизнь общественную и всего государства. Подобное право, однако ограничено международными соглашениями, которыми страны объединяются. При этом подобные соглашения приняты и в области производственного права. Например, в данной работе, приведено, как государства при решении проблемы с получением данных за пределами границы, идут разным путем. Из больших государств, например, США, Бельгия и Португалия приняли порядок, который дает им право, на основании которого у судов в некоторых случаях есть возможность выдавать ордеры на обыск и осмотр в тех случаях, когда физическое местонахождение компьютера неизвестно. Есть страны, которые относятся либерально к поискам данных из серверов других стран (и есть страны, в

которых данная область вообще не урегулирована законом, за исключением общей оговорки, что уголовное производство можно вести на территории своего государства.

В данной работе выдвинуто мнение, что разделение мнении и недоверие имеет прямое влияние на международную безопасность стран. Нельзя исключать того, что в теории различность в интерпретации может в один момент повлечь за собой недовольную реакцию государства по отношению к другому государству, которое может в мягком случае выразиться в прекращении сотрудничества, а в худшем случае в применении силы.

В настоящее время инструменты оговоренного международного сотрудничества не идут в ногу со временем. Миру нужны быстрые решения. Решения должны быть такими, чтобы их принял как частный сектор, так и госсектор и которые уважали бы основные права граждан и правила защиты данных.

Следует ускорить производство по ходатайствам о правовой помощи, во-вторых, следует повысить доверие между организациями частного и госсектора. Очевидно, первую проблему можно решить тем, чтобы например установить соглашением, между государствами срок на ответ по ходатайству о правовой помощи. Вторым решением проблемы, можно рассмотреть то, чтобы совместно с частным сектором разработать определённые правила, на основании которых у частного сектора появится обязанность отвечать на подобные запросы. Иными словами, была бы польза от того, чтобы в случае неполучения данных от частного сектора, можно было бы отослать соответствующее сообщение связанному с делом государственному правоохранительному органу, который смог бы в какие-то временные рамки обязать организацию частного сектора огласить данные.

В скором времени ожидаются поправки к действующему в Эстонии уголовно-процессуальному кодексу.

9 февраля настоящего года министерство Юстиции предоставила точку зрения по поводу намерения разработки ревизии уголовно-процессуального кодекса. Целью плана разработки является системный анализ уголовно-процессуального кодекса исходя из перспективы досудебного производства.

Разные стороны высказали мнение по той части, устанавливать или нет особый порядок для уголовное производство дел связанных с цифровыми доказательствами и в настоящее время весы склоняются в сторону установления специальной регуляции.

Это необходимо для того, чтобы обеспечить единую практику при использовании цифровых доказательств. Необходимость точной регуляции утвердили канцлер права, министерство юстиции, Государственный суд.

Каким должно стать это особое положение, покажет дальнейшее развитие создания права.

В ходе анализа данной работы получило подтверждение выдвинутая гипотеза, что цифровые доказательства и их отличие от классических доказательств таково, что они нуждаются в специальной регуляции. Знания, такие как поиск цифровых доказательств, их используемость и сохранность, допустимость цифровых доказательств, особенные специфики кибер-криминалистики, связанное с цифровыми доказательствами судебное производство, являются неотъемлемой частью современного уголовного производства.

Проблемы возникают из практики, соглашения заключаются на уровне государств. Внутригосударственные и суды над государствами решают споры, однако в спорах не всегда выявляется правда. Не задавая вопросов, не получишь ответов. Очевидно, можно читать еще много судебных решений, в которых приводятся аргументы, связанные с особенностями цифровых доказательств. 7 раз отмерь, 1 отрежь. Именно так, по мнению автора данной работы, следует поступить при введении новой внутригосударственной регуляции уголовно-процессуального кодекса. При этом следует учитывать, как лучшие международные практики, так и то, какие проблемы возникают при применении внутригосударственного права.

Kasutatud kirjandus

Kirjandus

1. C.Velasco,A-M.Osula,J.Hörnle. Global Views on Internet Jurisdiction and Trans-Border Access. Volume 24 of the series Law, Governance and Technology Series, lk 465-476
2. Case Study (2016) 24 (4) International Journal of Law and Information
3. E.Laurits. Mõned probleemid arvutisüsteemi läbiotsimisel. Kohtute aastaraamat 2016
4. Electronic CSI, A Guide for First Responders, 2nd edition, National Institute of Justice, April 2008
5. J.Coleman, S.Shapiro, K.Himma. The Oxford Handbook of Jurisprudence and philosophy of law. Oxford Handbooks, 2004.
6. J.Riekkinen. Digital Evidence and Electronic Signature Law Review. 13 (2016).
7. L.Selinšek. Electronic evidence in the Slovene criminal procedure act. Digital Evidence and Electronic Signature Law Review, Vol 7 - http://sas-space.sas.ac.uk/5586/1/1927-2717-1-SM.pdf
8. Law & Security Review 719 Technology 343
9. Osula A-M, 'Remote Search and Seizure in Domestic Criminal Procedure: Estonian
10. Osula A-M, Transborder Access and Territorial Sovereignty (2015) 31 Computer
11. R.Narits. Ühest tänapäevasest põhiseaduse mõttest arusaamise viisist. Juridica X 1999. lk 466-472
12. S.Mason.International electronic evidence. British Institute of International and Comparative Law, 2008.
13. Up in the Cloud: Finding Common Ground in Providing for Law Enforcement Access to Data Held by Cloud Computing Service Providers, 1417

