TALLINNA TEHNIKAÜLIKOOL

Majandusteaduskond

Õiguse instituut

Harold Kaha

Elektroonilise sõnumi saladuse problemaatika kriminaalmenetluses

Magistritöö

Juhendaja: Eneli Laurits, baccalaureus artium

Kaasjuhendaja: Agnes Kasper, doktorikraad

Tallinn 2017

Deklareerin, et käesolev magistritöö,
mis on minu iseseisva töö tulemus, on
esitatud Tallinna Tehnikaülikooli
magistrikraadi taotlemiseks ja selle
alusel ei ole varem taotletud akadeemilist
kraadi.

Harold Kaha
“ ..... “ ..... 201…
Töö vastab kehtivatele nõuetele

Juhendaja: Eneli Laurits, baccalaureus artium
“ ..... “ ..... 201...

Kaasjuhendaja: Agnes Kasper, doktorikraad
“ ..... “ ..... 201...

Kaitsmisele lubatud “ ..... “ ..... 201...
Õiguse instituudi magistritööde kaitsmiskomisjoni esimees

Sisukord

Lühendid:

m-määrus

o-otsus

RKKK-Riigikohtu kriminaalkolleegium

TlnRnK- Tallinna Ringkonnakohus

EK-Euroopa Kohus

EIK-Euroopa Inimõiguste Kohus

PS- Eesti Vabariigi Põhiseadus

KrMS- Kriminaalmenetlue seadustik

PostiS- Postiseadus

ESS- Elektroonilise side seadus

ProkS- Prokuratuuriseadus

Sissejuhatus

Suhtlemine ja vaba teabevahetus kuuluvad isikuvabaduse alla, mistõttu on õigusriigis viibivatel isikutel põhjus eeldada, et austataks tema suhtluse privaatsust.[1] Enamasti soovivad inimesed soovivad suhelda privaatselt, kartmata, et keegi võiks nende kirjavahetust või kõnesid jälgida. Kuna inimkonna ajaloo jooksul kujunesid välja põhiõigused, ning järjest enam hakati tunnustama isikute eraelu ja privaatsust, tekkis ka kommunikatsiooni kaitseks sõnumisaladuse printsiip. Sõnumisaladuse eesmärk on kaitsta kahe või enama isiku vahel toimuvat kommunikatsiooni, mida edastatakse posti või selleks loodud tehniliste vahendite kaudu.

Sõnumite saladuse õigust võib leida erinevate riikide konstitutsioonidest. Kitsamalt saab sõnumisaladust rahvusvahelise inimõiguste dogmaatika järgi pidada eraelu ja privaatsuse osaks.[2] Sealhulgas kaitseb sõnumisaladust ka Inimõiguste ja põhivabaduste kaitse konventsioon (edaspidi inimõiguste konventsioon), mille arikkel 8 kohaselt on igaühel õigus sellele, et austataks tema era- ja perekonnaelu, kodu ning korrespondentsi saladust.[3]

Ka Eesti Vabariigi Põhiseaduses on põhiõigusena sätestatud sõnumite saladus. Põhiseaduse paragrahvi 43 kohaselt on igaühel õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele.[4] Riigil on õigus sõnumite saladusse sekkuda üksnes kohtu loal, kui see on vajalik kuriteo tõkestamiseks või tõe väljaselgitamiseks kriminaalmenetluses.[5]

Siiski on inimõiguste konventsioonis ja põhiseaduses sätestatud sõnumisaladuse õigus erineva kaitsealaga. Kui inimõiguste konventsioon sätestab sõnumite saladusele üldise kaitse, kaitstes samaaegselt nii edastatavaid kui ka vastuvõetud sõnumeid, siis riigikohtu kriminaalkollegium on tõlgendanud põhiseaduses sätestatud sõnumisaladuse kaitseala kitsendavalt, mis tähendab seda et põhiseadusliku sõnumite saladuse kaitse alla kuuluvad vaid edastamisprotsessis olevad

[1] § 43, p 1. Põhiõigused ja vabadused. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. pohiseadus.ee/ptk-2/pg-43/
[2] Maruste, R. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse.Tallinn, Juura 2004, lk 531
[3] Convention for the Protection of Human Rights
and Fundamental Freedoms. Artikkel 8 www.echr.coe.int/Documents/Convention_ENG.pdf (12.11.2016)
[4] PS RT I, 15.05.2015, 2 §43
[5] *Ibid.*

sõnumid.[6] Sõnumid, mis on adressaadile kohale toimetatud, kuuluvad aga pere-ja eraelu puutumatuse kaitse alla, millesse sekkumine alati kohtu luba ei vaja.[7]

Käesolevas töös uurib autor sõnumisaladuse kaitseala ajalist kitsendamist tänapäevaste kommunikatsioonivahendite valguses. Tänapäeval on suhtlusvahendid ja nende kasutamine võrreldes varasemaga oluliselt muutunud. Tavaposti osakaal on vähenenud, telegrammi kasutamine on valdavalt jäänud minevikku. Suhtlemiseks eelistatakse kasutada tehnoloogiat, mis võimaldab edastada teavet kiirelt ja mugavalt. Igapäevaselt saadetakse erinevaid elektroonilisi sõnumeid, nagu näiteks e-kirjad, sms-id, internetis tehtavad hääl- ja videokõned, kiirsõnmid jne.

Riigikohtu praktikast tulenev sõnumisaladuse kitsendamine võib tänapäeva kommunikatsioonivahendeid arvestades olla problemaatiline. Eriti puudutab see olukordi, kus kriminaalmenetluses soovitakse tutvuda süüdistatava või kahtlustatava elektrooniliste sõnumitega. Võrreldes tavalise kirjapostiga, edastatakse elektroonilisi sõnumeid vaid sekundite jooksul. Õiguskaitseorganitel on peaaegu võimatu elektroonilise sõnumi teeloleku ajal sõnumite saladusse sekkuda. Sõnumitega tutvumine on võimalik vaid siis kui sõnum on adressaadile kohale toimetatud. Sellisel juhul on aga edastatav teave väljaspool põhiseaduses sätestatud sõnumite saladuse kaitseala.

Sõnumite saladuse kitsa ajalise tõlgenduse kohaselt jäävad sõnumisaladuse kaitsealast välja ka sõnumite sideandmed, mis on elektrooniliste sõnumite puhul oluliseks osaks. Antud olukorra teeb problemaatiliseks asjaolu, et Euroopa õigusruumis peetakse elektrooniliste sõnumitega kaasnevaid sideandmeid sõnumite sisu osaks ning seetõttu väärivad sõnumite saladusega samaväärset kaitset.

Lähtudes eeltoodust, tekkis käesoleva töö autoril küsimus, kas üle kahekümne aasta tagasi loodud sõnumite saladuse printsiibi, mis kaitseb vaid sõnumeid nende teeloleku ajal, arvestab piisavalt tänapäevaste kommunikatsioonivahenditega ning on kooskõlas rahvusvaheliselt tunnustaud põhiõigustega ning Euroopa õigusruumi seisukohtadega? Kuigi vähesed Eesti õigusteadlased on antud probleemi üle diskuteerinud, ei ole seda seni tehtud veel teadustöö tasemel. Seetõttu on käesoleval tööl väga oluline väärtus. Töö autor koostas magistritöö

[6] RKKKo 3-1-1-14-14, p 816
[7] *Ibid.*, p 817

eesmärgi saavutamisega hüpoteesi: "Põhiseaduse paragrahvis 43 sätestatud sõnumite saladuse kaitseala on liiga kitsas elektrooniliste sõnumite kaitsmiseks kriminaalmenetluses.“

Käesoleva magistritöö puhul on tegu kvalitatiivse uuringuga. Töös kasutatakse erinevaid õiguse tõlgendamise meetodeid nagu näiteks grammatiline ja teleoloogiline tõlgendamine. Autor on töö koostamisel lähtunud Eesti kui ka välismaa autorite poolt koostatud õigusalastest teaduspublikatsioonidest. Lisaks on autor töö kirjutamisel kasutatud analüüse ja uuringuid, ajakirjanduses avaldatud artikleid, siseriiklike ja rahvusvahelisi õigusakte ning kohtupraktikat.

Autor jagas käesoleva magistritöö kolmeks erinevaks peatükikst. Antud peatükkide pealkirjad on järgnevad: „Sõnumisaladusest üldiselt“, „Sõnumisaladuse kaitse elektrooniliste sõnumite puhul“ ning „Elektrooniliste sõnumite saladusse sekkumine kriminaalmenetluses“.

Esimeses peatükis annab autor ülevaate ja võrldeb sõnumisaladuse printsiipi nii rahvusvahelises kui ka Eesti õigusraamistikus. Autor toob lühidalt välja sõnumite saladuse printsiibi ajaloolise arengu kirjelduse ning uurib milline on antud põhiõiguse isikuline ja esemeline kaitseala, ehk kes ja milliseid kommunikatsioonivahendid on sõnumisaladuse õigusega kaitstud. Muuhulgas otsib autor vastust küsimusele, kas tänapäevased sidevahendid peaksid olema sõnumisaladusega kaitstud.

Töö teises peatükis uurib autor lähemalt elektroonilisi sõnumeid sõnumite saladuse kontekstis. Autor annab hinnangu selle kohta, kas üle 20 aasta tagasi koostatud Eesti Vabariigi Põhiseaduse sõnumisaladuse printsiip arvestab tänapävase kommunikatsioonitehnoloogiaga. Antud peatükis analüüsib autor, kas elektroonilised sõnumid vajavad põhiõiguste seisukohast senisest intensiivsemat kaitset. Kuna elektrooniliste sõnumite osaks on sideandmed, uurib töö autor, kas sideandmed peaksid sarnaselt sõnumite sisuga kuuluma sõnumite saladuse kaitse alla või mitte.

Kolmandas peatükis keskendub autor sellele, kuidas Eesti kriminaalmenetluses sekkutakse elektrooniliste sõnumite saladusse ning millised on kehtiva regulatsiooni kitsaskohad. Autor annab ülevaade elektrooniliste sõnumite kogumisega seotud toimingutest kriminaalmenetluses. Selle saavutamiseks on autor eraldi uurinud jälitustegevust, arvutite ja pilveteenuste läbiotsimist ja elektrooniliste sõnumite sideandmete kogumist. Autor analüüsib, kas kehtiv menetluskord on piisavalt selge ning arvestab piisavas ulatuses isikute põhiõigustega. Kuna elektroonilised sõnumid on digitaalsel kujul, uurib autor töö ka digitaalsete tõendite kogumise ja käitlemise

regulatsiooni Eestis kriminaalmenetluses ning otsib kehtiva regulatsiooni kitsaskohtadele lahendusi.

1. Sõnumite saladusest üldiselt

Kommunikatsioon on vahend inimestevaheliseks teabe vahetamiseks. Peale silmast silma suhtlemise on peamiseks kommunikatsioonivahendiks sõnumid. Sõnumid võivad olla nii füüsilisel kujul, ehk reeglina kirja pandud paberi peale või elektroonilisel kujul, nagu näiteks telefonivestlused ja elektroonilised kirjavahetused.

Üldiselt loetaks sõnumiks kirjavahetuse või sidevahendi abil edastatud informatsiooni, mis sisaldab teavet isiku mõtete, arvamuste, veendumuste, kavatsuste või millegi muu kohta, mida isik soovib teise isikuga jagada.[8] Kuna sõnumite edastamine toimub enamasti kolmanda osapoole vahendusel, kelleks võib olla näiteks sideettevõtja või postiteenuse osutaja, tuleneb sellest ka sõnumite saladuse kaitsmise vajadus.[9]

1.1. Sõnumisaladus kui põhiõigus

Inimeste soov suhelda salajaselt ja privaatselt on peaaegu sama vana kui kirjutamine ning seega ulatub salajase suhtlemise ajalugu inimkonna tsivilisatsiooni algusesse.[10] Nii suhtlemine, kui ka vaba teabevahetus on isikuvabadust iseloomustavad elemendid ning sõnumisaladust võib rahvusvaheliselt kujunenud inim- ja põhiõiguste kohaselt pidada privaatsuse ja eraelu osaks.[11]

Inimõigusete hulgas kuulub korrespondentsiõigus nii-öelda esimese generatsiooni õiguste kategooria hulka, sest tänapäevased kommunikatsioonivahendid on olulised muutnud nii kommunikatsiooniviise, aga ka inimeste vahelist suhtluskultuuri.[12] Üldiselt võib sõnumite saladuse õigugs tänapäeval vaadelda kui vana õigust tänapäevases maailmas.[13]

Inimõiguste konventsiooni artikli 8 punktis 1 on sätestatud, et igaühel õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust.[14] Hoolimata sellest, et inimõiguste konventsioonis kasutatakse mõistet „korrespondents“, on Euroopa Inimõiguste

[8] §156, 2 Karistusseadustiku kommenteeritud väljaanne, Tallinn, Juura 2015, lk 446
[9] §118 p 2.1. Tõendamine. Kriminaalmenetlusseadustiku kommenteeritud väljaanne. Juura, Tallinn 2012
[10] Ekert, A. A Very Brief History Of Secrecy www.arturekert.org/crypto/history.pdf (9.12.2016) lk 1.
[11] Maruste (2004) *supra* nota 2, lk 531.
[12] Karovska-Andonovska, B. The Right To Secrecy Of Communications-Situations And Challenges. Journal of Process Management – New Tecehnologies, International 2014, 2 (4), lk 114
[13] *Ibid.*
[14] Inimõiguste ja põhivabaduste kaitse konventsioon RT II 2000, 11, 57

Kohus sellele mõistele andnud sõnumi tähenduse, kuna kaitse alla kuulub sõnumi saatja poolt edastatav teave.[15] Konventsiooni uuendatud eesti keelses tõlkeversioonis sõna „korrespondents“ asendatud sõnaga „sõnum“.[16] Kuigi õigusaktis tuleks omakeelse sõna kasutamist eelistada, tuleb siiski tõdeda, et „sõnum“ ja „korrespondents“ ei ole siiski samatähenduslikud mõisted.[17] Korrespondents tähendab eelkõige kirjavahetust, aga sõnum tähistab teavet.

Tänapäeval tunnustavad sõnumisaladust põhiõigusena enamus Euroopa riikide kontsitutsioonidest. Ka Euroopa Liidu siseselt on sõnumisaladuse, kui põhiõiguse, olulisust toonitatud, sest Euroopa konstitutsioonaalne traditsioon kaitseb igaühe kommunikatsiooni, aga samad põhimõtted ja kaitemeetmed kehtivad ka riigisisese ning rahvusvahelise kommunikatsiooni kohta.[18] Just seetõttu sätestab Euroopa Liidu põhiõiguste harta (edaspidi põhiõiguste harta) artikkel 7 igaühe õiguse tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladuse austamiseks.[19] Muuhulgas lepiti 2009. aastal jõustunud Lissaboni lepinguga kokku, et põhiõiguste harta on õiguslikult siduv ning kinnitab sealhulgas ka inimõiguste konventsiooniga tagatud põhiõigusi.[20]

Lisaks põhiõiguste hartale ja inimõiguste konventsioonile on sõnumisaladust tunnustatud ka teistes rahvusvahelistes dokumentides. Näiteks keelab lapse õiguste konventsioon artikkel 16 meelevaldse ja ebaseadusliku sekkumise laste kirjavahetusse.[21] Ka Ühinenud Rahvaste Organisatsiooni poolt loodud Kodaniku- ja poliitiliste õiguste rahvusvahelise pakti artiklis 17 on sätestatud õigus korrespondentsi kaitsele.[22]

Enamasti soovivad inimesed, et kommunikatsioon, sõltumata selle vahendist või viisist, oleks privaatne. Sõnumite privaatsuse eesmärgiks on vältida telefonide või vestluste pealtkuulamist ning sekkumist kirjavahetusse, sealhulgas ka elektroonilisse kirjavahetusse.[23] Seega tähendab

[15] Lõhmus, U. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. Juridica, 2008 (7), lk 464
[16] Inimõiguste ja põhivabaduste kaitse konventsioon RT II 2010, 14, 54
[17] Lõhmus, U. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. Juridica 2016 (3), lk 177
[18] Irion, K. Privacy and Security: international communications Surveillance. Communications of the ACM, 2009, 52 (2), lk 27
[19] Artikkel 17. Euroopa Liidu Põiõiguste harta (2012/C 326/02)
[20] Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut sõlmitud Lissabonis 13. detsembril 2007 ELT C,17.12.2007 ,lk 249
[21] Lapse õiguste konventsioon RT II 1996, 16, 56
[22] Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt RT II 1994, 10, 11
[23] Finn, R.L., Wright, D., Friedewald, M. European Data Protection: Coming of Age. Springer Netherlands 2013, lk 8

sõnumisaladuse printsiip seda, et sõnumite sisu peab olema kättesaadav vaid nendele isikutele, kes sõnumi saatmisest ja vastuvõtmisest osa võtavad.[24] Sõnumi saatjal ainuõigus otsustada, kellele ja mis tingimustel see edastada ning samas on ka teabe adressaadil ainupädevus otsustada, kuidas ta talle edastatud teabega edasi käitub.[25]

Kuna isikutel on soov ja vajadus tagada vahendajate kaudu edastatavate sõnumite puutumatus ning samas ka tahe rajada teatud usaldus sõnumeid vahendava teenuseosutaja suhtes, on aegade jooksul välja kujunenud sõnumite saladuse printsiip.[26] Eriti Euroopa riikide seas on sõnumisaladust peetud võõrandamatuks õiguseks väga pikka aega.[27] Näiteks Saksamaal võeti juba 18. sajandil vastu regulatsioon, mis nägi ette, et postiasutused peavad austama kirjade ja dokumentide konfidentsiaalsust.[28] Kirjade ja telegraafide kasutamine tõi kaasa võimaluse sekkuda postiteenustesse ning telefoniside leiutamine võimaldas õiguskaitseorganitel hakata kodanike suhtlust pealt kuulama. Kuigi telegraaf leiutati 1870ndatel aastatel ning telefon 1890ndatel, hakkas politsei esmakordselt nende kommunikatsioonivahendite sidet pealt kuulama ja jälgima juba 19. sajandi lõpus.[29]

1.2. Sõnumisaladus Eesti Vabariigi Põhiseaduses

Eesti Vabariigi Põhiseaduse üheks olulisemaks eesmärgiks on tagada isikule puutumatu eraeluline sfäär, mis peab teatud osas jääma riikliku sekkumise eest lõplikult ja täiel määral kaitstuks.[30] Üldiselt võib olla seisukohal, et põhiseaduses on perekonna- ja muu eraelu puutumatusel väga oluline väärtus, sest seda kaitstakse mitmetes paragrahvides.