Normatiivmaterjalid

14. Arvutikuritegevusvastane konventsioon - RT II 2003, 9, 32
15. Data Retention and Investigatory Powers Act 2014 https://www.gov.uk/government/collections/data-retention-and-investigatory-powers-act-2014
16. Eesti Vabariigi ja Poola Vabariigi vaheline leping õigusabi osutamise ja õigussuhete kohta tsiviil-, töö- ning kriminaalasjades - RT II 1999, 4, 22 -

17. Eesti Vabariigi ja Ukraina leping õigusabi ja õigussuhete kohta tsiviil- ning kriminaalasjades - RT II 1995, 13, 63
18. Eesti Vabariigi ja Vene Föderatsiooni leping õigusabi ja õigussuhete kohta tsiviil-, perekonna- ja kriminaalasjades - RT II 1993, 16, 27
19. Eesti Vabariigi, Leedu Vabariigi ja Läti Vabariigi õigusabi ja õigussuhete leping - RT II 1993, 6, 5
20. Inimõiguste ja põhivabaduste kaitse konventsioon – RT II 2010, 14, 54
21. Elektroonilise side seadus - RT I, 17.05.2016, 2 -
22. Euroopa Liidu Põhiõiguste harta – Euroopa Liidu Teataja 2012/C 326/02
23. Euroopa Parlamendi ja Nõukogu direktiiv 2006/24/EÜ,15. märts 2006 ELT L 105, 13.04.2006, lk 54–63
24. Kriminaalasjades vastastikuse abistamise Euroopa konventsioon - RT II 1997, 7, 36 –
25. Kriminaalmenetluse seadustik - RT I, 31.12.2016, 16
26. Kriminaalmenetluse ülevõtmise Euroopa konventsioon- RT II 1997, 8, 37 -
27. Põhiseadus - RT I, 15.05.2015,
28. Rahapesu ning kriminaaltulu avastamise, arestimise ja konfiskeerimise konventsioon - RT II 2000, 7, 41
29. Zakon o kaznenom postupku 2009 – neslužbeni procišceni tekst - www.legislationline.org/.../action/.../id/.../Croatia_Criminal_proc_code_am2009_en.p

Kohtupraktika

Euroopa Liidu kohtute lahendid

30. EIKo 03.09.2015 Servulo ja Associados – Sociedade de Advogados, RL vs. Portugal
31. EIKo 14.03.2013 Bernh Larsen Holding AS jt vs. Norra
32. EKo .08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, Digital Rights Ireland Ltd
33. EKo. 21. detsember 2016, liidetud kohtuasjad C-203/15 ja C-698/15 Tele2 Sverige AB

Riigikohtu lahendid

34. RKKKm 3-1-1-112-16, 23.02.2017

35. RKKKm nr 3-1-1-57-12, 16.05.2012
36. RKKKo 3-1-1-5-09, 26.03.2009
37. RKKo , 3-1-1-89-12, 18.02.2013
38. RKKo, 3-1-1-46-10, 18. 06. 2010
39. RKKo, 3-1-1-55-14, 4.12. 2014
40. RKKo, 3-1-1-82 – 16, 07.11.2016

Muud kohtulahendid

41. Harju Maakohtu otsus nr 1-14-3221, 03.05.2014
42. Tallinna Ringkonnakohtu kriminaalkolleegium, 1-15-509, 15.04. 2016
43. Tartu MK Tartu kohtumaja otsus - 1-06-14599, 14.11.2006
44. Viru Maakohus, Narva kohtumaja kohtuotsus nr 1-12-12478, 28.oktoobril 2015

Muud allikad

45. Apple Inc. Report on Government Information Requests January 1 - June 30, 2016 – leitav veebis : https://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf
46. Council of Europe. Chart of signatures and ratifications of Treaty 185. Status as of 17/04/2017 - https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=N1Folg06
47. Cybercrime Convention Committee (T-CY) . Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the T-CY Final report of the T-CY Cloud Evidence Group, 16 September 2016 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e
48. Department of Justice. Digital evidence and forensics - https://www.nij.gov/topics/forensics/evidence/digital/Pages/welcome.aspx
49. DigitalTrends. Apple vs. the FBI: A complete timeline of the war over tech encryption. 03.04.2016 – leitav veebis - http://www.digitaltrends.com/mobile/apple-encryption-court-order-news/