Põhiseaduse paragrahv 26 annab igaühele õigus perekonna- ja eraelu puutumatusele ning riigiasutustel, kohalikel omavalitsustel ja nende ametiisikutel on keelatud perekonna- ega eraellu sekkuda muidu, kui seaduses sätestatud juhtudel ja korras, kui see on tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija

[24] Maruste, *supra* nota 2, lk 532
[25] TlnRnK 1-14-3029
[26] §43, p4. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. http://www.pohiseadus.ee/ptk-2/ (23.11.2016)
[27] Karovska-Andonovska, *supra* nota 12, lk 114
[28] *Ibid.*
[29] Diffie, W., Landau, S. Communications surveillance: Privacy and security at risk. ACM Queue 2008, 7(8), lk 44
[30] TlnRnK 1-07-15425

tabamiseks.[31] Eraelu puutumatuse kaitse alla kuulub ka privaatsusõigus, mille eesmärgiks on kaitsta kodu puutumatust, isikuandmeid ja sõnumisaladust.[32]

Sõnumisaladus, mis on ühtlasi üheks tugevamini kaitsud põhiõiguseks, on põhiseaduses sätestatud eraldi paragrahvina perekonna- ja eraelu puutumatusest[33] Põhiseadusese paragrahvi 43 annab igaühele õiguse tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele ning lubab erandeid teha üksnes kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks seadusega sätestatud juhtudel ja korras. [34]

Põhiseaduses sätestatud sõnumisaladuse kaitse printsiip tähendab sisult seda, et riik ei tohi saadetavaid sõnumeid kustutada, moonutada ega tsenseerida ning samuti on riigil kohustus mitte takistada sõnumite jõudmist saatja valitud sihtkohta.[35] Lisaks põhiseadusele on ka teistes siseriiklikes õigusaktides toonitatud sõnumisaladuse olulisust ja sellesse sekkumise lubatavust. Näiteks on postiseaduse paragrahv 33 lõikes 1 sätestatud, et postisaladus on postisaadetise sisu ja konkreetse isiku postikäivet puudutav informatsioon. Sama paragrahvi lõike 2 kohaselt peavad nii postiteenuse osutaja, tema töötaja ja postiteenuse osutajat juhtima õigustatud isik hoidma postisaladust nii teenuse osutamise ajal kui ka pärast seda.[36] Ka Karistusseadustiku paragrahv 156 näeb ette, et sõnumisaladuse rikkumine on kriminaalkorras karistatav.[37]

Ajaloolises kontekstis vaadatuna on Eesti konstitutiooniõiguses peetud sõnumisaladust põhiõigusena juba esimesest, 1920 aasta, põhiseadusest saadik.[38] Tollal sätestas põhiseadus, et Eestis on kindlustatud sõnumite ja kirjade saladus, mis antakse edasi posti, telegraafi ja telefoni või mõnel muul üldtarvitataval teel ning erandeid võisid kohtuvõimud teha vaid seadustes ettenähtud juhtumistel.[39] Järgmise, 1938. aasta, põhiseadusega lisati sõnumisaladuse printsiipi

[31] PS RT I, 15.05.2015, 2
[32]Inimõiguste instituut. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad Kättesaadav: www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-I-osa-Saateks1.pdf lk1 (03.12.2016)
[33] Lõhmus, U. Põhiõigused kriminaalmenetluses. Teine, täiendatud ja ümbertöötatud väljaanne. Tallinn, Juura 2014, lk 325
[34] PS. RT I, 15.05.2015, 2
[35] Annus, T. Riigiõigus. Juura, Tallinn 2006, lk 310
[36] PostiS RT I, 12.07.2014, 107 §33
[37] Karistusseadustik RT I, 31.12.2016, 14 §156
[38] Lõhmus (2008), *supra nota* 15, lk 462
[39] PS. RT, 09.08.1920, 113/114, 243

täiendus, mis lubas sõnumisaladusse sekkuda juhul, kui seda oli vaja teha kuritegeuvse vastu võitlemiseks seaduses sätestatud alustel ja korras.[40]

Ka Nõukogude Sotsialistlike Vabariikide Liidu ajal kehtisid seadused, mis kaitsesid sõnumite saladust ning üldiselt vastasid nõukogudeaegsed sõnumisaladust kaitsvad õigusnormid rahvusvaheliste inimõiguste printsiipidele.[41] Näiteks 1977. aasta konstitutsiooni kohaselt olid nii eralu, kirjavahetus kui ka telefonikõned ja telegraafid seadustega kaitstud.[42] Siiski on küsitav, kuivõrd nõukogude võim pidas lugu sõnumisaladust kaitsvatest normidest. Kuna tol ajal kontrolliti ja vaigistati inimeste nõukogudevastast meelsust, siis on ka loogiline, miks tänapäeva Eesti ühiskonnas võib veel esineda pealtkuulamisfoobiat.[43]

1.2.1. Sõnumisaladuse ja eraelu puutumatuse eristamine Eesti põhiseaduses

Kui inimõiguste ja põhivabaduste kaitse konventsioonis on eraelu puutumatus ja sõnumite saladuse õigus määratletud ühes paragrahvis, siis põhiseaduses on need õigused eraldatud erinevatesse paragrahvidesse.[44] Sarnaselt Eestile leiab eraelu puutumatusele ja sõnumisaladusele eraldi paragrahvi pühendamist ka teiste riikide põhiseadustest. Näiteks sätestab ka Rumeenia põhiseadus eraldi artikli telefonisuhtluse, kirjade, telegrammide ja teiste kommunikatsiooniviiside saladuse kaitsele.[45]

Nende kahe põhiõiguse olulisemaks erinevuseks on see, et erinevalt eraelu puutumatusesse sekkumisest nõuab sõnumisaladusse sekkumine alati kohtu luba. Kuigi tingimused nende kahe põhiõiguse riiveks on erinevad, kaasneb ka sõnumisaladusse sekkumisega kahtlemata eraelupuutumatuse riive.[46]

Kuid käsitleb põhiseadus antud põhiõiguseid erinevas paragrahvis? Tartu Ülikooli külalisprofessori Uno Lõhmuse arvates võib vastus peituda nii ajaloolites kui ka sisulistes

[40] Lõhmus (2008), *supra* nota 15, lk 462

[41] Saueauk, M. „Salajane kontroll". Sõnumisaladuse rikkumisest Nõukogude Liidus ja Eesti NSV-s" Tuna Ajalookultuuri ajakiri 2014 (2), lk 52

[42] *Ibid.*

[43] Strandberg, M., Rahumägi, J. Rahumägi ja Strandberg: kas ja miks meid pealt kuulatakse? Postimees, 2007. arvamus.postimees.ee/1726661/rahumagi-ja-strandberg-kas-ja-miks-meid-pealt-kuulatakse (12.12.2016)

[44] Marute, R. *supra* nota 2, lk531

[45] Constitution of Romania 429/2003

[46] Lõhmus (2014) *supra* nota 33, lk 324

põhjustes.[47] Üheks eristamise põhjuseks võib olla asjaolu, et kuigi 1920. ja 1938. aasta põhiseadused sätestasid õiguse sõnumisaladusele, puudus tolleaegsetes põhiseadustes paragrahv era- ja perekonnelu kaitse kohta.[48] Teiseks põhjenduseks võib pidada seda, et Eesti taasiseseivumisel olid põhiseaduse autoritel veel meeles nõukogude julgeolekuorganite poolt kasutatavad meetodid kodanike jälgimisel.[49] Tollal jälgis Nõukogude Liidu Julgeoleku Komitee, ehk KGB, isikuid väga tähelepanelikult, kuid tuleb samas tõdeda, et ka demokraatlikus ühiskonnas teostatakse isikute vahelise suhtluse jälgimist.[50] Kuigi demokraatlikus ühiskonnas õigustab suhtluse jälgimist nii riiklik julgeolek kui ka kuritegevusega võitlemine, on inimeste jälgimise ja info kogumise eesmärgid ja tagatised oluliselt erinevad totalitaarsetest ja autoritaarsetest ühiskondadest.[51]

Seetõttu tuleb tõdeda, et Eesti Vabariigi põhiseaduses on sõnumite saladuse kaitseala piiride kindlaksmääramine ja eristamine teiste privaatsuse elementide kaitsealast palju olulisem, kui selliste põhiseaduste ja rahvusvaheliste inimõigusaktide puhul, kus era- ja perekonnaelu, kodu puutumatusel ning sõnumite saladusel ühesugused piirangute alused.[52] Selline põhiseaduslik kästitlus annab märksa rangema kaitse kui rahvusvahelised aktid, sest sõnumisaladuse riivamiseks lubavaid aluseid on vähem.[53] Kahjks võib selline põhiseaduse normitehniline lahendus muuta keerukaks võrdlev- õigusliku tõlgenadamisemeetodi kasutamise ning seetõttu on vajalik sõnumisaladuse ja teiste privaatsusõiguste kaitsealade selge piiritlemine.[54]

Ei saa ka märkimata jätta, et kui põhiseadus annab igaühele sõnumite saladuse õiguse, siis Inimõiguste konventsiooni ning põhiõiguste harta järgi on igaühel õigus sõnumite saladuse austamisele. Endine Euroopa Inimõiguste Kohtu kohtunik Rait Maruste on arvamusel, et õigus sõnumite saladusele ja õigus saladuse austamisele on erineva mahu kui ka tugevusastmega ning tõdeb, et kuigi põhiseaduse kohaselt on sõnumitele saladusel väga tugev formaalne kaitse, siis konventsiooni ja harta sõnastus arvestab tegeliku elu rohkem.[55]

[47] Lõhmus (2008), *supra* nota 15, lk 464
[48] *Ibid.*
[49] Lõhmus (2014) *supra* nota 33, lk 327
[50] Lõhmus (2008) *supra* nota 15, lk 462
[51] *Ibid.*
[52] *Ibid.*
[53] Maruste. *supra* nota 2, lk 532
[54] Lõhmus (2014) *supra nota* 33, lk 32
[55] Maruste. *supra* nota 2, lk 533

1.2 Sõnumisaladuse isikuline ja esemeline kaitseala

Eesti Vabariigi põhiseaduse paragrahvi 9 kohaselt kuuluvad põhiseadusest tulenevad õigused, vabadused ja kohustused nii Eesti kodanikele, Eestis viibivatele välisriigi kodanikele kui ka kodakondsuseta isikutele.[56] Sama paragrahvi lõike 2 järgi laienevad juriidilistele isikutele niivõrd, kui see on kooskõlas juriidiliste isikute üldiste eesmärkide ja selliste õiguste, vabaduste ja kohustuste olemusega.[57] Kuigi ka sõnumisaladuse isikulise kaitseala kindlaksmääramine ei tekita praktikas probleeme, on esemelise kaitseala määramine aga hoopis keerulisem.[58]

Põhiseaduse paragrahvi 43 kohaselt on sõnumisaladuse esemelises kaitsealas posti, telegraafi, telefoni või muul üldkasutataval teel edastatavad sõnumid. Hoolimata sellest, et põhiseaduse vastuvõtmise ajaks olid sidevahendite arengus toimunud olulised muutused, näiteks hakati kasutama internetti ja GSM sidet, sälitati põhiseaduses arhailine sõnastus, alustades loetelu posti ja telegraafiga.[59]

Sõnumite saladuse kaitseala ulatuse kindlaksmääramisel on üheks olulisemaks küsimuseks sõnumi mõiste maht.[60] Eesti õiguskirjanduses on täheldatud, et sõnumite saladuse kaitse alla kuuluvad sõnumid, mida edastatakse posti vahendusel, aga sinna alla kuuluvad ka erinevate tehniliste sidevahendite abil edastatud teave.[61] Kuna tänapäeval on infotehnoloogias väga kiire areng, tuleb sõnumisaladuse esemelise kaitseala määratlemisele läheneda evolutsiooniliselt ning kasutada avarat teleoloogilist tõlgendamist.[62] Seetõttu kuulub sõnumite saladuse kaitse alla eelkõige informatsioon, mida isik soovib enda poolt valitud suhtluskaaslasega jagada, sõltumata sellest, milline on sõnumite edastamise viis või vahend.[63]

Nii inimõiguste konventsioon kui ka põhiõiguste harta ei sätesta seda, millised sõnumite edastamise viisid on kaitstud ning seetõttu on oluline roll kohtupraktikal. Näiteks on Euroopa Inimõiguste kohus leidnud lahendis *Michaud v. Prantsusmaa*, et korrespondentsi õigus hõlmab

[56] PS RT I, 15.05.2015, 2 §43
[57] *Ibid.*
[58] Lõhmus (2008), *supra* nota 15, lk 465
[59] Lõhmus (2014),*supra* nota 33, lk 326
[60] *Ibid.*, lk 330
[61] §43, p2. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. http://www.pohiseadus.ee/ptk-2/
[62] Maruste. *supra* nota 2, lk 532
[63] *Ibid.*

kõiki erasuhtlusi, sõltumata sellest, milline on selle sisu või vorm.[64] Kaasuses *Klass and others v. Federal Republic of Germany,* leidis inimõiguste kohus, et telefoni pealtkuulamine riivab isiku õigust era-, perekonnaelu ja korrespondentsi austamisele.[65]

Õiguskirjanduses on täheldatud, et praktikas puuduvad põhjused, miks sõnumisaladuse kaitseala ei peaks arvestama tehnoloogia arenguga.[66] Uno Lõhmus pooldab inimõiguste konventsiooni lähenemist, mille kohaselt on lahtiseks jäetud sõnumite edastamise viiside loetelu, märkides, et sellise lähenemise puhul laieneb põhiõiguse kaitseala automaatselt koos uue sõnumi edastamise vahendi tekkega [67]

Käesoleva töö autor on seisukohal, et ka põhiseaduse sõnastusest võib välja lugeda, et sõnumite saladus kaitseb kõiki sõnumiedastamise viise, sest esemelise kaitseala loetelu hulka kuuluvad ka muud üldkasutaval teel edastatavad sõnumid. Üldkasutatavaks sideteenuseks loetakse teenust, mida sideettevõte pakub sideteenuse turul üldistel alustel kõigile isikutele.[68] Põhiseadusliku sõnastuse kohaselt võib välja lugeda, et sõnumite saladuse printiibist jääb välja selline teave, mida ei edastata üldkasutataval teel, nagu näiteks sõnumite edastamine läbi kinnise elektroonilise sidesüsteemi või raadiside.[69] Uno Lõhmus on siinkohal tõdenud: „Raske on leida õigustust, miks üldkasutataval teel edastatud sõnumid väärivad suuremat kaitset kui muul viisil edastatud sõnumid“.[70]

Ka käesoleva töö autori arvates peaks sõnumite saladus kaitsma kõiki sõnumeid, hoolimata sellest, kas sõnumi edastamise vahend on üldkasutatav või mitte. Autor ei leia põhjendusi, miks põhiseaduse autorid on sellise piirangu seadnud, sest sõnumeid on võimalik pealt vaadata või kuulata ka kinnises elektroonilise side süsteemis. Kahjuks ei ole siiani riigikohus antud küsimuse üle diskuteerinud. Autori peab võimalikuks, et Riigikohus võib tulevikus siiski leida, et sõnumite saladuse kaitset väärivad ka sõnumid, mida üldkasutataval teel ei edastata.

[64] EIKo 12323/11 *Michaud v. France,* p 90
[65]EIKo 06.11.1978, 5029/71 *Klass and others v. Federal Republic of Germany,* p 41
[66] Harris, D. J., O'Boyle, M., Bates, E., Buckley, C. Harris. O'Boyle & Warbrick: Law of the European convention on human rights. Oxford University Press, USA 2014, lk 320
[67] Lõhmus, (2008), *supra* nota 15, lk 464
[68] §43, p3. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. http://www.pohiseadus.ee/ptk-2/
[69] Lõhmus (2014) *supra* nota 33, lk 329
[70] *Ibid.*

Käesoleva peatüki kokkuvõtteks võib väita, et kuigi sõnumite saladusele on põhiseaduses pühendatud eraldi paragrahv, mida käsitletakse era- ja perekonnaelu puutumatusest eraldi, ei tekita sõnumisaladuse isikuline ja esemeline kaitseala määratlemine erilisi probleeme.

Järgmises peatükis uurib autor lähemalt elektrooniliste sõnumite saladuse kaitset. Sealhulgas analüüsib autor, kas kehtivas Eesti Vabariigi Põhiseadus sätestatud sõnumisaladuse kaitse printsiip arvestab tänapäevaste kommunikatsioonivahenditega. Lisaks uurib, kas sõnumite edastamisega kaasnevad sideandmed peaks sarnaselt sõnumite sisuga väärima kaitset sõnumisaladuse õiguses.

2. Sõnumite saladuse kaitse elektrooniliste sõnumite puhul

Kuigi endiselt kasutatakse ka postisidet sõnumite vahetamiseks, siis tänapäeval toimub sõnumite vahetamine enamasti läbi elektroonilise side võrgu. Nagu eelnevast peatükist nähtus, peaks sõnumite saladuse kaitsealla igasugune sõnum, sõltumata sellest millist vahendit selle edastamiseks kasutatakse. Käesolevas peatükis analüüsib autor, kas põhiseaduses sätestatud sõnumite saladuse kaitse kehtib ka elektroonilisete sõnumite puhul.

2.1. Sõnumisaladuse ajaline kaitseala

Põhiseaduse paragrahvi 43 kohaselt on igaühel õigus tema poolt või temale posti, telegraafi, telefoni või muul üldkasutataval teel edastatavate sõnumite saladusele.[71] Põhiseaduse paragrahv 43 lubab grammatilise tõlgenduse abil selgitada, et sõnumite saladuse õigusega on kaitstud vaid selline teabevahetus, mis on edastamise protsessis, sest paragrahvis kasutatakse määratlust „edastatavad sõnumid".

Uno Lõhmus leiab seevastu, et paragrahvi 43 sõnastust on võimalik grammatiliselt tõlgendada ka teisiti, tuues välja, et edastavate sõnumite saladus võib ka osutada viisile, kuidas sõnum edastatakse, mitte seda, et sõnumisaladuse kaitse kuulub ainult edastamisprotsessis olevatele sõnumitele.[72] Käesoleva töö autori arvates võisid põhiseaduse autorid kasutada edastavate sõnumite mõistet ka just seetõttu, et normitehnilistel kaalutlustel sooviti vältida mõistete korrespondents või kommunikatsiooni kasutamist ning asendada see mõistega edastatavad sõnumid, mis viitab üldisele kommunikatsiooniprotsessile. Võrreldes sõnumitega on mõisted korrespondents ja kommunikatstioon palju laiema tähendusega, tähistades teate edastamist kui ka vastuvõtmist.[73]

Kui vaadata põhiseaduse inglise keelset tõlget, siis nähtub, et seal ei ole sõnumisaladuse kaitseala piiratud nii, et see kohalduks vaid üksnes edastavatele sõnumitele.[74] Kuigi põhiseaduse

[71] PS RT I, 15.05.2015, 2 §43
[72] Lõhmus(2016), supra nota17, lk180
[73] Lõhmus (2014),supra nota 33, lk 332
[74] The Constitution of the Republic of Estonia Translation published: 21.05.2015 www.riigiteataja.ee/en/eli/521052015001/consolide (12.12.2016)

tõlgete erinevus väärib märkimist, ei saa neid grammatilise tõlgenduse kohaselt hinnata, sest seaduste tõlked ei oma Eestis iseseisvat õigusjõudu.[75]

Euoopa inimõiguste konventsioon sätestab aga üldise sõnumite saladuse õiguse ning kaitseb sõnumit tervikuna. Euroopa Inimõiguste Kohus on leidnud, et arvuti läbiotsimine ja sellel asuvatest dokumentidest koopiate tegemine riivab õigust korrespondentsi saladusele.[76] Seega võib järeldada, et inimõiguste kohtu praktika kohaselt korrespondentsi mõiste alla korraga nii sõnumid, mis on andmekandjale talletatud, aga ka sõnumid, mis on parasjagu saatmisprotsessis.

Euroopa Liidu Põhiõiguste harta eestikeelsest tõlkest nähtub, et sarnaselt põhiseadusega, kaitseb ka harta artikkel 7 vaid edastavaid sõnumeid. Siinkohal väärib märkimist, et harta inglise keelse versiooni kohaselt on aga kaitstud kommunikatsioon.[77] 2014. aastal ilmunud harta kommenaarides ollakse seisukohal, sõnumite saladuse kaitse ei sõltu sellest, kas sõnum on edastamiseprotesssis või mitte.[78]

Käesoleva töö autor on arvamusel, et kuigi põhiõiguste harta tõlkijad lähtusid tõlke loomisel põhiseadusest, on siiski erinev sõnastus taunimist väärt, sest sellega muudetakse oluliselt artiklist 7 tulenevat eesmärki. Ometi sätestab põhiõiguste harta artikkel 53, et harta sätteid ei või tõlgendada neid inimõigusi või põhivabadusi kitsendavate või kahjustavatena[79]

Näiteks on ka Euroopa Inimõiguste kohus pidanud problemaatiliseks konventsiooni keeleliste tõlgete erinevusi.[80] Kohtuajas *Niemietz v. Saksamaa* analüüsis kohus olukorda, kus konventsiooni prantsuskeelne versioon kasutas mõistet „domitsiil", aga ingliskeelses versioonis kasutati mõistena „kodu".[81] Kohus jõudis seisukohale, et prantsuskeelne tõlge annab konventsioonile märksa laiema kaitse.[82]

---

[75] Tuulik, M-E., Sellest aastast on kõik Eesti seadused inglise keeles kättesaadavad. Justiitsministeerium. www.just.ee/et/uudised/sellest-aastast-koik-eesti-seadused-inglise-keeles-kattesaadavad (16.02.2017)

[76] EIKo 14.03.2013, 24117/08, Bernh Larsen Holding AS and others vs Norway, p 105

[77] Charter Of Fundamental Rights Of The European Union (2012/C 326/02)

[78] Peers,S., Hervey, T.K., Kenner, J., Ward, A. The EU Charter of Fundamental Rights: A Commentary. Hart Publishing, 2014, lk 161

[79] Euroopa Liidu Põiõiguste harta (2012/C 326/02)

[80] EIKo *13710/88* Niemietz v. Germany ,p30

[81] *Ibid.*

[82] *Ibid.*

2.2 Ajalise kaitseala problemaatika elektrooniliste sõnumite puhul

Kuigi postiside on endiselt kasutusel sõnumite edastamisel, siis tänapäeval toimub sõnumite vahetamine peamiselt elektroonilist sidet kasutades.[83] Elektroonilist sidet vahetatakse reegilina andmesidevõrku, mobiiltelefonivõrku või kaabellevivõrku kasutades.[84] Peamisteks elektroonilise side eelisteks võrreldes tavalise postisidega on selle kiirus ning võimalus vahetada teavet äärmiselt kaugete vahemaade tagant. Näiteks saab e-kirja abil edastada teavet adressadile teavet ühest maailma otsast teise vaid sekundite jooksul

Ringkonnakohus on kohtupraktikas leidnud, et teenusepakkuja serverisse salvestatud elektroonilised kirjad on võrdsustatavad teel olevate sõnumitega, sest nende sõnumite kaitse ei sõltu kirja adressaadist.[85] Eelnimetatud kohtuasja kassatsioonikaebust analüüsides jõudis aga riigikohus vastupidisele järeldusele, märkides, et e-kirjade puhul jõuab sõnum isiku mõjusfääri alles siis, kui tal on olnud võimalus sellega tutvuda ja otsustada selle üle, kas sõnum salvestada või kustutada.[86] Lisaks on varasemas riigikohtupraktikas tõdetud, et kui arvutisse salvestatud e-kirjade juurdepääsuks oleks vaja kohtu luba, muudaks see sõnumisaladuse kaitseala liiga avaraks.[87]

Riigikohtu kriminaalkolleegium on sõnumisaladuse printsiibi laienemist vaid edastavatele sõnumitele defineerinud põhiseaduse range kaitsena ning leidnud, et e-kirja ja sms-sõnumile põhiseaduslik kaitseala kohaldub vaid selle ärasaatmisest kuni saajani jõudmiseni.[88] Lisaks on kolleegium märkinud, et telefonikõned on sõnumisaladuse kaitsealas vaid toimumise hetkel ning postisaadetised on kaitstud vaid postiasutusele üleandmisest kuni adressaadini toimetamiseni.[89]

Riigikohus on sõnumisaladuse ajalist kaitseala põhjendanud sellega, et kui sõnum on saatja valdusest väljunud, kuid pole veel adressaadini jõudnud, on sõnum isiku mõjusfäärit väljas ning seetõttu puudub tal võimalus seda kolmandate isikute eest kaitsta.[90] Riigikohtu arutluse järgi on

[83] §43, p2. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. http://www.pohiseadus.ee/ptk-2/ (12.12.2016)
[84] *Ibid.*
[85] TlnRnK 1-14-3029/6, p27.3
[86] RKKKo 3-1-1-93-15, p 98
[87] RKKKo 3-1-1-14-14 p 816
[88] *Ibid.*, p 817
[89] *Ibid.*
[90] RKKKo 3-1-1-14-14 p 460

kommunikatsiooniprotsessi läbinud teave võrdsustatav teabega, mis ei ole kunagi kommunikatsiooniprotsessis olnudki. [91]

Uno Lõhmus ei ole eelnevalt välja tooduid riigikohtu arutlusega nõus, sest tema arvates on sõnumisaladuse ajalise kaitseala piiritlemine tänapäeva kommunikatsioonitehnoloogiat ja selle võimalusi arvestades vale.[92] Ta tõdeb, et olukorras, kus elektronkiri muutub saaja e-posti kontol kättesaadavaks, ei ole tegemist veel automaatselt sõnumi edastamise lõppemisega, sest e-kirja postkasti jõudmine ei tähenda veel seda, et see on jõudnud adressaadini[93] Seda eelkõige just põhjusel, et kuna e-kirja lugemiseks on isikul vaja parooli, siis võib ajavahemik sõnumiga tuvumiseks olla märksa pikem sellest ajavahemikust, mis kulub sõnumi jõudmisele saaja elektroonilisse postkasti.[94]

Siinkohal toob käesoleva töö autor võrdluse tavalise kirjaümbrikuga, mille saatja ise või postitöötaja paneb adressaadi postkasti. Kui ümbrikuga saadetud kiri või postkaart jõuab adressaadini märksa pikema ajavahemiku jooksul kui e-kiri, siis võib ka kirjaga tutvumiseks kuluv aeg olla pikk. Sagel võib see tutvumisperiood olla elektroonilisest kirjast pikem, sest tänapäeva infotehnoloogia võimaldab elektroonilist postkasti peaaegu kõikjal endaga kaasas kanda, seda näiteks sülearvuti või nutitelefoni abil.

Töö autor peab võimalikuks, et riigikohtu kriminaalkollegium on põhiseaduse sõnumisaladuse kaitseala ajalise piirangut kehtestanud liiga kergekäeliselt, sest on lähtutud ainult grammatilisest tõlgendamisest, mis tänapäeva tehnoloogiaajastu kommunikatsioonivõimalustega ei arvesta. Autor nõustub Raul Naritsaga, kelle arvates ei saa ükski grammatiline tõlgendus ei saa lõplikult kehtida igas järgnevas ajas ja ruumis, sest õiguse iga konkreetne aeg ja ruum võivad koosneda einevatest väärtusmastaapidest.[95]

Sarnaselt Uno Lõhmusega on riigikohtunik Eerik Kergandberg riigikohtu lahendis tehtud eriavamuses seisukohal, et kohtu tõlgendus sõnumisaladuse ajaline kaitse kohta, kitsendab põhjendamatult põhiõiguse toimeala.[96] Kergandberg tõdeb, et tänapäeva ühiskonnas ei tohiks

[91] RKKKo 3-1-1-93-15 p 102
[92] Lõhmus 2016, *supra* nota 17, lk 181
[93] *Ibid,*
[94] *Ibid.*
[95] Narits, L. Õiguse entsüklopeedia. Tallinn, Juura 2007 lk 152
[96] Kegandberg, E. Eriarvamus Riigikohtu kriminaalkolleegiumi 20. novembri 2015. aasta otsuse 3-1-1-93-15 juurde. www.riigikohus.ee/?id=11&tekst=222579511 (04.11.2016)

põhiõigusi tähtsuse järgi reastada ning maailma virtuaalsuse piiramatu kasvuga ei saa sõnumisaladuse olulisuse kahanemist pidada ratsionaalseks.[97]

Autor nõustub täielikult eelnevalt välja toodud Lõhmuse ja Kergandbergi seisukohtadega. Autor leiab, et ka inimõiguste konventsiooni ja inimõiguste kohtu lahendite eiramist võib pidada problemaatiliseks. Ometigi on Riigikohus tõdenud, et Euroopa inimõiguste ja põhivabaduste kaitse konventsioon riigikogu poolt ratifitseeritud, see on Eesti õiguskorra lahutamatu osa ning sellel on prioriteet Eesti seaduste ja muude aktide suhtes.[98]

Lisaks e-kirjadele kasutatakse teabe vahetamiseks erinevaid suhtlusvõrgustikke. Näiteks võimaldab Facebooki portaal palju erinevat liiki teenuseid, sealhulgas e-kirjade saatmist, reaalajas vestlusi ja fotode jagamist. Siiski võimaldavad suhtlusvõrgustikud võrreldes tavaliste e-kirjadega suhelda reeglina palju kiiremini, ning seetõttu sarnanevad sellised teenused telefonikõnedega. Kui õiguskaitseorganid kuulavad pealt telefonikõnesid, kohaldub sellele põhiseaduslik sõnumisaladuse printsiip. Kui reaalajas vaadatakse pealt suhtlusvõrgustikus toimuvat vestlust, on tegu eraelupuutumatusega, sest ajal, mil sõnum on muutunud teisele osapoolele arvutiekraanil nähtavaks, on riigikohtu seisukoha kohaselt kommunikatsiooniprotsess siusliselt lõppenud. Töö autori arvates on selline olukord väga problemaatiline ning toetab käesoleva töö hüpoteesi.

Käesoleva töö autor tõdeb, et elektrooniliste sõnumite sõnumisaladuse kaitseala määratlemine võiks olla seotud faktiga, kas kirja adressaat on kirja avanud või mitte. Näiteks Ameerika Ühendriikides võib menetleja ainult läbiotsimisorderi alusel saada ligipääsu veel avamata e-kirjale, mis on pilvteenuses olnud maksimaalselt 180 päeva ning kirjad mis on rohkem kui 180 päeva vanad, enam orderit ei nõua.[99] Käesoleva töö autor sellist lähenemist täielikult ei poolda, sest põhiõigustesse sekkumise seisukohalt ei ole oluliselt erinev olukord, kas avamata e-kiri on pilvteenuses olnud 180 või 181 päeva. Autor on siiski arvamusel, et kuigi kirjaga tutvumise fakt peaks sõnumi saladuse kaitseala määratlemisega olema seotud, võib praktikas selle tuvastamine olla äärmiselt keeruline.

[97] *Ibid.*

[98] RKKKo 3-1-3-13-03, p31

[99] Kattan, I. R. Cloudy privacy protections: Why the Stored Communications Act fails to protect the privacy of communications stored in the cloud. Vanderbilt Journal of Entertainment & Technology Law *2010 (13),* lk 631

Kuid miks peaksid kommunikatsiooniprotsessis olevad sõnumid saama tugevama kaitse saatmisele kuuluvatest või kohale jõudnud sõnumitest? Siiani ei ole esitatud piisavaid põhjendusi, kuigi mõlemal juhul on tõenäoline, et riivatakse inimväärikusega seotud sõnumite saladust.[100] Samuti ei esine põhjuseid, miks peaks kandma põhiseaduse sisustamisel eirama hartat ja seda selgitavat Euroopa Kohtu kui ka inimõuguste kohtu praktikat.[101]

Professor Orin Kerr leiab, et kui varasemalt võis lugeda kõige olulisemaks just sõnumite teeloleku aega, siis tänapäeval nõuavad suuremat tähelepanu juba talletatud/salvestatud sõnumid, põhjusel, et andmete hoiustamine on odav ning seetõttu maailmas ka laialdaselt levinud.[102] Tema arvates on vahetegu reaalajas jälgimise ja juba talletud andmete ligipääsemise puhul kadumas, sest talletatud andmed võimaldavad anda palju rohkem informatsiooni ning seda palju pikema ajavahemiku kohta.[103]

Töö autor on seisukohal, et kuna e-kirjade teenust pakkuvad teenuseosutajad annavad kasutajale võimaluse mitmete gigabaitide ulatuses salvestada erinevat teavet, võib juba talletatud sõnumite puhul olla riive märksa suurem kui reaalajas pealtvaatamise- või kuulamise korral, sest informatsiooni on reeglina märksa rohkem.

Kokkuvõtvalt leiab autor, et võrreldes tavapostiga on elektrooniline kommunikatsiooniprotsess väga lühike ning kuna see ei sõltu postiteenustest võib seetõttu sõnumisaladuse rikkumist elektroonilise sõnumi teelolekuajal pidada äärmiselt ebatõenäoliseks. Seetõttu on küsitav, kas põhiseaduses sätestatud sõnumite saladuse ajaline piirang ühtib tänapävase kommunikatsioonivahenditega eripäradega.[104] Autori hinnangul ei ole eelpool viidatud riigikohtu kriminaalkollegiumi lähenemine sõnumisaladuse ajalisele kaitseala kohta piisavalt põhjendatud ning on vatuolus inimõigusalaste dokumentidega. Siinkohal väärib märkimist, et põhiseaduse paragrahv 123 sätestab, et olukorras, kus Eesti seadused või muud aktid on vastuolus Riigikogu poolt ratifitseeritud välislepingutega, tuleb kohaldada välislepingu sätteid.[105]

[100] Lõhmus(2014), *supra* nota 33, lk 344 (Põhõigused kriminaalmenetluses)
[101] Kalmo, H. Põhiseaduse põkkumine Euroopa Liidu põhiõiguste hartaga. Juridica 2016 (3), lk 163
[102] Kerr, Orin S., The Next Generation Communications Privacy Act 162 University of Pennsylvania Law Review 2014 (162) lk 376
[103] *Ibid.*, lk 393
[104] Lõhmus (2016), *supra* nota 17 ,lk181
[105] PS RT I, 15.05.2015, 2 §123

Kahjuks on sõnumisaladuse ajalise kaitseala ulatuse määratlemine olnud siiani vaid riigikohtu kriminaalkolleegiumi arutelus.[106] Uno Lõhmuse arvates tuleks antud probleem pigem vaagida riigikohtu üldkogus, põhjusel, et neil on põhiseaduse tõlgendamisel märksa suurem legitiimsus võrreldes kriminaalkollegiumiga.[107]

2.3. Elektroonilise sõnumite sideandmed kui osa sõnumisaladusest?

Elektrooniline kommunikatsioon ei koosne ainult teabevahetuse sisut, vaid sellega kaasnevad ka metaandmed, mis sisaldavad informatsiooni sõnumite koostamise, ülekandmise ja edastamise kohta.[108] Kuna elektrooniline suhtlus toimub reeglina läbi sideettevõtjate teenuse ning suhtlusega kaasneb informatsioon, siis jääb ka sideettevõtjatele suhtlusest teave. Näiteks saame telefonioperaatoritelt küsida informatsiooni enda tehtud kõnede kohta ning e-posti teenust pakkuvad ettevõtted salvestavad side toimimiseks teatud andmeid. U. Lõhmus on märkinud, et selliseid suhtlusega kaasnevaid fakte võib tähistada terminiga „sõnumi liikumise andmed".[109] Kirjanduses võib kohata ka mõisteid metaandmed ning sideandmed.

Sõnumite saladuse kaitseala ulatuse kindlaksmääramisel on üheks kesksemaks küsimuseks sõnumite mõiste maht.[110] Kui sõnumi sisu suhtes ollakse konsensusel, et sisu kuulub sõnumite saladuse esemelise kaitse alla, siis sõnumi liikumise andmete puhul on see hoopis keerulisem.[111]

Euroopas õigusruumis ollakse seisukohal, et elektrooniliste sidevahendite ajastul ei ole põhjendatud põhiõiguste kaitse seisukohast suhtluse sisu ja metaandmete eristamine.[112] Euroopa Inimõiguste kohus on sealjuures tõdenud, et sõnumitega kaasnevad sideanandmed kuuluvad korrespondentsi saladuse alla, sest näiteks leidis kohus kaasuses *Malone v. Ühendkuningriigid*, et telekommunikatsiooni alla kuuluvad sellised andmed, mis sisaldavad helistaja ja vastuvõtja telefoninumbrit ning annavad informatsiooni kõne aja ja kestuse kohta.[113] Ka kohstuasjas

[106] Lõhmus (2016), *supra* nota 17 ,lk 176
[107] *Ibid.*
[108] Andmekaitse inspektsioon. Metaandmed ja privaatsus Juhis organisatsioonidele1 ja kodukasutajale seaduse rakendamisel. www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Metaandmed.pdf (18.02.2017)lk 4
[109] Lõhmus (2014),*supra* nota 33, lk lk 330
[110] *Ibid.*
[111] *Ibid.*
[112] Lõhmus (2016), *supra* nota 17, lk 179
[113]EIKo 26.04.1985, 8691/79 Malone v. The United Kingdom

Copland v. Ühendkuningriik rõhutas inimõiguste kohus eelnevat põhimõtet, lisades, et sõnumisaladuse alla kuuluvad ka andmed, mis kajastavad e-kirjade adressaate ja saatmisaegu.[114]

Erinevalt Euroopas valitsevat arvamusest, ollakse Ameerika Ühendriikides seisukohal, et sõnumite sideandmed ei vääri sõnumite saladuse kaitse alla kuulumist.[115] Näiteks leidis ülemkohus kohtuasjas *Smith v. Maryland*, et olukorras, kus telefonioperaator näeb helistaja poolt valitud telefoninumbreid, ei ole tegemist siiski sõnumite sisusse sekkumisega.[116] Kohtuasjas *Ameerika Ühendriigid v. Forrester* leidis kohus, et kui riik saab ligipääsu ainult andmetele nagu IP aadressid, e-posti konto kontaktid või külastatud veebilehed, ei ole sellistest andmetest võimalik välja lugeda sõnumi sisu.[117] Kohus märkis, et selliste andmete põhjal on võimalik vaid ainult oletada, millest osapooled võisid suhelda ning tõdes, et sellisel juhul on tegu vaid spekulatsioonidega.[118] Hoolimata sellest, et sõnumite sideandmed ei kuulu Ameerika Ühendriikuide konstitutsioonilise kaitse alla, on nendele andmetele ligipääsuks vajalik siiski kohtu luba.[119]

Eesti Vabariigi Põhiseaduse paragrahvis 43 puudub igasugune viide selle kohta, kas sõnumite edastamise informatsioon kuulub sõnumite saladuse kaitse alla. Põhiseaduse grammatilist tõlgendust kasutades võib jõuda järeldusele, et sõnumi liikumise andmed ei ole sõnumisaladuse printsiibiga kaetud ning seega tuleb sideandmeid käsitleda sõnumite sisust erinevalt. Kuigi sarnaselt Eestiga puudub ka Saksamaa Põhiseaduses märge selle kohta, et sõnumite sideandmed kuuluks sõnumisaladuse kaitse alla, on Saksamaa konstitutsioonikohus leidnud, et sideandmeid tuleb siiski lugeda kommunikatsiooni osaks.[120] Ka Prantsusmaa põhiseadus ei võrdsusta sideandmeid sõnumite saladusega, on need siiski kaitsud seaduse tasemel samaväärselt sõnumi sisuga.[121]

[114] EIKo 03.04.2007, 62617/00. Copland v. The United Kingdom, p44
[115] Lõhmus (2008), *supra* nota 15, lk 468
[116] United States Supreme Court Smith V. Maryland, (1979) No. 78-5374
[117] United States Court of Appeals,Ninth Circuit. United States v. Forrester. 05-50410, 05-50493.
[118] *Ibid.*
[119] Kerr, O. Applying the Fourth Amendment to the Internet: A General Approach. 62 Stanford Law Review 2010, 62 (4), lk 1033
[120] Kaiser, A. B. German Federal Constitutional Court: German Data Retention Provisions Unconstitutional in Their Present Form. European Constitutional Law Review 2010 6(03) lk 512
[121] Lõhmus (2014),*supra* nota 33, lk 332

Ka Eesti õiguskirjanduses on leitud, et sõnumite sideandmed ei kuulu põhiseadusliku sõnumisaladuse kaitse alla, sest sideandmetest ei nähtu sõnumi sisu.[122] Näiteks on õiguskantsler Ülle Madise tõdenud, et kuna sideandmete kogumine ja töötlemine riivab eelkõige õigust perekonna- ja eraelupuutumatusele ning sideandmeid ei saa lugeda sõnumite sisu osaks ning seetõttu ei kaasne sellega ka riivet sõnumite saladusele. Õiguskantsleri arvates ei saa sideandmete kogumisega kaasnevate riivete intensiivsust üldiselt võrrelda sõnumi saladuse õigusesse sekkuvate jälitustoimingute intensiivsusega.[123]

Uno Lõhmus on õiguskantsleriga vastupidisel arvamusel ning tunneb muret selle üle, et suhtluse metaandmete kogumist ja õiguskaitseorganitele kättesaadavaks tegemist peetakse põhiõiguse vähem intensiivseks riiveks võrreldes sõnumisaladusega.[124] Ta leiab, et selline salajane jälgimine vajab kohtulikku kontrolli, sest see tagaks märksa parema kaitse omavoli eest.[125] Kuna Eesti seadusandja tunnustab vajadust kaitsta rangemini sõnumi sisu kui sõnumi sideandmeid, siis on vägagi tõenäoline, et inimõiguste kohus võib tulevikus leida, et Eesti seadused ei vasta selles osas inimõiguste konventsioonile.[126]

Ka Garri Ginter ja Piret Schasmin on ajakirjas Juridica avaldatud artiklis seisukohal, et Eestis kehtiv elektroonilise side andmete säilitamise regulatsioon on vastuolus Euroopa Liidu õigusega.[127] Sarnaselt Uno Lõhmusega on ka nemad arvamusel, et sõnumisaladuse kitsas tõlgenudus on problemaatiline ning tõdevad, praktikas tuleb arvestada et sõnumisaladuse ja eraelu puutumatuse kaitse laienemisega.[128]

Käesoleva töö autor nõustub, et sideandmete eristamine sõnumite sisust ei ole tänapäva info- ja kommunikatsioonitehnoloogia ajastu puhul ajakohane. Selline eristamise võib eelkõige olla seotud tavaposti kasutamisega, sest kirjaümbrikul on reeglina informatsioon ainult kirja saaja

[122] § 43, p 6. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. pohiseadus.ee/ptk-2/pg-43/

[123] Madise, Ü. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus. www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (03.12.2016) lk 2

[124] Lõhmus(2016), *supra* nota 17 lk 180

[125] *Ibid.*, lk 182

[126] Lõhmus (2014),*supra* nota 33, lk 333

[127] Ginter, G., Schasmin, P. Lahendite Tele2 Sverige ja Digital Rights Ireland mõju sideandmete mugavkasutusele Eestis. Juridica 2017 (1), lk 52

[128] *Ibid*., lk 51

kohta ning see ei anna teavet kirja sisu kohta.[129] Kuna metaandmetel on tänapäeva ühiskonnas väga suur roll, tuleks nende kaitsetaset tugevdada.[130] Seni võib aga kehtivat sideandmete kogumist pidada vastuolevaks sõnumite kaitseala eesmärgiga.[131]

Käesoleva peatüki kokkuvõtteks võib väita, et põhiseaduses sätestatud õigus sõnumite saladusele on oluliste puudustega. Kehtiv põhiseaduslik regulatsioon on tänapäeva kommunikatsioonivahendeid arvestades vananenud ning ei arvesta Euroopa õigusruumis valitsevate seisukohtadega. Eriti oluline on just rõhutada, et lisaks põhiseadusele on ka inimõigsalastel dokumentidel oluline roll. Töö autor leiab, et põhiõiguste tagamiseks tuleks põhiseadusega ette nähtud sõnumite saladuse õigust korrigeerida nii, et antud sõnumisaladuse õiguse alla kuuluksid ka sõnumid, mis on edastamise protsessi läbinud. Samuti peaksid sõnumite saladuse kaitsealla kuuluma ka elektrooniliste sõnumite sideandmed. Autor on arvamusel, et põhiseaduse muutmine on lähitulevikus kahtlemata vajalik.

Järgnevas peatükis vaatleb autor lähemalt, millised kriminaalmenetluslikud võimalused on sõnumisaladusse sekkumiseks. Töös analüüstakse elektrooniliste sõnumite kogumist jälitustegevuse ja läbiotsimise raamistikus ning sealhulgas ka kriminaalmenetluses toimetavat sideandmete kogumist . Kuna elektroonilised sõnumid esinevad digitaalselt kujul, kajastab autor töö viimases osas ka digitaaltõendite regulatsiooni kitsaskohti Eesti kriminaalmenetluses.