50. Eesti küberkurjategija Vladimir Tšaštin mõisteti USA-s seitsmeks aataks vangi - http://www.delfi.ee/news/paevauudised/krimi/eesti-kuberkurjategija-vladimir-tsastsin-moisteti-usa-s-seitsmeks-aastaks-vangi?id=74355403
51. Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012.
52. Euroopa Liidu infokeskus. EL-i aruanne: uimastiturg ja terrorism on omavahel tugevalt seotud – 05.05.2016
53. G.M.Graff. How FBI tood down russias spam king – and his massive botnet. 11.04.2017 - https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/https://www.wired.com/2017/04/fbi-took-russias-spam-king-massive-botnet/
54. Guardian Project. What is Orbot? - https://guardianproject.info/apps/orbot/ http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters
55. J.Tehver. Digitaalsete tõendite kasutamise võimaldamine, mai 2016 - http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf
56. J.Sootak. jt. (koost). Karistusseadustik. Kommenteeritud väljaanne. Tallinn: Juura 2008
57. K.Masing. Riigiprokuratuur alustas küberrünnakute uurimiseks kriminaalasja – Eesti Päevaleht 02.05.2007, leitav veebis - http://epl.delfi.ee/news/eesti/riigiprokuratuur-alustas-kuberrunnakute-uurimiseks-kriminaalasja?id=51085514
58. Kaitsepolitsei aastaraamat 2016
59. K-C.Kruusmaa, M.Kärner. Majanduskuritegude menetluspraktika analüüs. Kriminaalpoliitika analüüs nr 5/2015 – leitav veebis: http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/majanduskuritegude_menetluspraktika_analuus.pdf
60. Kriminaalmenetluse seadustik. Komm vlj. Tallinn: Juura 2012
61. Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seadus 770 SE, seletuskiri - https://www.riigikogu.ee/tegevus/eelnoud/eelnou/d5492f26-424d-42ad-83e4-cce202a5524d
62. Kriminaalmenetluse seadustiku muutmise seaduse eelnõu, http://eelnoud.valitsus.ee/main/mount/docList/aca7e3cf-d349-4a40-a700-bbdb2b5a115c#qGL4zV3Q

63. Kutsestandard, kohtukriminalistikaekspert, tase 7 – leitav veebist http://www.innove.ee/UserFiles/Kutseharidus/Malle/kohtukriminalistikaekspert-tase-7.3.pdf
64. Küberjulgeoleku strateegia 2014 – 2017 - https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf
65. Küberrünnakud Eesti vastu - http://www.vm.ee/sites/default/files/content-editors/web-static/115/cyber_attacks.pdf
66. Microsoft Secure staff blog - The Budapest Convention on Cybercrime – 15th Anniversary , 16-17.november 2017 - https://blogs.microsoft.com/microsoftsecure/2016/11/17/the-budapest-convention-on-cybercrime-15th-anniversary/
67. P.Hõbemägi. Interneti pimedam pool – Eesti Ekspress 05.12.2009
68. Prokuratuuri aastaraamat 2016 – kättesaadav veebis: http://www.prokuratuur.ee/et/prokuratuuri-aastaraamat-2016/rahvusvaheline-koostoo
69. Prokuratuuri IT- tõendite menetlemise soovituslik juhend, 24.05.2016.
70. Rule 41 Coalition Letter - https://noglobalwarrants.org/assets/Rule41CoalitionLetter.pdf
71. S. De Schrijver, T.Daenens. The Yahoo! Case: The End of International Legal Assistance In Criminal Matters – Who`sWhoLegal, september 2013, leitav veebis - http://whoswholegal.com/news/features/article/30840/the-yahoo-case-end-international-legal-assistance-criminal-matters
72. T-CY (Cybercrime Convention Committee) 2016.a raport - https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e
73. Tor Project - https://www.torproject.org/
74. United Nations Office on Drugs and Crime, „World drug report 2016“ https://www.unodc.org/doc/wdr2016/WORLD_DRUG_REPORT_2016_web.pdf, XXV
75. Wikipedia. Dennis Radder - https://en.wikipedia.org/wiki/Dennis_Rader
76. Välisministeeriumi teadaanded - RT II 2004, 30 - https://www.riigiteataja.ee/akt/807271https://www.riigiteataja.ee/akt/807271
77. Õiguskantsleri 05.12.2012.a. arvamus kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõule (295 SE) -

http://www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=52727c38-5c97-433d-bc25-eda7af8db244&

78. Kriminaalmenetluse seadustiku muutmise seaduse eelnõu väljatöötamise kavatsus 09.02.2017 - leitav veebis : http://eelnoud.valitsus.ee/main/mount/docList/aca7e3cf-d349-4a40-a700-bbdb2b5a115c#qGL4zV3Q
79. Transborder access to data and jurisdiction: Options for further action by the T-CY (2014), leitav veebis: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Mari Luuk (sünnikuupäev: 06.10.1982)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Digitaalsete tõendite kasutamise erisused“, mille juhendaja on professor Jaan Ginter

1.1. reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace-is lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
1.2. üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace´i kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, 02.05.2017.