[129] Conley, C. Non-Content is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction, 54 Santa Clara Law Review 2014, 54 (4), lk 828

[130] Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf (14.02.2017) lk 27

[131] *Ibid.*

3. Elektrooniliste sõnumite saladusse sekkumine kriminaalmenetluses

Demokraatlikus õigusriigis on keelatud põhjendamata ja vajaduseta koguda andmeid inimeste eraelu ja omavahelise suhtlemise ning selle sisu kohta[132]. Igal inimesel on õigus eeldada oma tegevuse vabadust ja seda, et tema eraelulised kontaktid kuuluvad üksnes talle.[133] Samuti peavad siseriiklikud õigusaktid olema piisavalt selged, et kodanikud mõistaks, millistel eeldustel ja asjaoludel võib avalik võim sekkuda eraelu puutumatusesse ja sõnumite saladusse.[134]

Sõnumisaladuse piiramise vajalikkus on aga rahvusvaheliselt kujunenud välja peamiselt terrorismi ning piiriülestest kuritegudest tuleneva ohuga.[135] Samuti aitab sõnumite pealtvaatamine ja pealtkuulamine ka teiste kuritegude uurimisele kaasa ning seetõttu on ka jälitusasutustel sellise jälgimismeetodi vastu kõrgendatud huvi.[136]

Võrreldes varasemaga on tänapäeva digitaalajastu on kommunikatsioonitehnoloogia andnud rohkelt võimalusi jälitustoiminguteks, pealtkuulamiseks ja andmete kogumiseks.[137] Perioodi 1999-2007 peetakse digitaalse kriminalistika kuldseks ajaks, sest tollal tekkis riikidel üha rohkem võimalusi e-kirjadele ja teistele arvuti abil edastavate sõnumitite ligipääsuks.[138] Tehnoloogia võimaldab isikuid ja nende suhtlust jälgida ja salvestada suurelt kauguselt. Hoolimata sellest, kas politsei kuulab telefonivestlusi pealt, loeb e-kirjavahetust või jälgib sideandmeid, on siiski alati tegu sekkumisega privaatsusõigusesse.

Vaatamata tõsiasjale, et elame infoühiskonnas, kus on rohkelt innovatsiooni nii poliitikas kui ka tehnoloogias, on siiski paljud riigid hetkel tutvumas ja lisamas seadustesse kommunikatsiooni jälgimist puudutavaid sätteid.[139] Sageli on normid väga vanamoelised, sest neid võetakse

[132] Maruste. *supra* nota2, lk 533
[133] *Ibid.*
[134] EIKo 26.04.1985,8691/79 Malone v. The United Kingdom
[135] Marute, R., lk 532
[136] *Ibid.*
[137] Lõhmus (2016), *supra* nota 17, lk 179
[138] Garfinkel, S. L. Digital forensics research: The next 10 years 2007. Digital investigation 2010, 7, lk66
[139] Hosein, G., Palow, G.W Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques, Ohio State Law Journal 2013 (74), lk 1072

peamiselt üle Ameerika Ühendriikide ja Suurbritannia õigusaktidest, mis vajaksid ka teatud määral uuendamist.[140]

Paljudes riikides ei ole kehtivat regulatsiooni ja tavasid ega uuendusi just selles osas, mis puudutab ohtusid ja väljakutseid digitaalse kommunikatsiooni jälgimises.[141] Siiani kasutatakse tavalise kirjavahetuse mõistet arvutite ja digitaalse kommunikatsiooni jälgimiseks, arvestamata sellega, et selliseid kommunikatsioonitehnoloogiaid kasutatakse väga laialdaselt ning neil on tugev mõju üksikisikute õigustele.[142] Kuna riigi poolt läbiviidav elektrooniline jälgimine kujutab endast uut tüüpi sekkumist isikute privaatsusesse, seab see ohtu ka isikute eraelu puutumatuse.[143]

Kui vaadelda jälitusstatistikat Eestis, nähtub, et viimaste aastatega on teabe salajane pealtkuulamine ja –vaatamine liikunud tõusvas joones.[144] Võrreldes eelnevate aastatega on 2015. aastal toimunud arvutiandmetesse sekkumisi üle kahe korra rohkem ning arvutisüsteemi toimimise taistamisi on registeeritud poole rohkem.[145] Sama tendentsi võib leida ka postisaadetiste varjatud läbivaatamise ning varjatult arvutisüsteemi või arvutivõrku sisenemise puhul[146]

Tekib küsimus, kui kaugele võivad riigid ja nende õiguskaitseorganid kriminaaluurimises minna, et isikute suhtlust jälgida. Ühelt poolt kaitseb sihilik kommunikatsiooni jälgimine ühiskonda, sest selles peituv teave võib kaasa aidata kurjategijate tabamisele ja nende süüdimõistmisele. Samas sekkub selline jälgimine aga ka isikute privaatsusesse ning seeläbi ohustab ka teisi põhiõiguseid.

Kriminaalmenetlusõigus on omavahel väga tihedalt seotud konstitutsiooniõigusega, sest kriminaalmenetlus on riikliku tegevuse valdkond, kus kõige rohkem aksepteeritakse erinevaid

---

[140] *Ibid.*

[141] La Rue, F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 2011 www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.(02.01.2017) lk5

[142] *Ibid.*

[143] Fondamentaux, M. D. D. Commentary of the charter of fundamental rights of the european union. http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf (02.01.2017) lk 8

[144] Justiitsministeerium. Aruanne jälitusstatistikast 2015. aastal. Kriminaalpoliitika analüüs nr2/2016 www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/jalitusstatistika_aruanne_2015.pdf (03.01.2017) lk 5

[145] *Ibid.*

[146] *Ibid.*

põhiõiguste riiveid.[147] Euroopa Inimõiguste Kohus on kohtupraktikas mitmel korral toonitanud, et tõendite kogumine peab olema demokraatlikus ühiskonnas vajalik ja eesmärgipärane, aga samas ka kontrollitud ja piiratud ulatusega. Kaasuses Klass ja teised v. Saksamaa, leidis kohus, et tõendite kogumisel tuleb arvestada nende kogumise kestuse, ulatuse ja meetoditega.[148] Põhiõiguste riive peab olema kooskõlas inimõiguste riivemehhanismiga ja arvestama Euroopa Inimõiguste kohtu praktikat.[149]

Tahest tahtmata põrkuvad kriminaalmenetluses ühiskonna ja kahtlustatava elulised huvid, aga lisaks kriminnaalmenetluslikele reeglitele peab ka arvestama põhiõigustega.[150] Menetlejate tegevus peab alati jääma nii põhiseaduses kui ka inimõigusalastest dokumentides määratud raamidesse[151]

Käesoleva töö autori arvates ei tohiks isikute suhtluse jälgimine olla lihtne. Ilma privaatuseta ei saa inimesed omavahel pidada eraelulist suhtlust seetõttu kannatab ka sõnavabaduse printsiip. Tänapäeva ühiskonda iseloomustab igapäevane tehnoloogia kasutamine ning seetõttu peaksid kriminaalmenetluslikud normid arvestama nende eripäradega Autor usub, et seadusandjal on äärmiselt oluline roll kriminaalmenetluslike piiride paikapanemisel ning seda ei saa teha kergekäeliselt.

Siiki tuleb tõdeda, et kehtiv jälitustegevuse ja läbiotsimise regulatsioon on elektrooniliste sõnumite puhul problemaatiline. Järgmistes alapeatükkides uurib autor lähemalt, milliseid vahendeid kasutatake kriminaalmenetluses elektrooniliste jälgimiseks ja kogumiseks ning toob välja kehtiva regulatsiooni puudused.

3.1. Elektroonilistesse sõnumitesse sekkumine jälitustoimingutega

Enne inforevolutsiooni koosnes jälitustegevus peaasjalikult füüsilistest jälitustoimingutest, mis tähendas seda, et isikut tegevust vaadati ja tema suhtlust kuulati füüsiliselt.[152] Viimase kolmekümne aasta jookusl on ühiskonna arusaam jälitustegevusest ja selle ulatusest väga

[147] Kergandberg, E., Sillaots, M. Kriminaalmenetlus. Juura, Tallinn 2006, lk 29
[148] EIKo5029/71 *Klass and others v Germany*, p 50
[149] *Ibid.*
[150] Lõhmus (2014),*supra* nota 33, lk 15
[151] *Ibid.*
[152] O'Brien, M. Law, privacy and information technology: a sleepwalk through the surveillance society?. Information & Communications Technology Law. 2008, 17(1) lk 28

oluliselt muutunud.[153] Tehnoloogia areng on avardanud jälitustegevuse võimalusi, sealjuures lihtsustanud jälitustoiminguteks antavate lubade menetlemist ning seetõttu jälitustegevusega seotud temaatika üha aktuaalsem.[154] Kuna jälitustoimingute salajasuse tõttu on märksa suureb oht, et riik võib sekkuda meelevaldselt isikute eraellu, on oluline, et seaduste tasemel oleksid sätestatud tõhusad menetlusgarantiid.[155]

Euroopa Inimõiguste kohus leidnud, et jälitustegevust reguleerivad õigusaktid peavad olema piisavalt selged ja üheselt mõistetavad.[156] Kui rahvusvahelistes õigusaktides on jälitustoimingud õigustatud vaid raskete kuritegude puhul siis, Eestis on jälitustoimingud õigustatud ka paljude vähem raskete kuritegude uurimisel.[157] Kuigi jälitustoimingute regulatsiooni üle võiks laiemalt ja põhjalikumalt diskuteerida, vaatleb käesoleva töö autor vaid neid toiminguid, mis on seotud elektrooniliste sõnumitega.

Kriminaalmenetluse seadustiku kohaselt on jälitustoiming isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti eest ning jälitustoiming on lubatud vaid juhul, kui andmete kogumine muude toimingutega või tõendite kogumine muude menetlustoimingutega ei ole võimalik, ei ole õigel ajal võimalik või on oluliselt raskendatud või kui see võib kahjustada kriminaalmenetluse huve.[158] Jälitustoimingud, millega Eestis sekkutakse sõnumite saladuse õigusesse on posti- või telegraafsaadetiste läbivaatus, asja varjatud jägimine või läbivaatus ning sidekanalite kaudu edastatava teabe salajane pealtkuulamine- või vaatamine.[159]

Kriminaalmenetluse seadustiku paragrahv 126^7 kohaselt võib eeluurimiskohtuniku loa alusel salvestada üldkasutatava elektroonilise side võrgu kaudu edastatavaid sõnumeid, mis on saadud salajasel pealtkuulamisel või –vaatamisel.[160] Seevastu paragrahv 126^5 sätestab, et isiku, asja või

[153] *Ibid.*
[154] Parmas, A. jt. Kohtute aastaraamat 2015. Riigikohtu kommunikatsiooniosakond 2016, lk 5
[155] Parmas, A. jt. Tractatus Terribiles: artiklikogumik professor Jaan Sootakki 60. jubeliks. Juura, Tallinn 2009 lk 137.
[156] EIKo 8691/79 Malone V. The United Kingdom, p 67
[157] Lõhmus (2014),*supra* nota 33, lk 338
[158] KrMS RT I, 31.12.2016, 46
[159] Lõhmus (2014),*supra* nota 33, lk334
[160] KrMS RT I, 31.12.2016, 46

paikkonna varjatud jälgimine, võrdlusmaterjali varjatud kogumine ja esmauuringute tegemine ning asja varjatud läbivaatus või asendamine toimub aga prokuratuuri loal.[161]

Selliselt sõnastatud regulatsioon on praktikas toonud kaasa arusaama, et kui jälitusasutus soovib tutvuda informatsiooniga, mis on andmekandjale salvestatud, on vajalik prokuratuuri luba, aga reaalajas infovahetuse jälgimine nõuab kohtuniku luba.[162] Kuna käesoleva töö autor jõudis eelnevalt seiuskohale, et sõnumite saladuse kaitseala peaks kaitsma ka andmekandjale talletatud sõnumeid, võib prokuratuuri loa alusel tehtavat jälitustoimingut pidada autori arvates pidada problemaatiliseks, sest sõnumisaladuse riiveks on alati vajalik kohtu luba.

Ka endine riigi peaprokurör Norman Aas on tõdenud Riigikogu põhiseaduskomisjonile koostatud üevaates, et arvutisüsteemide salajase jälgimise regulatsioon vajab uuendamist.[163] Näiteks ei ole hetkel selge, milline õiguslik režiim kehtib isiku füüsilise kontrolli all olevale elektroonilisele teabekandjale salvestatud infoga varjatud tutvumise kohta, mis tegelikkuses võib olla seotud ka mõne juba edastatud või vastvõetud sõnumiga.[164] Sarnaselt käesoleva töö autorile, on ka Aas seisukohal, et elektrooniliste teabekandjate ja arvutisüsteemidega varjatud tutvumine peaks alati toimuma vaid kohtu loal.[165]

Kuigi põhiõiguste kaitse seisukohalt ei ole võrreldavad arvutisse sisenemine ja ruumi sisenemine, ei tee kriminaalmenetlusseadustik nendel vahet.[166] Vastavalt kriminaalmenetluse seadustiku paragrahvile 126^3 on jälitusasutusel õigus jälgida varjatult isikut, asja või paikkonda, koguda varjatult võrdlusmaterjali ja teha esmauuringuid, teostada varjatult asja läbivaatust ning asendada selle varjatult.[167]

Kuigi põhiseadus nõuab sõnumite saladusse sekkumiseks kohtu luba, ei täpsustata mida kohus peab loa andmisel hindama.[168] Siiani on jäänud selgusetuks, kas jälitustoimingu luba peab nimetama, milliseid kommunikatsioonivahendeid on lubatud jälgida ning kas loas peavad olema

[161] Ibid.
[162] Aas, N. Riigi peaprokuröri ülevaade Riigikogu põhiseaduskomisjonile seadusega prokuratuurile pandud ülesannete täitmise kohta 2012. Aasta. Eesti prokuratuur, 2013, lk 16 www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/riigi_peaprokurori_ettekanne_pohiseaduskomisjonile_2013_0.pdf (12.01.201)
[163] *Ibid.*,lk 15
[164] *Ibid.*, lk 16
[165] *Ibid.*, lk 17
[166] Kergandberg, E. Eesti kriminaalmenetlus: mõned rindeteated. Juridica2013 (4), lk 256
[167] KrMS RT I, 31.12.2016, 46 § 126^3
[168] Lõhmus (2014),*supra* nota 33, lk 335

määratletud isikuid, kelle sõnumite vaatamiseks või pealtkuulamiseks luba antakse.[169] Kohtunikul on võimalus jälitustoimingu loa andmisel kontrollida selle aluseid, kuid toimingu teostamisel ta põhiseadusele vastavust kontrollida ei saa, sest selle üle teostab kontrolli prokurör.[170]

Riigikohtunik Eerik Kergandberg on Juridica artiklis tõdenud: „Meenub, et 20. novembril 2009 kogunes Riigi prokuratuuri initsiatiivil üks ümarlaud ka Riigikohtus. Sellel osalejad otsustasid põhimõtteliselt hääletusega näiteks selliseid küsimusi, et SIM-kaardi ja PUK-koodi kohta tehtavad järele pärimised sideettevõtetele ei ole käsitatavad jälitus tegevusena ja seega on uurimisasutusel õigus neid nõuda ka vaatluse käigus ning arvuti IP-aadresside tuvastamine on käsitatav andmete kogumisena sõnumite kohta ja see saab toimuda prokuröri loa alusel. Hääletamise tulemina nenditi siis ka seda, et luba täna kehtiva KrMS § 126^2 alusel arvutisse sisenemiseks hõlmab võimalust saada teavet kõige arvutis sisalduva kohta ja seega ka dokumentide kohta, mis on arvutis loodud või sinna saadetud enne vastavaks jälitustoiminguks loa saamise kuupäeva. Eriti viimase hääletamise tulemuse õigsuses ja põhjendatuses kahtlen ma täna väga. Kuid tegelikult ei tohiks ju selliseid küsimusi lahendada hääletamisega. Siin on vaja seadusandjat.“[171]

3.1.1 . Nuhktarkvara kasutamine elektrooniliste sõnumite jälgimiseks

Selleks, et kommunikatsiooni arenguga kaasas käia, arendatakse pidevalt ka jälitustehnikad- ja tehnoloogiad. Viimasel ajal on üha aktuaalsemaks muutunud kaugläbiotsimine nuhktarkvara abil. Kui tavaline läbiotsimine toimub reeglina isiku enda või seaduses nimetatud isikute juuresolekul, siis kaugläbiotsimisel tutvutakse arvuti sisuga salaja.[172]

Nuhktarkvaravara puhul on tegu spetsiaalse tarkvaraga, mille abil saab aktiveerida seadmete mikrofone ja kaameraid ning reaalajas jälgida seadme kasutamist. Nuhkvara eeliseks on see, et seda saab isiku aruvutisüsteemi paigaldada varjatult ning ilma füüsilise ligipääsuta.[173] Näiteks

[169] Parmas jt (2016), *supra* nota lk 68
[170] *Ibid.*
[171] Kergandberg, *supra* nota166 lk 266 (Eesti kriminaalmenetlus: mõned rindeteated)
[172] Lõhmus(2014) *supra* nota 33, lk 322
[173] Abel, W. Agents, Trojans and tags: The next generation of investigators. International Review of Law, Computers & Technology 2009 23(1-2), lk100

piisab sellest, et isik avab talles spetsiaalselt saadetud e-kirja, mille avamisel nuhkvara rakendub.[174]

USA oli esimene riik, kes võttis kasutusele elektroonilise jälgimise tarkvara, mis võimadas reaalajas uurida ning salvestada kõike, mida inimene arvutis trükkis või tegi.[175] Saksamaal on nuhkvara kasutamise tõttu kehtestatud uus põhiõigus infotehnoloogia terviklikuse ja konfidentsiaalsuse kaitseks, sest varasemad põhiõigused ei olnud piisavad, kaitsmaks isikuid infotehnoloogisasüsteemide jälgimise eest.[176]

Meedias on leivinud informatioon, et ka Eesti õiguskaitseorganid on hakanud nuhkvara kasutama. Näiteks Wikileaksi poolt avaldatud andmete kohaselt on Eesti Vabariik ostnud 34 Finfisheri nuhkvara litsentsi[177] Siiani ei ole avalikustatud, kas või millistel eesmärkidel antud nuhkvara kasutati, sest jälitustegevust kaitseb riigisaladus.[178]

Seni ei ole ka Eesti kohtute praktikas arututatud selle, kas nuhkvara arvutisüsteemi paigaldamine võib käsitleda tehnilise abivahendi paigaldamisena vastavalt kriminaalmenetluse seadustikule nõuab kohtu luba.[179] Kuna nuhktarkvara paigaldamise ja selle abil andmete kogumisega kaasneb riive eraelu puutumatusele ja sõnumite saladusele, peaks see toiming toimuma üksnes kohtu loal.[180] Iseigi kui nuhkara on Eestis kasutusel, võib ka siin esineda problemaatika seoses sõnumite saladuse ajalise piiranguga. Näiteks kirjedab Põhiseaduslikkuse järelevalve kolleegiumi nõunik Alexander Lott, et kui arvutis toimuva suhtluse jälgimine nuhkimistarkvara abil kuulub põhiseaduse paragrahvi 43 kaitsealla, siis olukorras kui samal seansil tutvutakse juba toimunud vestluste logidega on kuulub see aga pearekonna- ja eraelu kaitse all.[181]

Sisepoliitika asekansler Erkki Koort on öelnud, et:“ Eesti suhtub kindlasti tõsiselt kõikidesse taolistesse indikatsioonidesse nimetatud tarkvarade võimalikust kasutamisest Eestis. Kui

[174] *Ibid.*

[175] Ortiz, J. C. Fighting Cybercrime in Europe: The Admissibility of Remote Searches in Spain.European Journal of Crime, Criminal Law and Criminal Justice 2014, 19 (4),lk 14

[176] Abel, W., Schafer, B. The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems-A Case Report on BverfG. SCRIPTed 2009 6 (1) lk 107-123

[177] FinFisher – Customers www.wikileaks.org/spyfiles4/customers.html (01.11.2016)

[178] Änilane, E. Peep Aru FinFisheri nuhkvara kasutamistest: jälitustegevust kaitseb Eestis riigisaladus. www.delfi.ee/news/paevauudised/eesti/peep-aru-finfisheri-nuhkvara-kasutamistest-jalitustegevust-kaitseb-eestis-riigisaladus?id=69762871 (01.11.2016)

[179] Parmas jt (2016) *supra* nota154, lk 62

[180] *Ibid.*

[181] Lott. supra nota 129, lk 26

tegemist on mistahes ebaseadusliku tegevusega, siis kavatseb Eesti riik sellist tegevust kindlasti takistada. Eesti riik ise kasutab inimeste turvalisuse tagamiseks neid vahendeid, mida on eesmärgi saavutamiseks vaja. Nende vahendite loetelu ei avaldata, kuna see annab ülevaate riigi võimekustest".[182] Eeltoodust on keeruline, kas nuhktarkvara leiab kasutust, sest seda kaitseb riigisaladus. Autor on siiski arvamusel, et seaduse tasemel tuleks nuhktarkvara kasutamist siiski reguleerida.

3.1.2. Isiku õigus teada tema suhtes tehtud jälitustoimingutest ning jälitustegevuse kontroll

Kuna jälitustoiminguid tehakse isiku eest varjatult, on tavaline, et isik ei saa enda kohta käivate andmete töötlemisest alles hiljem teada ning mõningatel juhtudel ei teavitata isikut üldse. Tartu Ülikooli õigusteaduskonna magister Meelis Rondel kirjeldab ajakirjas Juridica, et isiku õigus saada teada jälitustoimingutega kogutud andmetest kuulub informatsioonilise enesemääramise õiguse alla.[183] Informatsiooniline enesemääramine tähendab sisuliselt seda, et igal isikul on õigus otsustada seda, kas ja kui palju informatsiooni tema kohta kogutakse ja salvetatakse.[184]

Kriminaalmenetluse seadustiku paragrahv 65 lõike 4 sätestab, et kui kriminaalmenetluses kasutatakse tõendite hankimiseks tehnikavahendeid, tuleb sellest eelnevalt teavitada menetlustoimingus osalejaid ning nende vahendite kasutamise eesmärki.[185] Vastavalt paragrahvile 126^{13} tuleb jälitustoimingu tegemise loa tähtaja lõppemisel teavitada kelle suhtes jälitustoiming tehti, ning isikut, kelle perekonna- või eraelu puutumatust jälitustoiminguga oluliselt riivati.[186] Kahjuks pole teada, kas antud paragrahvis oli vaid perekonna- ja eraelu puutumatuse nimetamine seadusandja teadlik valik.[187] Antud juhul võib sättest välja lugeda, et kui jälitustoiminguga riivatakse sõnumite saladuse õigust, siis jälitusasutus sellisel juhul isikut teavitama ei pea.[188]

Jälitustoimingute puhul saab Eestis probleemseks pidada ka seda, et kriminaalmetlusseadustikus puudub jälitustoimingute dokumenteerimise kohustus ning seetõttu sõltub dokumenteeritakse

[182] Aasmäe, K. Siseministeerium ei kinnitanud ega lükanud ümber Finfisheri nuhkvara võimalikku kasutamist. Postimees 2012. majandus24.postimees.ee/941996/siseministeerium-ei-kinnitanud-ega-lukanud-umber-finfisheri-nuhkvara-voimalikku-kasutamist?_ga=1.137999731.2113773778.1491122744 (15.03.2017)
[183] Rondel, M. Informatsioonilise enesemääramise õigus ja jälitustegevus. Juridica 2016 (7), lk 714
[184] § 19, p 31.2.1. Põhiõigused ja Vabadused. II peatükk. Eesti Vabariigi põhiseadus. pohiseadus.ee/ptk-2/pg-19/ (15.03.2017)
[185] KrMS RT I, 31.12.2016, 16 § 65 lg 4
[186] *Ibid.*, § 126^{13}
[187] Parmas jt (2016) *supra* nota 154, lk 70
[188] *Ibid.*

põhjalikkus üksnes menetlejast.[189] Sellise regulatsiooni puudumine on vastuolus digitaalkriminalistika põhimõtetega, mille kohaselt tuleb dokumenteerida kõik kasutatud töö- ja uurimismeetodid, sest dokumenteerimata jätmisel ei ole hilisemalt võimalik tõendite usaldusväärust kohta hinnangut anda.[190].

Olukorra parandamiseks lisatud kriminaalmenetluse seadustikku paragrahv 126[10], mille kohaselt peab jälitustoimingu või jälitustoimingut taotlenud asutuse ametnik koostama jälitustoiminguga kogutud teabe alusel jälitustoimingu protokolli.[191] Samas ei lahenda selline dokumenteerimise kohustus veel digitaalkriminalistika põhimõtteid, sest regulatsioon ei pane menetlejale kohustust kirjeldada digitaalandmete kogumise protsessi ning seda, kuidas on säilitatud andmete algupärasus ja terviklikkus.[192]

3.2. Arvutisüsteemi ja andmekandja läbiotsimine

Arvutikuritegevusvastase konventsiooni artikkel 19 punkt 1 kohaselt peavad konventsiooniosalised võtma seadusandlikke ja muid meetmeid volitamaks pädevat asutus tema territooriumil korraldama otsingu, et saada juurdepääs arvutisüsteemile või selle osale ning selles salvestatud andmetele ning andmekandjale, milles arvutiandmed on salvestatud.[193]

Paljud digitaalkriminalistid on arvamusel, et tänapäevasel infotehnoloogiaajastul võiks läbiotsimismäärused sisaldada ka luba digitaalsete tõendite otsimiseks või arestimiseks, hoolimata sellest, kas nende tõenditega on võimalik ka kuritegu tõendada.[194] Sellise arvamusega ei saa siiski nõustuda, sest vastasel juhul oleksid põhjendamatult riivatud isikute põhiõigused.

Kriminaalmenetluslike normide üheks peamiseks eesmärgiks on kehtestada reeglid mida riik peab tõendite kogumisel järgima.[195] Vastavalt Kriminaalmenetluse seadustiku paragrahv 91

---

[189] Ginter, J. jt. Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses. Tartu Ülikool 2013. www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/analuus_isikute_pohioiguste_tagamisest_ja_eeluurimise_kiirusest_kriminaalme netluses.pdf (04.11.2016) lk 153

[190] *Ibid.*

[191] KrMS RT I, 31.12.2016, 16 §126[10]

[192] Trehver, J. Digitaalsete tõendite kasutamise võimaldamine. 2016. www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf (15.11.2016) lk 9

[193] Arvutikuritegevusvastane konventsioon RT II 2003, 9, 32 artikkel 19 p 1

[194] Ginter (2013) *supra* nota191, lk 129

[195] Hirsnik, E. Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid. Juridica 2014 (8) lk 621

lõikele 2 võib läbiotsimist toimetada prokuratuuri taotlusel eeluurimiskohtuniku määruse või kohtumääruse alusel.[196] Sama paragrahvi lõike 3 kohaselt võib läbiotsimist teostada ka ainult prokuatuuri määruse alusel, kui on piisavalt alust arvata, et kahtlustatav kasutab või kasutas läbiotsitavat kohta kuriteosündmuse või kohtueelse menetluse ajal. [197]

Kriminaalmenetluse seadustiku paragrahvi 91 kohaselt on läbiotsimise eesmärgiks 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.[198] Sama paragrahvi lõike 4 kohaselt peab läbiotsimismäärus sisaldama otsitavat objekti, läbiotsimise põhjendust ja kohta. [199]

Märksa keerulisem on aga olukord siis, kui hakatakse otsima teatud informatsiooni arvutisüsteemilt või andmekandjalt endalt. Kirjanduses on välja toodud, et kuigi arvutisüsteemide läbiotsimise vajadus võib esineda enamustes kriminaalmenetlusest, ei sätesta kehtiv regulatsoon läbiotsimise kohana arvutisüsteemi.[200]

Kuigi uurimispraktikas on levinud läbiotsimise käigus arvuti äravõtmine ja selle sisu piiranguteta uurimine, võib selline praktika tuua kaasa erinevaid probleeme.[201] Näiteks ei saa arvutit lugeda ruumiks, hooneks ega sõidukiks ning seetõttu võib järeldada, et eraelu riiveks puudub õiguslik alus ning kehtivad läbiotsimist reguleerivad normid on ajale ja selle vajadustele jalgu jäänud.[202] Kuna kriminaalmenetluse seadustikus sätestatud läbiotsimise objektid on sõnastatud lõpliku loeteluna, ei saa seda ka õiguse tõlgendamise abil laiendada.[203]

Praktikas lähtutakse arvutisüsteemi läbiotsimisel kriminaalmenetluse seadustiku paragrahvist 86, mille kohaselt selgitatakse vaatlusega dokumendi või muu objekti kuriteojäljed ja muud tunnused vaatluse abil.[204] Andmekandjate vaatlus teeb probleemseks asjaolu, et praktikas võimaldab vaatlus menetlejal võimalik praktiliselt piiramatu aja jooksul ning piiramatu arv kordi

[196] Kriminaalmenetluse seadustik RT I, 31.12.2016, 16 §91 lg2
[197] *Ibid, lg3*
[198] *Ibid*. §91
[199] *Ibid*. lg 4
[200] Parmas jt (2016), *supra* nota 154 ,lk140
[201] Lõhmus (2014),*supra* nota 33, lk 312
[202] *Ibid*., lk 313
[203] *Ibid*., lk 312
[204] KrMS RT I, 31.12.2016, 46 §86

vaadata läbi andmekandjat ning menetlejal on otsustusõigus, mida ta arvutisüsteemilt otsida soovib.[205]

Käesoleva töö autor leidis varasemalt, et sõnumisaladuse alla peaksid kuuluma ka edastamisprotsessi läbinud elektroonilised sõnumid. Praktikas võib vägagi tõenäoline olla, et menetleja võib menetleja leida arvutisüsteemidelt ja andmekandjatelt erinevaid e-kirju või vestluste salvestusi ning olukorras kahtlustatava kinnipidamise käigus avastatakse töötav arvuti koos avatud e-posti kontoga, ei ole seaduse kohaselt menetlejatel vajalik toimetada läbiotsimise regulatsiooni kohaselt, sest andmete läbivaatamine toimub vaatlusena.

Ühe konkreetse e-kirjavahetuse otsimiseks tuleb sageli töödata läbi väga palju informatsiooni, sealhulgas ka sellist teavet, mis ei ole kriminaalmenetluse jaoks relevantne. Samas ei saaks narkootiliste ainete valmistaja arvuti läbiotsimisel, menetlejaid määrusega kohustada vaid otsima teatud nimedega andmeid, sest kurjategijad ei pruugi enda kriminaalseid andmeid teistest andmetest erinevalt sildistada.[206]

Tegelikkuses on arvutite ja andmekandjate sisu läbiotsimise piiramine väga keeruline. Ühelt poolt muudaksid piirangud ainult kindla sisu või kindlat tüüpi informatsiooni otsimiseks menetlejate töö väga keeruliseks, teisalt oleks põhiõiguste kaitse seisukohalt selline piirang teatud ulatuses vajalik. Ameerika Ühendriikides on kohtud ja teadlased üritanud probleemile lahendust leida, aga siiani on jõutud järeldusele, et ühte kindlat reeglit on peaaegu võimatu paika panna.[207]

Kuna arvutisüsteemides talletatakse väga palju andmeid, on läbiotsimise käigus võimalus menetlejatel avatada ka juhuleide.[208] Praktikas on juhuleiud eelkõige lubatavad tõendina vaid siis, kui see leid kajastab kataloogikuritegu puudutavaid andmeid.[209] Sätted, mis reguleerivad Kriminaalmenetlusseadusikus vaatlust, ei piira menetleja tegevust vaatlustoimingute tegemisel,

[205] Parmas jt (2016) *supra* nota 154 ,lk 138

[206] Dripps, D. A. Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure. The Journal of Criminal Law & Criminology 2013, 103 (1). lk 106

[207] Trepel, S. Digital Searches, General Warrants, and the Case for the Courts. Yale Journal of Law and Technology 2007, 10 , lk 150

[208] § 91, p4. Läbiotsimine ja uurimiseksperiment. Kriminaalmenetlusseadustiku kommenteeritud väljaanne. Juura, Tallinn 2012

[209] *Ibid.*

mille tulemuseks võiks olla ka sellise inkrimineeriva materjali leidmine, mida esialgu otsidagi ei osatud.[210]

Käesoleva töö autor on arvamusel, et praktikas võib esineda olukordi, kus e-posti konto või või meiliteenuse programmi vaadeldes võib menetleja ka ilma kirja avamata saada infiormatsiooni sõnumi sisu kohta. Näiteks võib teatud juhtudel ka e-kirja pealkirja kohelda sarnaselt sõnumi sisuga, sest pealkirjad avalikustavad teemat, annavad kommunikatsiooni sisu kohta selgitusi ning on osaks teabest, mida üks osapool soovib teisega jagada..[211]

Endine õiguskantsler, Indrek Teder, on öelnud:“ Arvestades elektroonilise suhtluse laia kasutusala ning elektroonilistes andmekandjates sisalduvainfo teatavaks saamisega kaasnevat põhiõiguste riive ulatust, oleks siiski asjakohane kaaluda, kas täpsem regulatsioon (koos vajalike menetlusgarantiidega) aitaks kaasa põhiõiguste ja –vabaduste paremale tagamisele.“[212] Käesoleva töö autor nõustub eelneva väitega ning on arvamusel, et kahtlemata on seadusandjal vajalik kiiremas korras teha muudatused ning viia normid kooskõlla tänapäevase tehnoloogiaga,

3.2.1 Elektrooniliste sõnumite ja andmekandjate kopeerimine

Kui füüsilise asitõendi puhul on tavapärane asitõendi otsimine valdusest ning seejärel selle ära võtmine, siis arvutitehnoloogia puhul tuleks eelistada digitaalsete andmete kopeerimist[213] Koopiate tegemise vajadus tuleneb sellest, et kuna arvutid sisaldavad hulgaliselt informatsiooni, on nende läbivaatamine äärmiselt ajamahukas.[214] Näiteks on professor Rait Maruste arvamusel, et suuremahulist dokumentide äravõtmist ja arvutite konfiskeerimist saab võrrelda dokumendikapi äravõtmisega, sest lisaks sõnumi-, omandi ja eraeluvabadusele sekkutakse ka isiku kaitseõigusesse, kuna isik ei saa enda kohtulikku kaitset ette valmistada.[215]

---

[210] Parmas jt (2016) *supra* nota 154 ,lk 139

[211] Tokson, M. The Content/Envelope Distinction in Internet Law. William & Mary Law Review 2009, 50, (6), Lk 2131

[212] Teder, I. Arvamus eelnõule Kriminaalmenetluse seadustiku jt seaduste muutmise eelnõu (295 SE). www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_arvamus_eelnoule_kriminaalmenetluse_seadustiku_jt_seaduste_muutmise_eelnou_295_se.pdf (15.11.2016) lk 7

[213] Kerr, O. S. Fourth Amendment Seizures of Computer Data. The Yale Law Journal 2010, 119 (4), lk 702

[214] *Ibid.*, lk 704

[215] Maruste, R. Rait Maruste: Kas prokuratuur ja kapo suudavad tõrjuda mõjuvõimu ärakasutamise kahtlustusi? Eesti Päevaleht 2012 epl.delfi.ee/news/arvamus/rait-maruste-kas-prokuratuur-ja-kapo-suudavad-torjuda-mojuvoimu-arakasutamise-kahtlustusi?id=63833640 (21.03.2017)

Kui isiku elektroonilised andmekandjad võetakse isikult ära mitmeks kuuks, takistab see oluliselt nende omanike igapäevast tegevust. [216] Kui isikult on võetud ära andmekandja, mis sisaldab majandustegevuse jätkamiseks olulisi andmeid raamatupidamise kohta, tuleb esimesel võimalusel neile tagastada, sest muidu võidakse liiga intensiivselt. sekkuda isiku ettevõtlusvabadusse.[217] Sama probleem võib ka esineda elektrooniliste sõnumitega, sest isikud võivad neid salvestada võrguväliseks kasutamiseks andmekandjale ning meiliteenuse serverist kogu kirjavahetuse ära kustutada. Mobiiltelefonidele saadetud sms- id jäävad tihtipeale ainult seadme sisemällu ning mobiiltelefonide konfiskeerimine võib kahtlemata piirata erinevaid põhiõiguseid.

Süüditataval või kahtlustataval võib olla mitmeid erinevaid erinevaid andmekandjaid ning see seab omakorda piirid tõendite otsimisele.[218] Kahjuks tuleb tõdeda, et Eesti läbiotsimispraktikale on omane, olukord, kus läbiotsimist toimetav menetleja võtab isiku valdusest ära arvutite kõvakettaid, hoolimata sellest et need võivad sisaldada kirjavahetust, ärisaladusi jne.[219] Kuigi Kriminaalmenetluse seadusik ei reguleeri asitõenditest koopiate tegemist on riigikohus andnud juhtnööre, et arvuti, arvutisüsteemi või andmekandja äravõtmise asemel tuleks võimaluse korral asjassepuutuvad andmed kopeerida.[220]

Justiitsministeeriumi poolt läbiviidavas kriminaalõiguse revisjonis tuuakse välja, et kuna digitaalset teavet on äärmiselt kerge mõjutada ning andmete manipuleerimist on väga raske hiljem tuvastada, tuleks seadusega täpsemalt reguleerida teabetalletuse koopiate tegemise nõuded.[221] Näiteks Sloveenias on seaduse tasemel määratletud, et võimalusel peab menetleja tegema digitaalsetest andmetest koopia.[222] Käesoleva töö autor on seisukohal, et teabetalletusest koopiate tegemine riivab oluliselt vähem ka omandipõhiõiguse riivet, sest isikule jääb õigus neid vallata, kasutada ja käsutada.

---

[216] § 86, p4.2. Vaatlus.Kriminaalmenetlusseadustiku kommenteeritud väljaanne. Juura, Tallinn 2012 lk 257

[217] Kriminaalmenetluse seadustiku kom Sarv lk 339 3 ptk 9. Jag p2

[218] Kerr, O. S. Ex ante regulation of computer search and seizure. Virginia Law Review 2010, 96 (6), lk 1249

[219] Reps, M. Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu 295 SE. https://www.riigikogu.ee/download/7457e622-fe01-4d20-9af1-cd6cda20829d (06.04.2017) Lk 12

[220] RKKKm 3-1-1-57-12 p16

[221] Trehver(2016) *supra* nota194, lk 7

[222] Selinsek, L. Electronic evidence in the Slovene Criminal Procedure Act. Digital Evidence & Electronic Signature Law Review 2010, (7) lk 79

Juhul kui koopia tegemine ei ole võimalik ning andmekandja tuleb arvutisüsteem või andmekandja isiku käest ära võtta. Kuid see, kui pikaks ajaks andmekandja ära võetakse, sõltub konkreetsetest asjaoludest, sest kehtivas kriminaalmenetluse seadustikus ei ole sätestatud piiranguid läbiotsimise ega ka vaatluse kestuse kohta. Riigikohus on seisukohal, et ajalist piiri ei saa läbiotsimise kohta rakendada just seetõttu, et läbiotsimise kestus sõltub väga mitmetest teguritest.[223]

Töö autori arvates peaks arvutisüsteemideemide vaatlus olema siiski ajaliselt piiratud. Autor nõustub, professor Orin S. Kerr-iga, kes leiab, et mõistlik aeg arvuttiandmetest koopiate tegemiseks võiks olla 30 päeva ning vajadusel võiks saada seda taotluse alusel pikendada.[224]

3.2.2. Kaugläbiotsimine ja pilveteenused

Pilvandmetöötlus on vahend, mis võimaldab isikul salvestada ja hoiustada digitaalseid andmeid, kaugel asuvates serverites, selle asemel, et neid salvestada tavalistele andmekandjatele.[225] Selliste andmete mobiilsus võib tekitada õiguskaitseorganitele erinevaid probleeme arvutisüsteemi läbiotsimisel.[226]

Kui menetleja asub uurima isiku arvutit või andmekandjat, on tal reeglina ligipääs ainult seadmes salvestatud sõnumitele. Märksa suuremat kommunikatsiooniteavet salvestatakse tänapäeval pilvteenusesse. Paljud e-maili teenust võimaldavad ettevõtted võimaldavad tänapäeval hoiustada väga suurtes andmemahtudes sõnumeid ja sõnumite sisuks olevaid manuseid. Reeglina ei pea teenuse kasutajad sõnumite kustutama või eraldi andmekandjale salvestama.

Juurdepääsu saamine digitaalsetele tõenditele, mis asuvad pilveteenuses või teises riigis on üldiselt tehniliselt ja juriidiliselt keerulised.[227] Interneti globaalsuse tõttu esineb väga palju jurisdiktsioonilisi probleeme, sest näiteks üks veebimajutust pakkuv ettevõtte võib olla

[223] RKKKo 3-1-1-31-11 p 18.3

[224] Kerr, O. S. Search Warrants in an Era of Digital Evidence. 75 Mississippi Law Journal 2005 (85), lk136

[225] Kohls, S. J. Searching the Clouds: Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account. Case Western Reserve Journal of Law, Technology and the Internet 2012, 4(1), lk 169.

[226] *Ibid.*

[227] Komisjoni Teatis Euroopa Parlamendile, Euroopa Ülemkogule Ja Nõukogule Neljas Eduaruanne Tulemusliku Ja Tegeliku Julgeolekuliidu Suunas Liikumise Kohta. 2017 Eur-Lex.Europa.Eu/Legal-Content/Et/Txt/Pdf/?Uri=Celex:52017dc0041&From=Et lk 8 (23.03.2017)

registreeritud ühte riiki, aga nende serverid võivad olla laiali erinevates riikides.[228] Samuti on tavapärane, et ühes ja samas riigis vestlevad isikud võivad suhelda läbi teenusepakkuja, kes asub hoopis teises jurisdiktsioonis.[229]

Kui läbiotsimise käigus võetakse isikult ära tema arvuti, võib see tekitada probleeme, sest tihtipeale võib kaduda informatsioon selle kohta, milliseid pilveteenuseid isik kasutada võis.[230] Käesoleva töö autori arvates saab problemaatiliseks pidada olukorda, kus menetlejal on ligipääs isiku arvutile ning seega võimalus tutvuda serveris talletatud elektrooniliste sõnumitega, sest kehtiv seadus ei reguleeri pilvteenuse läbiotsimist. Eraldi probleemida võib välja tuua, et enamasti asuvad pilveteenuste serverid teiste riikide territooriumil ja seetõttu ka teises õigussüsteemis.[231] Näiteks võib ka üks fail olla jagatud erinevateks osadeks ning salvestatud erinevate pilveteenuste serveritesse, mis kõik asuvad erinevate riikide territooriumil.[232]

Rahvusvahelistest allikatest reguleerib kaugläbiotsimist Avutikuritegevuse vastase konventsioon, mille artikli 32 kohaselt võib üks konventsiooniosaline teise konventsiooniosalise loata saada juurdepääsu avalikele arvutiandmetele nende asukohast sõltumata, 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.[233] Kuigi Arvutikuritegevusevastane konventsioon annab üldised reeglid, on läbiotsimise laiendamise juriidiline vormistus jäetud siseriikliku õiguse reguleerida, ei ole Eesti seadusandja seda siiski teinud.[234] Seetõttu peavad menetlejad lootma, et serveri asukohariik avalikustaks vajalikud andmed läbi õigusabipalvete.

Hiljuti kaitstud doktoritöös, uuris Anna-Maria Osula piiriüleste andmete kaugläbiotsimist ning jõudis järeldusele, et kuigi praktikas on kaugläbiotsimise kriminaalmenetluses vajalik, tuleb

[228] Kerr. (2014),*supra* nota 103, lk 3
[229]Hosein, *supra* nota 139 lk 1077
[230] Parmas jt (2016), *supra* nota 151, lk140
[231] *Ibid.*
[232] Pearson, S., Yee, G. Privacy and Security for Cloud Computing. Springer London 2013, lk 47
[233] Arvutikuritegevuse vastane konventsioon RT II 2003, 9, 32
[234] Parmas jt (2016) *supra* nota 151, lk 148

tõdeda, et Eestis kehtiv õiguskord selles osas puudulik.[235] Ta jõudis järeldusele, et kaugläbiotsimine vajab läbipaistvat regulatsiooni ja konkreetsemaid kontrollimehhanisme.[236]

3.2.3. Läbiotsimise käigus leitud krüpteeritud sõnumid

Tartu ülikooli arvutiteaduse instituudi andmeturbe professor Dominique Unruh on tõdenud, et sõnumisaladust aitab kaitsta kvantkrüptograafia, mis kindlustab erinevates asukohtades paiknevate osapoolte side privaatsust.[237] Kuigi andmete krüpteerimine kaitseb andmete konfidentsiaalsust ja sisu terviklikust kolmandate osapoolte eest, tunnevad siiski paljud riigid muret, et krüpteerimine aitab kurjategijatel tagada enda anonüümuse ning seetõttu on valitsustel keeruline nii kuritegusid ennetada kui kriminaaluurimisi läbi viia.[238]

Kuigi andmete krüpteerimist ei ole rahvusvahelises õiguskirjanduses peetud inimõiguseks, on siiski küsimus selles, kas krüpteerimine on hädavajalik vahend inimõiguste kaitseks.[239] Ameerika Ühendriikides ja Suurbritannias on paljud poliitilised juhid ja õiguskaitseorganid avaldanud soovi internetisüsteemide muutmiseks, et tagada riiklik juurdepääs isikute privaatsetele andmetele, isegi juhul kui need on krüpteeritud.[240]

Kriminaalmenetluse revisjonis tõdetakse, et kuna seaduse tasandil ei ole sätestatud krüpteeritud või muul viisil vaatlemise eest kaitstud andmetele juurdepääsu saamise tingimused, oleks nende loomine Eesti õiguskorda vajalik.[241] Revisjonis pakutakse välja, et olukorras, kus andmekandjale salvestatud andmed on krüpteeritud, peaks menetlejal olema õigus nõuda andmekandja omanikult krüpteerimisvõtit või kasutada krüpteeringu kõrvaldamiseks spetisaalseid

---

[235] Osula, A-M. Remote search and seizure Of extraterritorial data. Tartu Ülikool. dspace.ut.ee/bitstream/handle/10062/55683/osula_anna_maria.pdf?sequence=1&isAllowed=y lk 86 (23.04.2017)

[236] *Ibid*. lk 87

[237] Paulus, S. Teadlane: sõnumisaladust aitab kaitsta kvantkrüptograafia. Eesti Rahvusringhääling. http://novaator.err.ee/v/yhiskond/bea946cf-9c59-4df3-80ac-2aa46035d48b/teadlane-sonumisaladust-aitab-kaitsta-kvantkruptograafia (19.02.2017)

[238] Kaye, D. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc. lk 6 (05.02.2017)

[239] Murphy, M. H.Technological solutions to privacy questions: what is the role of law?. Information & Communications Technology Law 2016 25(1) , lk 22

[240] Abelson, H. jt. Keys under doormats: mandating insecurity by requiring government access to all data and communications. Journal of Cybersecurity 2015 (1) ,lk 72

[241] Trehver (2016) *supra* nota 194, lk 8

tehnikavahendeid.[242] Ka Tartu Ülikooli poolt tehtud uuringus tõdetakse, et seaduses tuleb sätestada krüpteeritud või parooliga kaistud andmete arestimise erikord.[243]

3.4. Elektrooniliste sõnumid kui digitaalsed tõendid

3.4.1 Digitaalsete tõendite eripära

E-posti või sotsiaalmeedia konto võimaldavad uurijatele anda nii teoreetilist kui ka faktilist informatsiooni kuriteo toimepanemise kohta.[244] Tõendamine on kriminaalmenetluse keskseks osaks, sest kohtuotsus, sõltumata sellest, kas see on süüdimõistev või õigeksmõistev, peab tuginema tõenditele.[245] Selleks, et kohtuotsus oleks usaldatav, on riigid välja töötanud nii tõendi kui ka protseduurireeglid.[246]

Kriminaalmenetluses on tõendamisel hakatud üha enam kasutama infotehnoloogat, sest inimeste kommunikatsioon on muutunud väga suures osas digitaalseks. Nagu autor eelnevalt kirjeldas, on menetlejatel võimalik läbi vaatluse arvutisüsteeme läbi otsida ning jälitustoimingutega vaadata pealt sõnumeid. Seetõttu on tehnoloogia aregnu tõttu tekkinud tavatõendite kõrvale ka digitaalsed tõendid.

Digitaalne tõend on tehnoloogiaajastul välja kujunenud uus tõendi vorm, mille tõendamiseseme asjaolud on osaliselt või täielikult digitaalsel kujul.[247] Stephen Mason tõdeb, et digitaalsed tõendid koosnevad ainult digitaalsetel kujul esitatavatest andmetest, mis on salvestatud arvutisse, andmekandjale või tehtud kättesaadavaks internetis.[248] Mõiste „elektrooniline tõend“ on kasutusel pigem üldisena, mitte spetsiifilise terminina, mis tähistab igasuguseid andmeid, olgu need loodud analoogseadme poolt või digitaalsel kujul.[249] Käesolevas magistritöös kasutatakse siiski antud mõisteid sünonüümidena.

---

[242] *Ibid.*,lk 9
[243] Ginter(2013) *supra* nota 191 ,lk 152
[244] Day, R. Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services. Kansas Law Reviw. 2015 (64), lk 492
[245] Lõhmus (2014),*supra* nota 33, lk 75
[246] *Ibid.*, lk 77
[247] Ginter(2013), *supra* nota 191, lk29
[248] Mason, S. Rethinking Concepts in Virtual Evidence. The Icfai Journal of Cyber Law 2008 (7) lk 51
[249] *Ibid.*

Elektrooniliste sõnumitega seotud digitaalseid tõendeid on väga erinevaid. E-kirja vahetused on reeglina salvestatud pilveteenusesse või andmekandjale. Mobiiltelefonide SIM kaardid võivad pakkuda väärtuslikku informatsiooni isiku kontaktandmete, kõnelogide ja sõnumite kohta.[250] Üha enam kasutatakse ka kõnede tegemiseks internetitelefoni ning väga levinud ka on erinevad suhtlusvõrgustikud, kus suhtlus salvestatakse reeglina serveritesse. Seetõttu jätavad elekroonilised sõnumid peaaegu alati maha mingi jälje, olgu selleks siis sõnumi sisu või sideandmed.

Kriminaalmenetluses ei ole digitaalsed tõendid abivahendiks ainult arvutikuritegude tõendamisel, sest peaaegu kõikide kuritegude puhul võib leida teatud digitaalseid andmeid, nagu näiteks telefonikõned, videosalvestused ja liikumisandmed. Teisalt on infotehnoloogiasüsteemid ka kuritegude toimepanemise vahendiks. Näiteks kasutatakse telefone ja e-kirju isikute või organisatsioonide anonüümseks ahistamiseks ning internet võimaldab kurjategijatel läbi viia pettuseid ja jagada illegaalseid pornograafilisi materjale.[251]

Õnneks teeb internet ja tänapäevane kommunikatsioonitehnoloogia mõnevõrra ka kurjategijate tegevuse haavatavaks.. Nii on tuvastatud mõrvareid tänu nende on-line tegevusele ning lapspornograafia jagajate kaudu on tuvastatud laste vastu suunatud kuritegusid.[252]

2005. aasta viidi Euroopas läbi uuring, millest selgus, et enamus Euroopa riikide kohtunikest on arvamusel, et elektrooniline tõendusmaterjal ei erine suures osas traditsioonilistest tõenditest ning nad peavad seda oma olemuselt samaväärseks dokumentaalsete tõenditega.[253] Eelnimetatud uuringust selgus, et kui osad kohtunikud pidasid digitaalseid tõendeid nende objektiivsuse ja täpsuse tõttu usaldusväärseks, siis teised olid vastupidisel arvamusel, sest puuduvad efektiivseid vahendeid kontrollimaks digitaalsete tõendite õigsust.[254] Siiski tuleb silmas pidada, et eelnimetatud uuringust on möödas üle kümne aasta ning vahepeal on infoehnoloogia oluliselt edasi arenenud ning võimaldab koguda palju täpsemat informatsiooni.

[250] Ibrahim, N., Al Naqbi, N., Iqbal, F.m., AlFandi, O. SIM Card Forensics: Digital Evidence. Annual Conference on Digital Forensics, Security and Law 2016 (3) lk 220

[251] Casey, E. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011, lk 289

[252] *Ibid.*, lk290

[253] Insa, F. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study, Journal of Digital Forensic Practice 2007 (3) lk 286

[254] *Ibid.*

Tuleb tõdeda digitaalsed tõendid vajavad kõrgelt spetsialiseeritud tehnilist teadmist, aga ka teatud menetluslikke erireegleid. Informatsiooni väärkasutuse tagajärjel võib informatsioonist puudutatud isiku elule ja tegevusele avalduda ulatuslik negatiivne mõju ning eriti tõsised tagajärjed võivad avalduda juhul, kui sellist informatsiooni kasutatakse riigi poolt läbi viivates menetlustes.[255]

Selleks, et digitaalseid tõendeid saaks ka kohtus kriminaalasja tõendamisel kasutada, on hädavajalik kehtestada digitaalsete tõendite jaoks standardne ja formaliseeritud protsess.[256] Huvide tasakaalustamise seisukohast on oluline, et riigid järgiks proportsionaalset, selget, läbipaistvat ja perioodiliselt kontrollitud õiguslikku raamistikku.[257] Sellise raamistiku eesmärk on välja selgitada, millistel tingimustel ja kuidas võib riik kasutada isikute digitaalseid andmeid, tagamaks sealjuures, et meetmete kasutamiseks oleks antud kohtu luba ning, et need meetmed oleksid piiratud sellega, mis on hädavajalik õiguspärase eesmärgi saavutamiseks.[258]

3.4.2. Digitaalsed tõendid Eesti kriminaalmenetluses

Euroopa Nõukogu liikmesriigid võtsid 2001. aasta novembris vastu Arvutikuritegevusevastase konventsiooni, mis jõustus Eestis 2004. aastal.[259] Täpsemalt paneb konventsiooni artikkel 19 konventsiooniosalistele kohustuse võtta vastu meetmeid, et volitada pädev asutus tema territooriumil korraldama otsingu, et saada juurdepääs arvutisüsteemile või selles salvestatud andmetele ja andmekandjatle.[260] Samuti peavad konventsiooniosalised järgima, et tema siseriiklikes seadustes ettenähtud proportsionaalsuspõhimõtet ja asjaomaseid kaitsenõudeid ning rahvusvahelistest inimõigusi käsitlevatest õigusaktidest tulenevaid kohustusi.[261]

Erik Kergandbergi sõnul on digitaaltõendite kontekstis antud konventsiooni puhul tegu ainsa rahvusvahelis-õigusliku dokumendiga, mida saab pidada tõsiseltvõetavaks.[262] Siiski nendib ta, et

---

[255] Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn, Juura 2007, lk 177

[256] Valjarevic, A., & Venter, H. S. A comprehensive and harmonized digital forensic investigation process model. Journal of forensic sciences 2015, 60(6), lk 1647

[257] Digitaleurope views on Law Enforcement Access to Digital Evidence http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2299&language=en-US&PortalId=0&TabId=353 (29.01.2017), lk 3

[258] *Ibid.*

[259] Arvutikuritegevusvastane konventsioon. RT II 2003, 9, 32

[260] *Ibid.*,artikkel 19

[261] *Ibid.*

[262] Kergandberg (2013) *supra* nota 166, lk.255

kuigi Eesti on materjaalõigusliku osa konventsioonist suuremalt jaolt karistusõigusesse üle võtnud, siis menetlusõiguslike põhimõtetega on siiani veel olulisi probleeme, sest meil puudub puudub elektrooniliste tõendite kogumiseks spetsiifiline erikord.[263] Ometi näeb Arvutikuritegevusvastene konventsioon ette, et konventsiooniosaline peab elektrooniliste tõendite kogumiseks nägema ette spetsiifilise korra.[264]

Peamiselt esineb digitaalsete tõenditega rohkelt materiaal- ja menetlusõiguslikke probleeme, sest praktikas puuduvad kuritegude uurimiseks interneti spetsiifilised põhiõiguste riiveks sätestatud pädevused ning seega menetlejatel endiselt võimalik kasutada neid õigusi, mis on varasemalt kehtestatud klassikalise kirjavahetussaladuse ning telefonikommunikatsiooni saladuse riive lubamiseks.[265]

Digitaaltõendite puhul tavaliste tõendite reguleerimiseks kasutavate normide rakendamine erinevaid probleeme nii tõendite mõistetavuse kui rakendamise kohapealt.[266] Näiteks on Eesti Advokatuur tõdenud, et tavatõenditele kohaldatavad normid ei taga digitaalse teabe puhul piisavalt isikute menetlusõigusi ega ka tõendite usaldusväärsust ning kontrollitavust. [267] Samuti on Eesti kohtutes probleemiks see, et ekspertiisi käigus leitud tõendid, nagu näiteks internetiväljavõtteid, arvuteid ja andmekandjaid ei ole sageli võimalik kohtus esitleda.[268]

Kuna digitaalset informatsiooni on väga kerge mõjutada, oleks mõistlik eeldada, et elektroonilisi tõendeid võib koguda ainult isik, kellel on spetsiaalsed teadmised. Siiski ei näe Eesti õigus ette, et menetleja kes otsib arvutiüsteemidelt või andmekandjatelt digitaalseid tõendeid, peaks omama spetsiaalset haridust või oskusi.[269]

Kohtupraktikas on tavaline, et tõendamiseks kasutatakse arvutiväljatrükke ning elektrooniliste kirjade väljatrükke.[270] Riigikohus on avaldanud arvamust, et juhul kui kriminaalasjas on

---

[263] *Ibid.*

[264] Arvutikuritegevusvastane konventsioon. RT II 2003, 9, 32. Artikkel 14, p2

[265] Kergandberg (2013) *supra* nota 166, lk 255

[266] Trehver, J. Arvamus Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõule (295 SE) https://www.riigikogu.ee/download/28f38ff9-5083-4d44-9838-b9b0b467a29a (15.01.2017) lk 10

[267] *Ibid.*, lk3

[268] Reinthal, T. Küberkuritegevuse kohtupraktika Eestis. Riigikohus, 2009. www.riigikohus.ee/vfs/1275/Kyberkuritegevus%202009.pdf (15.01.2017) lk 12

[269] Laurits, E. Criminal procedure and digital evidence in Estonia. Digital Evidence and Electronic Signature Law Review, 2016 (13) lk 119

[270] §123, p5. Dokument ja asitõend. Kriminaalmenetlusseadustiku kommenteeritud väljaanne. Juura, Tallinn 2012

küsimuseks kirja võimalik päritolu, tuleb vältimatult uurida selliseid andmeid kajastavaid andmekandjaid.[271] Seevastu Saksamaa kohtupraktikas ollakse seisukohal, et arvutiväljatrükil on märksa madalam tõenduslik väärtus võrreldes andmekandjal oleva teabega.[272]

Autor nõustub Orin S Kerriga, kelle arvates saab põhiseaduslikke väärtuseid kasutada kübermaailma puhul ainult ainult siis, kui neid võrdustatakse füüsilise maailmaga ning sealhulgas peaksid füüsilise maailma reeglid arvestama ka kübermaailmaga eripäradega.[273] Kuigi teaduse ja tehnika arenedes peaks asitõendite osatähtsus kasvama, siis Eesti kohtumenetluses on viimaste aastate jooksul olnud pigem vasupidine tendents.[274] See on tingitud sellest, et meil puudub ambitsioonikas riiklik programm, mis oleks suunatud kuritegude tehnilise uurimise arendamisele ja täiustamisele.[275]

Käesoleva töö autor eelneva põhjal jõudnud järeldusele, et digitaaltõendite küsimus tuleks kiiremas korras lahendada. Advokaat Leon Glikman on väitnud et kriminaalmenetlus on ainus õigusharu Eestis, kus viimase 25 aasta jooksul ei ole läbi viidud põhjalikku õigusreformi ning nendib, et mida aeg edasi, seda raskem on menetluskorda muuta.[276] Ka endine peaprokurör Norman Aas on tundnud muret Eesti kriminaalmenetluse arengu vastu ning leidnud, et tõde ja õigus pole alati piisavalt legitimeeritud menetluslike puudujääkide tõttu[277] Siinkohal on töö autor nõus Uno Lõhmusega, kes on öeldnud: „Tõendamissüsteem tuleks viia loogilistele alustele ja tagada selle üksikelementide süsteemne käsitlus.“ [278]

3.3. Elektrooniliste sideandmete kogumine kriminaalmenetluses

Sõnumite sideandmed on sõnumite sisuga kaasnev kõrvalprodukt, mida riigid hakkasid esmakordselt koguma 2000-ndate aastate alguses.[279] Kui varem peeti metaandmeid madala väärsusega informatsiooniks, siis nüüdseks on see arvamus muutunud, sest metaandmed

[271] RKKKo 3-1-1-104-05
[272] Eisenberg, U. Beweisrecht der StPO. Spezialkommentar. 7. Aufl. München: beck 1999, S 818
[273] Kerr, O. S. The Problem of Perspective in Internet Law. Georgetown Law Journal 2003 (91.2) lk 370
[274] § 124, p1. Dokument ja asitõend.Kriminaalmenetlusseadustiku kommenteeritud väljaanne. Juura, Tallinn 2012
[275] *Ibid.*
[276] Glikman, L. Igikestev mure põhiõiguste kaitstuse pärast. Eesti Päevaleht 2016. epl.delfi.ee/news/arvamus/igikestev-mure-pohioiguste-kaitstuse-parast?id=75525191 (09.04.2017)
[277] Aas, N. Austatud lugeja. Juridica 2011(8), lk 557
[278] Lõhmus, U. Tõendi lubatavus ja välistamine kriminaalmenetluses- Kui loogiline on Eesti tõendamissüsteem? Juridica 2014 (4), lk 699
[279] Hosein. *supra* nota 139, lk 1075

sisaldavad informatsiooni selle kohta, kus me oleme olnud, mida oleme lugenud ning millest me huvitume.[280]

Kui kirjapostiga jääb postiasutustele teada vaid saaja ja saatja aadress, siis elektrooniliste sõnumite puhul on informatsiooni palju enam. Näiteks Ameerika Ühendriikides ollakse siiski arvamusel, et ka ilma kirjaümbriku sisu vaatamata on ka ümbrikul olev teave väga olulise tähtsusega, sest see annab teavet selle kohta, mis ajal keegi kelelgagi suhtles ning seetõttu on Ameerika postiteenust vahendavatel ettevõtetele pandud kohustus teha kõikidest kirjaümbrikutest fotod.[281]

Arvutitega seotud kuriteod võivad sarnaselt teiste kuritegudega jätta maha jälje, mis omakorda võimaldab ekspertiisi käigus leida lisainformatsiooni või viiteid kuritöö koosseisu kohta.[282] See ei kehti siiki ainult arvutite kohta, vaid ka kogu elektroonilise suhtluse kohta. Näiteks annavad mobiilsidevõrgu metaandmed informatsiooni selle kohta, milliselt numbrilt kõne valiti, kellele helistati ning kaua kõne kestsis ning e-kirjade puhul on metaandmete abil võimalik kindlaks teha saaja ja saatja asukohad ning sõnumi saatmise aeg.

3.3.1 Sideandmete kogumise õiguslik regulatsioon Euroopas

Andmeprivaatsust saab Euroopa Liidus pidada üheks vanimaks inimõiguste üldsuunaks.[283] Kuigi algselt oli Euroopa Kohus üheks valitsevaks institutsiooniks, kes tegeles õiguste loomisega, siis alates 1990-ndatest aastatest hakkasid ka Euroopa seadusandjad aktiivsemalt tegutsema.[284]

Tehnoloogiline areng ning isikute ja teenuste vaba liikumine on andnud tõuke organiseeritud kuritegevusele, aga samas teinud raskeks ka selle vastu võitlemise[285] Sideandmete sälitamine toimub enamasti seetõttu, et teenuseosutajad soovivad sellega end kaitsta häkkerite ja pettuste eest. Euroopa Parlament ja Nõukogu võtsid 2006. aastal vastu direktiivi, mis käsitles üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate

[280] *Ibid*., lk1077

[281] Nixon, R. U.S. Postal Service Logging All Mail for Law Enforcement- www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?pagewanted=all (18.02.2017)

[282] Väli, M. Kriminalistikaekspertiisid. Sisekaitseakadeemia 2013, lk 388

[283] Bignami, F. Privacy and law enforcement in the European union: the data retention directive. Chicago Journal of International Law 2007 (8), lk 233

[284] Ibid.

[285] Goold, B.J., Neyland, D. New Directions in Surveillance Privacy. Willian Publishing 2009,lk 77

tegevusega kaasnevate või nende töödeldud andmete säilitamist.[286] Antud direktiivi kehtestamise ajendiks olid nii Ameerikas toimunud 9/11 terrorirünnakud kui ka Madriidis ja Londonis toimunud pommiplahvatused.[287]

Direktiivi artikkel 5 pani liikmesriikidele kohustuse säilitada erinevaid andmeid, nagu näiteks helistaja telefoninumberid, valitud numbrid, e-posti ja interneti-telefonide puhul nende kasutajatunnused ning muud andmed, millega saab kindlaks määrata side kuupäeva, aja ja kestuse, aga sealt jäeti välja sõnumite sisuandmed, nagu näiteks telefonikõnede ülestähendused.[288] Antud direktiiv tekitas koheselt negatiivset vastukaja, sest kommunikatsiooni liiklus- ja asukoha andmete säilitamise kohustus tõi kaasa intentsiivse sekkumise põhiõigustesse.[289]

Kaheksa aastat pärast direktiivi kehtestamist tunnistas Euroopa Kohus liidetud kohtuasjades C-293/12 ja C-594/1 antud direktiivi kehtetuks, sest leidis direktiiviga kaasneb ebaproportsionaalne piirang Euroopa Liidu põhiõiguste harta artiklite 7 ja 8 kohta, mis sätestavad eraelu ja isiku andmete kaitse.[290] Kuna direktiiv 2006/24/EÜ kuulutati kehtetuks, hakkas sideandmete kogumist reguleerima direktiiv 2002/58/EÜ, mis käsitleb isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris.[291] Antud direktiivi artikkel 5 kohaselt peavad liikmesriikd tagama üldkasutatava sidevõrgu ja üldkasutatavate elektrooniliste sideteenuste kaudu toimuva side ning ka sellega seotud liiklusandmete konfidentsiaalsuse.[292]

Euroopa Kohus on hiljutises kohtuotsuses Tele2 Sverige ja Watson jõudnud seisukohale, et sideandmete abil saab teha väga täpseid järeldusi isikute eraelu kohta, sest sideandmed võimaldavad informatsiooni isikute igapäevaelu harjumuste, alalise või ajutise elukoha,

[286] Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006 , mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ

[287] Vedaschi, A., Lubello, V Data retention and its implications for the fundamental right to privacy. Tilburg Law Review. 2015, 20(1) lk 18

[288] DeSimmone, C. Pitting Karlsruhe against Luxembourg-German Data Protection and the Contested Implementation of the EU Data Retention Directive. German Law Journal 2010 (11), lk 300

[289] Lõhmus, U. Elektroonilise side andmete säilitamise lõpetamata saaga. Juridica 2015 (10), lk 735

[290] EKo 08.04.2014 Liidetud kohtuasjades C‑293/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform,Commissioner of the Garda Síochána,
Iirimaa, The Attorney General ning C‑594/12 Digital Rights Ireland Ltd Kärntner Landesregierung, Michael Seitlinger,Christof Tschohl jt.

[291] Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris

[292] Ibid., artikkel 5

igapäevaste või muude liikumiste, tegevuste ja sotsiaalsete suhete kohta. Kohus rõhutas, et selliste andmete põhjal saab koostada asjaomaste isikute profiili, mis on aga sama tundlik teave, kui sideseansi sisu ise.[293] Lisaks oli kohus seisukohal, et kuritegevuse vastu võitlemise eesmärgil võib anda juurdepääsu vaid nende isikute andmetele, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises, või kui isik on sellise kuriteoga seotud.[294]

3.3.2. Sideandmete kogumine Eestis

Riigikohus on tõdenud, et sideandmete kogumine on kriminaalmenetlues väga vajalik vahend, sest see võimaldab koguda tõendeid isikute suhtlemise fakti ja viibimiskoha kohta.[295] Näiteks on kohtupraktikas tõdetud, et IP-aadressi võimaldab identifitseerida arvutit, kust e-kiri teele saadetud ja samuti on jälgitav kirja kulgemine. [296]

Eesti on nende riikide hulgas, kes ei ole pärast eelnimetatud Euroopa Kohtu otsust direktiivist üle võetud sätteid kehtetuks tunnisatnud.[297] Samas on leitud, et elektrooniline suhtluse laia kasutatavuse tõttu, oleks siiski oluline kaaluda, kas põhiõiguste ja –vabaduste paremaks tagamiseks oleks sideandmete kogumisele vaja kehtestada täpsem regulatsioon.[298]

Kahjuks ei ole avaldatud värskeid andmeid selle kohta, kui palju kommunikatsiooni sideandmeid sideettevõtetelt küsitakse. Tabelis nr 1 nähtub, et 2008. aastal nõuti sideandmeid kokku 4490. korral. Siiski võib arvata, et praegusel hetkel võib see arv olla kordades suurem, sest elektroonilise suhtlus on muutumas üha populaarsemaks.

---

[293] EKo 21.12.2016, liidetud kohtuasjad C-203/15 Tele2 Sverige AB v. Post- och telestyrelsen ja C-698/15 Secretary of State for the Home Department v. Tom Watson, Peter Price, Geoffrey Lewis.
[294] Ibid.
[295] RKKK 3-1-1-51-14 p22
[296] RKKKo 3-1-1-104-05 p6.2
[297] Lõhmus (2015) *supra* nota 290, lk 735
[298] Õiguskantsleri 05.12.2012.a. arvamus kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõule (295 SE). www.riigikogu.ee/?op=emsplain&page=pub_file&file_id=52727c38-5c97-433d-bc25-eda7af8db244& (20.12.2016) lk 7

Country	Requests	Population (m)	Requests/m population
Cyprus	34	0.761	45
Czech Republic	131560	10.323	12,744
Germany	13348	82.12	163
Denmark	3605	5.447	662
Estonia	4490	1.343	3,343
Greece	584	11.172	52
Finland	4010	5.27	761
France	538437	62.277	8,646
Ireland	14095	4.422	3,187
Latvia	16862	2.271	7,425
Malta	867	0.413	2,099
Slovenia	282	2.013	140
UK	470222	61.073	7,699

Tabel 1. Euroopa Liikmesriikide sideandmete taolused millioni isiku kohta 2008. aastal[299]

Elektroonilise side seadus, mis võeti üle direktiivi 2006/24/EÜ kohaldamiseks, annab endiselt pika loetelu selle kohta, milliseid andmeid peavad sideettevõtjad säilitama.[300] Riigikohus on nentinud, et hoolimata sellest, et antud direktiiv on kehtetu, ei tähenda see seda, et ka riigisisene regulatsioon oleks automaatselt kehtetu.[301] Riigikohus märkis, et riigisisese regulatsiooni kujundamisel on seadusandjal siiski teatud ulatuses kaalutlusõigus.[302]

Seetõttu peavad sideettevõtjad Elektroonilise side seaduse kohselt säilitama andmeid selleks, et oleks võimalik teha järgnevaid toiminguid:

1) sideallika seiramine ja tuvastamine;
2) side sihtpunkti tuvastamine;
3) side kuupäeva, kellaaja ja kestuse kindlaksmääramine;
4) sideteenuse liigi kindlaksmääramine;
5) sideteenuse kasutaja terminalseadme või oletatava terminalseadme kindlaksmääramine;
6) terminalseadme asukoha kindlaksmääramine.[303]

Vastavalt ESS paragrahvi 111^1 lõikele 2 peavad interneti-ühenduse, elektronposti ja interneti-telefoni teenust osutavad isikud sälitama järgmiseid andmeid:

[299] Brown, I. Communications data retention in an evolving internet. International Journal of Law and Information Technology 2011, 19 (2), lk 100
[300] ESS RT I, 17.05.2016, 2
[301] RKKKo 3-1-1-51-14, p 21
[302] *Ibid.*
[303] ESS RT I, 17.05.2016, 2 §111^1

1) sideettevõtja poolt eraldatud kasutajatunnused;

2) telefoni- või mobiiltelefonivõrku siseneva side kasutajatunnus ja telefoninumber;

3) kliendi nimi ja aadress, kelle nimele Interneti-protokolli aadress, kasutajatunnus või number olid side toimumise ajal eraldatud;

4) Interneti-telefoni kõne kavandatud vastuvõtja kasutajatunnus või number;

5) kavandatud vastuvõtva kliendi nimi, aadress ja kasutajatunnus elektronposti ning Interneti-telefoni teenuse korral;

6) Interneti-seansi alguse ja lõpu kuupäev ning kellaaeg konkreetse ajavööndi järgi koos Interneti-protokolli aadressiga, mille on kasutajale eraldanud Interneti-teenuse osutaja, ja kasutajatunnusega;

7) elektronposti või Interneti-telefoni teenuse kasutamise alguse (log-in) ja lõpu (log-off) kuupäev ning kellaaeg konkreetse ajavööndi järgi;

8) kasutatud Interneti-teenus elektronposti ja Interneti-telefoni teenuse korral;

9) helistaja number sissehelistamisega Interneti-ühenduse korral;

10) digitaalne kliendiliin (Digital Subscriber Line – DSL) või mõni muu tunnus side algataja kohta.[304]

Kui varasemalt loeti sideandmete kogumist jälitustoiminguks, siis alates 01.01.2013 jõustunud kriminaalmenetluse seadustiku kohaselt ei loeta seda enam jälitustoiminguks ning seetõttu on tegemist tavapärase menetlustoiminguga. Antud muudatust käsitlenud eelnõus toodi ühe muudatuse põhjuseks asjaolu, et kuigi sidevahend ei ole alati kuriteo sooritamise vahendiks, võivad need andmed olla siiski kuritegude tõendamisel olulise tähtsusega.[305]

U. Lõhmus on tõdenud, et kuna direktiiv 2006/24/EÜ on kehtetu, on seetõttu ka kommunikatsiooni liiklus- ja asukohaandmete kogumist ja säilitamist reguleerivad normid on väga oluliste puudustega, tuues välja järgnevad põhjendused:

- andmete säilitamine lähtub eeldusest, et kõik elektroonilise side teenuse kasutaja on potentsiaalsed õigusrikkujad;
- sideettevõtted on kohustatud edastama andmeid sõltumata sellest, kui kui kerge või raske kuriteoga on tegemist;

[304] *Ibid.,* lg 2

[305] Siitam-Nyiri, K. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 175 www.riigikogu.ee/download/0eb6bebb-9abf-470f-9842-abe51795206a lk5-6 (14.04.2017)

- isikute asukoha jälgimine reaalajas on jälitustegevus, kuid asukohaandmete ja isiku liikumiste tagantjärele uurimist loetakse tavaliseks menetlustoiminguks;
- kui sõnumi kaasaskantavasse jälgimisseadmesse ülekandmiseks tuleb sideettevõttele esitada taotlus koos kohtu loaga, siis sõnumi ülekandmine tsentraalsesse jälgimisseadmesse toimub ilma taotluse ja kohtu loata;
- puudub kontroll kommunikatsiooni liiklus- ja asukohaandmete riigiasutustele kätte saadavaks tegemise üle, sest nende kohta ei peeta arvestust;
- kuigi isik võib teada saada, et tema sideandmeid on kasutatud kriminaalmenetluse, siis seadus isiku teavitamist andmete taotlemisest ja töötlemisest ei reguleeri.[306]

Üldiselt ollakse Euroopas valitseval arvamusel, et sideandmete kogumine eeldab kohtu luba.[307] Näiteks leidis hiljuti Euroopa Kohus, et sideandmetele juurdepääsu saamise eeltingimuseks peab olema kohtu või sõltumatu haldusasutuse eelnev kontroll.[308]

Kriminaalmenetluse seadustiku paragrahv 90^1 lõige 2 sätestab, et olukorras, kus uurimisasutus tahab sideettevõtjalt saada sõnumi edastamise faktiga seotutud andmeid, võib teha teha sideettevõtjale pärnigu üksnes prokuratuuri loal kohtueelses menetluses või kohtu loal kohtumenetluses.[309] Prokuratuuriseaduse paragrahvi 1 lõike 1^1 kohaselt peab prokuratuur oma seadusest tulenevate ülesannete täitmisel olema sõltumatu.[310] Siiski ei saa prokuratuuri ei pidada sõltumatuks haldusasutuseks, sest prokuratuuri ülesandeks on juhtida kohtueelset menetlust ning esindada kohtus riikliku süüdistust.[311] Samuti välistab prokuratuuri sõltumatuse asjaolu, et andmeid kogutakse prokuröri käes oleva kriminaalasja tarbeks.[312] Seetõttu peaks ka kohtueelses menetluses olema sideandmete kogumiseks kohtu luba. Ka Euroopa inimõiguste kohus on tõdenud, et kohtulik kontroll pakub parimad tagatised sõltumatuse, erapooletuse ja kohase protseduuri osas.[313]

[306] Lõhmus, U. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. Juridica 2016, (10) , lk 701-702
[307] Lott, *supra* nota 129, lk 25
[308] EIKo Liidetud kohtuasjad Tele2 Sverige AB versus Post- och telestyrelsen((C-203/15) ja Secretary of State for the Home Department versus Tom Watson jt (C-698/15)
[309] KrMS RT I, 31.12.2016, 46
[310] ProkS RT I, 17.12.2015, 62
[311] Ginter, G., Schasmin, P. Lahendite Tele2 Sverige ja Digital Rights Ireland mõju sideandmete mugavkasutusele Eestis.Juridica, 2017 (1), lk 48
[312] *Ibid.*
[313] EIKo 47143/06 *Roman Zakharov V. Russia* p 233

Autor nõustub siinkohal õiguskantsleriga, kella arvates olukorras, kus kriminaalmenetluses nõuavad menetlejad sideettevõtjalt välja sideandmeid, sekkutakse kahtlemata isiku eraelu puutumatusesse ning selle riive intentsiivsust suurendab tõsiasi, et antud meedet on võimalik kasutada väga laialdaselt.[314]

Samas on käesoleva töö autor seisukohal, et peale eraelu puutumatuse riive, esineb sideandmete kogumise puhul ka sekkumine sõnumite saladusse. Nagu autor eelnevalt leidis, on sideandmed osa kommunikatsioonist, mida tuleb kaitsta sõnumiga samaväärselt. Kuigi sideandmed on kuritegude uurimisel väga olulise tähtsusega, ei tohiks nende kasutamine tulla siiski põhiõiguste arvelt.[315] Hoolimata tõsiasjast, põhiseaduse ja siseriikliku kohtupraktika kohaselt võib sideandmete kogumine olla siseriiklikus kontekstis õiguslik, läheb see siiski vastuollu Euroopas valitsevate põhimõtetega.

Ka õiguskantsler Ülle Madise on tõdenud, et praegune sideandmete töötlemise regulatsioon on oluliste puudustega ning sideandmete töötlemiseks tuleks täiendada õiguslike garantiisid.[316] Madise on arvamusel, et sideandmete väljanõudmisega kaasneb kriminaalmenetluses eraelu puutumatuse riive ning sealhulgas suurendab riive intensiivsust tõsiasi, et sideandmeid on võimalik kasutada sõltumata menetletavast kuriteost ja kõigi isikute suhtes.[317] Ka Euroopa kohus on leidnud, et sideandmete kogumine peab läbima väga põhjaliku kontrolli nii siseriiklikul tasandil, aga samas ka inimõiguste konventsiooni alusel.[318]

---

[314] Madise, Ü. Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus http://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf lk 7 (04.04.2017)

[315] Tuulik, M-E. Anvelt: sideandmete kasutamine ei tohi tulla isikute põhiõiguste arve. Justiitsministeerium www.just.ee/et/uudised/anvelt-sideandmete-kasutamine-ei-tohi-tulla-isikute-pohioiguste-arvel (15.11.2016)

[316] Madise, Ü. Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus. www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (03.12.2016) lk 7

[317] *Ibid.*

[318] EIKo Szabó And Vissy v. Hungary *37138/14* p. 70

Kokkuvõte

Sõnumite saladus on rahvusvaheliselt tunnustatud põhiõigus, mille tunnustamist võib leida erinevate riikide põhiseadustes kui ka erinevates rahvusvahelistes dokumentides nagu näiteks Euroopa Inimõiguste ja Põhivabaduste konventsioonis ning Euroopa Liidu Põhiõiguste hartas.

Ka Eesti Vabariigi Põhiseaduses on sätestatud sõnumisaladuse printsiip ning sõnumisaladust on peetud põhiõigusena juba esimese põhiseaduse sünnist saadik. Ka Nõukogude Liidu aegsel perioodil oli sõnumite saladuse õigus seadusega sätestatud, iseasi on aga see, mil määral sellega ka tolle aegsed julgeolekuorganid arvestasid. Näiteks pärineb nõukogude ajast nali, mille kohaselt on mikrobetooni koostisosaks 80 protsenti mikrofone ja 20 protsenti betooni.[319]

Kuigi Euroopas peetakse sõnumisaladust enamasti era- ja perekonnaelu osaks, siis Eesi Vabariigi Põhiseaduses on sõnumite saladusele pühendatud eraldi paragrahv. Esmapilgul ei tundugi antud põhiõigustele eraldi paragrahvi andmine problemaatiline. Siiski näeb selline käsitlus ette erineva kaitserežiimi. Kui põhiseaduse kohaselt ei ole era- ja perekonnaellu sekkumiseks vaja kohtu luba, siis sõnumisaladuss sekkumise üldtingimuseks on kohtu volitus. See aga toob vajaduse piiritleda sõnumisaladusse kaitseala eriti täpselt. Kahjuks toob kaitseala täpne piiritlemine kaasa olulisi probleeme ning praktikas ei pruugi arvestada tegeliku eluga.

Põhiseaduse isikulise kaitseala määratlemine praktikas probleeme ei tekita, sest see kohaldub üheskoos nii füüsilistele kui ka juriidilistele isikutele. Kahjuks ei saa seda väita esemelise kaitseala kohta. Autor leidis, et kuna põhiseaduslik sõnumisaladuse kaitse kohaldub ainult üldkasutatavatele side süsteemidele ning sealt jäävad välja kõik sellised sõnumid, mida üldkasutataval teel ei edastada. Kasutatavateks sidevahenditeks võivad seejuures olla näiteks raadioside või muu kinnine elektroonilise sidesüsteem.

Ka sõnumite saladuse ajaline kaitseala hõlmab endas mitmeid küsitatavusi. Nii on siseriiklikus õiguskirjanduses ja Riigikohtu praktikas tõlgendatud sõnumisaladuse ajalist kaitseala kitsendavalt, sest on leitud, et põhiseadus sätestatud sõnumisaladuse printsiipi on võimalik grammatiliselt tõlgendada ainult selliselt, et sellega on kaitsud vaid edastamisprotsessis olevaid

[319] Lõhmus (2008) *supra* nota 15 lk462

sõnumid. Töö autor jõudis seisukohale, et grammatiliselt on põhiseaduses sätestatud sõnumite saladust õigust võimalik tõlgendada ka märksa laiemalt.

Uurides Euroopa Inimõiguste ja Põhivabaduste konventsiooni ning Euroopa Inimõiguste kohtu praktikat, leidis autor, et sõnumite saladus peaks kaitsma kommunikatsiooni tervikuna, sõltumata sellest kas sõnum on parasjagu edastamisel või juba vastu võetud. Sarnast lähenemist võib näha ka Euroopa Liidu Põhiõiguste harta inglise keelses versioonis. Harta eestikeelne tõlge aga kitsendab sõnumite saladuse ajalist kaitseala sarnaselt põhiseadusega.

Eriti mõjutab sõnumite saladuse ajalise kaitseala kitsendamine tänapäeva kommunikatsioonitehnoloogiat. Elektroonilise sõnumid on järjest enam asendamas kirjaümbriku teel edastavat teavet. Seda just põhjusel, et valdavalt on elektrooniliste sõnumite eelisteks kiirus ning võimalus edastada suurt andmehulka korraga, arvestamata sealjuures saatja ja adressaadi vahelist kaugust.

Kriminaalmenetluse raames võib sõnumite saladusse sekkumine sõnumi teeloleku ajal olla tõenäoline vaid kirjaümbriku teel edastatava teabe või telefonikõnede pealtkuulamise korral. Näiteks võivad riiklikud õiguskaitseorganid kohtu loal lugeda jälitustoimingu käigus toimingule allutatud isiku poolt postiasutusele edastamiseks antud teavet. Elektrooniliste sõnumitega on teine lugu, sest nende edastamisprotsess kestab äärmiselt lühikest aega ning edastamise ajal on sõnumite saladusse sekkumine ebatõenäoline.

Töös analüüsitud kohtupraktika lubab järeldada, et edastamisprotsessi läbinud elektroonilised sõnumid, mis on salvestatud andmekandjale või serverisse, ei kuulu sõnumite saladuse õiguse, vaid hoopis perekonna- ja eraelu kaitse alla. Kui sõnumite saladuse õigussesse sekkumine toimub alati kohtu loal, siis perekonna- ja erallu sekkumine on teatud juhtudel võimalik ka ilma kohtu loata. Siiani on sõnumite saladuse printsiibi kitsast ajalist kaitseala põhjendatud sellega, et see tuleneb põhiseaduse grammatilisest tõlgendusest ning laiema tõlgenduse puhul oleks õiguskaitseorganiel märksa keerulisem elektrooniliste sõnumitega tutvuda.

Käesoleva töö autor jõudis seisukohale, et tegemist ei ole siiski ainuvõimaliku tõlgendusega. Võttes arvesse inim- ja põhiõigusi sätestavaid õigusakte ja nende alusel välja kujunenud kohtupraktikat, tuleb sõnumite saladuse kaitseala kohaldada märksa laiemalt. Euroopa

õigusruumis valitseva arvamuse kohaselt kaitseb sõnumite saladus ka juba kohale toimetatud sõnumeid aga sealhulgas ka sõnumitega kaasnevaid sideandmeid.

Sõnumite sideandmed on elekrooniliste sõnumite üheks oluliseks osaks ning enamasti ollakse Euroopas seisukohal, et suhtluse sisu ja sideandmete eristamine ei digitaalajastul ei ole põhjendatud. Töö autor leidis, et siinkohal on aga Eesti seadusandja, kohtupraktika kui ka õiguskantsler vastupidisel arvamusel. Seetõttu kuuluvad põhiseaduse kitsa tõlgenduse kohaselt sideandmed siiski era- ja perekonnaelu puutumatuse alla.

Kuigi sõnumite saladuse kitsas tõlgenudus on õiguskaiteorgante huvides, ei paku see siiski põhjendatud tasakaalu põhiõiguse riive ja seda õigustavate huvide vahel.[320] Käesoleva töö autor nõustub Uno Lõhmusega, kes tõdes, et kuigi põhiseaduse muutmine on keeruline, on see siiski käesoleval juhul vajalik. Kiiremas korras tuleb sõnumite saladust riivavad seadused üle vaadata ning muuta need selgemaks ja konkreetsemaks.[321]

Kuna antud töö eesmärgiks oli uurida elektrooniliste sõnumite kaitseala kriminaalmenetluses, ei saanud autor käsitlemata jätta seda, kuidas kehtiva kriminaalmenetluse kohaselt toimib sõnumite pealtvaatamine ning arvutisüsteemide ja pilveteenustel salvestatud sõnumite läbiotsimine.

Autor leidis, et elektroonilise kommunikatsiooni jälgimise ja seda sisaldavate andmekandjate läbiotsimise regulatsioon vajab täiendamist, kuna see ei arvesta tänapäevase kommunikatsioonitehnolgoogiaga. Kuigi elektroonilised andmekandjad ja pilveteenused võivad peaaegu igas kriminaalmenetluses olla olulise tähtsusega, ning neid tuleb vaadelda füüsiliselt maailmast erinevalt, ei ole seadusandja koostanud nende kogumiseks ja pealtvaatamieks eriregulatsiooni.

Autor jõudis järeldusele, et elektrooniliste sõnumite pealvaatamine või nende kogumine jälitustoimingutega on praktikas ebaselge. Praegused õigusaktid vajavad märksa täpsemat regulatsiooni. Sealhulgas on vaja ka senisest tõhusamaid menetlusgarantiisid, sest jälitustoimingute üle tehtav kontroll on puudulik.

[320] Lõhmus (2016) *supra* nota, 17 lk 183
[321] Lõhmus (2008) *supra* nota, 15 lk472

Praktikas tekitab probleeme kehtiv läbiotsimisregulatsioon, mis puudutab elektrooniliste sõnumite otsimist arvutisüsteemidelt, andmekandjatelt ning pilvteenustelt. Autor leidis, et kuigi digitaalsete andmete otsimine erineb füüsiliste asjade otsimisest, puudub kriminaalmenetluses digitaalsete andmete läbiotsimiseks eriregulatsioon. Eriregulatsiooni loomine on ausa kohtumenetluse tagamiseks siiski vajalik.

Kokkuvõtvalt on käesoleva töö autor seisukohal, et põhiõiguste tagamiseks tuleb tänapäeva infotehnoloogia ajastul kohelda elektroonilisi sõnumeid sõnumite saladuse eesmärgist tulenevalt samal tasemel nagu füüsilisi sõnumeid. Teisalt on autor arvamusel, et ka lektrooniliste sõnumite kogumine ja nende tõenditena kasutamine tuleb muuta kriminaalmenetlusõiguses senisest spetfiisilisemaks. Õigus peab käima kaasas tehnoloogiaga.

Abstract

ISSUES RELATED TO THE SECRECY OF ELECTRONIC MESSAGES IN CRIMINAL PROCEEDINGS

This topic of the Master's thesis is „Issues Related To The Secrecy Of Electronic Messages In Criminal Proceedings**"** and the hypothesis is formulated as follows:

„Paragraph 43 of The Constitution of the Republic of Estonia, protecting the secrecy of messages, is not wide enough to to protect the secrecy of electronic messages in criminal procedure."

Secrecy of letters is a fundamental right that is internationally recognized by many constitutions. It is also enacted by international documents, such as the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union which protect communication in general. Its main goal is to protect private communication, regardless of what means of communication are used or whether messages are in transmission or already delivered. Also, the majority of the European judical area is of the opinion that the metadata of electronic messages should be protected at the same level as messages.

The Estonian constitution paragraph 43 also respects messages that are sent or received by post, telegraph, telephone or other commonly used means. According to the constitution, government institutions may derogate from this right if they are authorised by a court and if it is necessary to prevent a criminal offence, or to ascertain the truth in a criminal case.

According to the Estonian version of the constitution and Supreme court decisions, the secrecy of message only applies to the messages that are in transmission. If the messages have been delivered to the addressee, then another basic right that protects inviolability of private and family life, applies. In that case the court authorisation is not generally needed.

The author found that, this kind of a narrow interpretation of the constitution is problematic because electronic messages are transmitted whithin seconds, the secrecy of messages cannot apply to them. Also, because of the narrow interpretation of the secrecy of messages, the

Estonian constitiution sets a much weaker protection to the metadata of electronic messages. There are no adequate reasons why the principle of the secrecy of messages is not applied to electronic communication.

The constitution of Estonia protects only the messages which are sent by commonly used means. In that case it can be concluded that, the secrecy of messages does not apply to communication systems which are used by a limited number of communicators.

The author examined the Estonian code of criminal procedure and found out that, there are many uncertainties regarding the collection of electronic messages by law enforcement agencies. The author found that Estonia's national legislation does not sufficiently regulate the surveillance of and searching for electronic messages from computer systems, hard drives or computer clouds. Estonian legislation does not include special rules for obtaining and processing digital evidence in criminal procedure. Therefore the current regulation generates a lot of uncertainties and controversy.

The author concluded that the Estonian government needs to start resolving the issues related to the secrecy of electronic messages in criminal proceedings.

,

Kasutatud kirjandus

Teaduslikud allikad ning nendega võrdsustatud ajakirja Juridica artiklid ja AS Juura poolt välja antud raamatud:

1. Aas, N. Austatud lugeja. Juridica 2011(8) Lk 557-557;
2. Abel, W. Agents, Trojans and tags: The next generation of investigators. International Review of Law, Computers & Technology 2009 (23) Lk 99-108
3. Abel, W., Schafer, B. The German Constitutional Court on the Right in Confidentiality and Integrity of Information Technology Systems-A Case Report on BverfG. SCRIPTed 2009 6 (1) Lk 106-123
4. Abelson, H., Anderson, R., Bellovin, S.M., Benaloh, J., Blaze, M., Diffie, W., Gilmore, J., Green, M., Landau, S., Neumann, P.G. and Rivest, R.L. Keys under doormats: mandating insecurity by requiring government access to all data and communications. Journal of Cybersecurity 2015 (1) Lk 69-79
5. Annus, T. Riigiõigus. Juura, Tallinn 2006
6. Bignami, F. Privacy and law enforcement in the European union: the data retention directive. Chicago Journal of International Law 2007 (8) Lk 233-256
7. Brown, I. Communications data retention in an evolving internet. International Journal of Law and Information Technology 2011, 19 (2) Lk 95-109
8. Conley, C. Non-Content is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction, 54 Santa Clara Law Review 2014, 54 (4) Lk 821-842
9. Day, R. Let the Magistrates Revolt: A Review of Search Warrant Applications for Electronic Information Possessed by Online Services. U. Kansas Law Reviw. 2015 (64) Lk 491- 525
10. DeSimmone, C. Pitting Karlsruhe against Luxembourg-German Data Protection and the Contested Implementation of the EU Data Retention Directive. German Law Journal 2010 (11) Lk 291-317
11. Diffie, W., Landau, S. Communications surveillance: Privacy and security at risk. ACM Queue 2008, 7(8) Lk 42-47
12. Dripps, D. A. Dearest Property": Digital Evidence and the History of Private "Papers" as Special Objects of Search and Seizure. The Journal of Criminal Law & Criminology 2013, 103 (1). Lk 49-110

13. Garfinkel, S. L. Digital forensics research: The next 10 years 2007. Digital investigation 2010 (7).
14. Ginter, G., Schasmin, P. Lahendite Tele2 Sverige ja Digital Rights Ireland mõju sideandmete mugavkasutusele Eestis. Juridica 2017 (1) Lk 42-52
15. Glikman, L., Põhjendamatu sekkumine majandustegevusse ja jälitustegevus. Juridica 2011 (4) Lk 63-73
16. Hirsnik, E. Arvutikuritegevuse regulatsioon Eestis: karistusõiguse revisjoniga toimunud muudatused ja lahendamata jäänud probleemid. Juridica 2014 (8) Lk 611-624
17. Hosein, G., Palow, G.W. Modern safeguards for modern surveillance: An analysis of innovations in communications surveillance techniques, Ohio State Law Journal 2013, (74). Lk 1071-1104
18. Ibrahim, N., Al Naqbi, N., Iqbal, F.m., AlFandi, O. SIM Card Forensics: Digital Evidence. Annual Conference on Digital Forensics, Security and Law 2016 (3) Lk 218-234
19. Insa, F. The Admissibility of Electronic Evidence in Court (A.E.E.C.): Fighting against High-Tech Crime—Results of a European Study, Journal of Digital Forensic Practice 2007 (3) Lk 285-289
20. Irion, K. Privacy and Security: international communications Surveillance. Communications of the ACM 2009, 52 (2) Lk 26-28
21. Kaiser, A. B. German Federal Constitutional Court: German Data Retention Provisions Unconstitutional in Their Present Form. European Constitutional Law Review 2010 6(3) Lk 503-517
22. Kalmo, H. Põhiseaduse põkkumine Euroopa Liidu põhiõiguste hartaga. Juridica 2016 (3) Lk 147-164
23. Karovska-Andonovska, B. The Right To Secrecy Of Communications-Situations And Challenges. Journal of Process Management – New Technologies, International 2014, 2 (4) Lk 114-118
24. Kattan, I. R. Cloudy privacy protections: Why the Stored Communications Act fails to protect the privacy of communications stored in the cloud. Vanderbilt Journal of Entertainment & Technology Law 2010 (13) Lk 617-656
25. Kergandberg, E. Eesti kriminaalmenetlus: mõned rindeteated Juridica, 2013 (4) Lk 249-256
26. Kergandberg, E., Pikamäe, P., Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Tallinn, Juura 2012.

27. Kergandberg, E., Sillaots, M. Kriminaalmenetlus. Juura, Tallinn 2006
28. Kerr, O. Applying the Fourth Amendment to the Internet: A General Approach. 62 Stanford Law Review 2010, 62 (4) Lk 1005-1049
29. Kerr, O. S. Ex ante regulation of computer search and seizure. Virginia Law Review 2010, 96 (6) Lk 1241-1293
30. Kerr, O. S. Fourth Amendment Seizures of Computer Data. The Yale Law Journal 2010, 119 (4) Lk 700-724
31. Kerr, O. S. Search Warrants in an Era of Digital Evidence. 75 Mississippi Law Journal 2005 (85) Lk 85-145
32. Kerr, O. S. The Next Generation Communications Privacy Act 162 University of Pennsylvania Law Review 2014 (162) Lk 373-419
33. Kerr, O. S. The Problem of Perspective in Internet Law. Georgetown Law Journal 2003 (91.2) Lk 357–405
34. Kohls, S. J. Searching the Clouds: Why Law Enforcement Officials Need to Get Their Heads Out of the Cloud and Obtain a Warrant Before Accessing a Cloud Network Account. Case Western Reserve Journal of Law, Technology and the Internet 2012, 4(1) Lk 169-206
35. Laurits, E. Criminal procedure and digital evidence in Estonia. Digital Evidence and Electronic Signature Law Review, 2016 (13) Lk 113-120
36. Lõhmus U. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. Juridica 2016 (3) Lk 175-183
37. Lõhmus, U. Elektroonilise side andmete säilitamise lõpetamata saaga. Juridica 2015 (10) Lk 735-745
38. Lõhmus, U. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. Juridica 2016 (10) Lk 698-708
39. Lõhmus, U. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. Juridica, 2008 (7) Lk 462-472
40. Lõhmus, U. Põhiõigused kriminaalmenetluses. Teine, täiendatud ja ümbertöötatud väljaanne. Juura, Tallinn 2014
41. Lõhmus, U. Tõendi lubatavus ja välistamine kriminaalmenetluses- Kui loogiline on Eesti tõendamissüsteem? Juridica 2014 (4) Lk 690-699
42. Maruste, R. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn, Juura 2004,

43. Mason, S. Rethinking Concepts in Virtual Evidence. The Icfai Journal of Cyber Law 2008 (7) Lk 48-54
44. Murphy, M. H. Technological solutions to privacy questions: what is the role of law?. Information & Communications Technology Law 2016, 25(1) Lk 4-31
45. Narits, L. Õiguse entsüklopeedia. Tallinn, Juura 2007
46. O'Brien, M. Law, privacy and information technology: a sleepwalk through the surveillance society?. Information & Communications Technology Law. 2008, 17(1) Lk 25-35
47. Ortiz, J. C. Fighting Cybercrime in Europe: The Admissibility of Remote Searches in Spain.European Journal of Crime, Criminal Law and Criminal Justice 2014, 19 (4) Lk 1-33
48. Parmas, A., Pruks, P., Ruttu, M. Tractatus Terribiles: artiklikogumik professor Jaan Sootakki 60. jubeliks. Juura, Tallinn 2009 Saueauk, M. „Salajane kontroll". Sõnumisaladuse rikkumisest Nõukogude Liidus ja Eesti NSV-s" Tuna Ajalookultuuri ajakiri 2014 (2)
49. Podkowik, J. Privacy in the digital era–Polish electronic surveillance law declared partially unconstitutional. European Constitutional Law Review 2015 11 (03) Lk 577-595
50. Rondel, M. Informatsioonilise enesemääramise õigus ja jälitustegevus. Juridica 2016 (7) Lk 709-717
51. Selinsek, L. Electronic evidence in the Slovene Criminal Procedure Act. Digital Evidence & Electronic Signature Law Review 2010, (7) Lk 77-86
52. Sootak, J., P. Pikamäe,P. Karistusseadustik : kommenteeritud väljaanne. Tallinn, Juura, 2015
53. Tikk, E., Nõmper, A. Informatsioon ja õigus. Tallinn, Juura 2007
54. Tokson, M. The Content/Envelope Distinction in Internet Law. William & Mary Law Review 2009, 50, (6) Lk 2105-2716
55. Trepel, S. Digital Searches, General Warrants, and the Case for the Courts. Yale Journal of Law andTechnology 2007 (10) Lk 120-150
56. Valjarevic, A., & Venter, H. S. A comprehensive and harmonized digital forensic investigation process model. Journal of forensic sciences 2015, 60 (6) Lk 1467-1483
57. Vedaschi, A., Lubello, V. Data retention and its implications for the fundamental right to privacy. Tilburg Law Review 2015 20 (1) Lk 14-34

Raamatud:

58. Casey, E. Digital evidence and computer crime: Forensic science, computers, and the internet. Academic press, 2011
59. Eisenberg, U. Beweisrecht der StPO. Spezialkommentar. 7. Aufl. München: beck 1999
60. Finn, R.L., Wright, D., Friedewald, M. European Data Protection: Coming of Age. Springer Netherlands 2013
61. Goold, B.J., Neyland, D. New Directions in Surveillance Privacy. Willian Publishing 2009,
62. Harris, D. J., O'Boyle, M., Bates, E., Buckley, C. Harris. O'Boyle & Warbrick: Law of the European convention on human rights. Oxford University Press, USA 2014
63. Parmas, A , Randma, P., Laos, S., Lillsaar, T., Kallin, J., Lind, S., Tamm, I. Kohtute aastaraamat 2015. Riigikohtu kommunikatsiooniosakond 2016
64. Pearson, S., Yee, G. Privacy and Security for Cloud Computing. Springer London 2013
65. Väli, M. Kriminalistikaekspertiisid. Sisekaitseakadeemia 2013

Eesti õigusaktid:

66. Eesti Vabariigi Põhiseadus RT, 09.08.1920, 113/114, 243
67. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt RT II 1994, 10, 11
68. Lapse õiguste konventsioon RT II 1996, 16, 56
69. Inimõiguste ja põhivabaduste kaitse konventsioon RT II 2000, 11, 57
70. Arvutikuritegevusvastane konventsioon RT II 2003, 9, 32
71. Inimõiguste ja põhivabaduste kaitse konventsioon RT II 2010, 14, 54
72. Postiseadus RT I, 12.07.2014, 107
73. Eesti Vabariigi Põhiseadus RT I, 15.05.2015, 2
74. Elektroonilise side seadus RT I, 17.05.2016, 2
75. Prokuratuuriseadus RT I, 17.12.2015, 62
76. Kriminaalmenetluse seadustik RT I, 31.12.2016, 16
77. Karitusseadustik RT I, 31.12.2016, 14

Õigusaktide kommenteeritud väljaanded:

78. Kergandberg, E., Pikamäe, P. Kriminaalmenetluse seadustik. Kommenteeritud väljaanne. Tallinn, Juura 2012
79. Madise, Ü., Aaviksoo, B., Kalmo, H., Mälksoo, L., Narits, R., Pruks, P., Vinkel, P. Eesti Vabariigi Põhiseadus. Kommenteeritud väljaanne. http://www.pohiseadus.ee/
80. Peers,S., Hervey, T.K., Kenner, J., Ward, A. The EU Charter of Fundamental Rights: A Commentary. Hart Publishing, 2014
81. Sootak, J., Pikamäe, P. Karistusseadustiku kommenteeritud väljaanne. Tallinn, Juura 2015

Euroopa Liidu ja rahvusvahelised õigusaktid:

82. Convention for the Protection of Human Rights and Fundamental Freedoms (Rooma, 4.11.1950) www.echr.coe.int/Documents/Convention_ENG.pdf
83. Euroopa Liidu Põiõiguste harta (2012/C 326/02)
84. Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris
85. Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006 , mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ
86. Lissaboni leping, millega muudetakse Euroopa Liidu lepingut ja Euroopa Ühenduse asutamislepingut sõlmitud Lissabonis 13. detsembril 2007 ELT C,17.12.2007
87. Charter Of Fundamental Rights Of The European Union (2012/C 326/02)

Teiste riikide õigusaktid:

88. Constitution of Romania 429/2003
89. The German Code Of Criminal Procedure StPO (BGBl. I S. 410)

Eesti kohtulahendid:

90. RKKKo 3-1-3-13-03

91. RKKKo 3-1-1-104-05
92. RKKKo 3-1-1-31-11
93. RKKKm 3-1-1-57-12
94. RKKKo 3-1-1-51-14
95. RKKKo 3-1-1-14-14
96. TlnRnKo 1-14-3029 31 märts 2015
97. RKKKo 3-1-1-93-15

Muud kohtulahendid:

98. EIKo 06.09.1978, 5029/71. Klass and others v. Federal Republic of Germany
99. United States Supreme Court 28.03.1979. 78-5374 Smith v. Maryland
100. EIKo 26.04.1985,8691/79, Case of Malone v. The United Kingdom
101. EIKo 16.12.1992 *13710/88* Niemietz v. Germany
102. EIKo 03.04.2007, 62617/00. Copland v. The United Kingdom
103. United States Court of Appeals,Ninth Circuit 06.07.2007. 512 F.3d 500 United States v. Forrester.
104. EiKo 10.02.2009, 25198/02, Case Of Iordachi And Others v. Moldova
105. EIKo 03.07.2012, 30457/06, Robathin v. Austria
106. EIKo 06.12.2012, 12323/11 Michaud v. France
107. EIKo 14.03.2013, 24117/08, Bernh Larsen Holding AS and others v. Norway
108. EKo 21.12.2016, liidetud kohtuasjad C-203/15 Tele2 Sverige AB v. Post- och telestyrelsen ja C-698/15 Secretary of State for the Home Department v. Tom Watson, Peter Price, Geoffrey Lewis.

109. EKo 08.04.2014 Liidetud kohtuasjades C‑293/12 Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, Minister for Justice, Equality and Law Reform,Commissioner of the Garda Síochána,
Iirimaa, The Attorney General ning C‑594/12 Digital Rights Ireland Ltd Kärntner Landesregierung, Michael Seitlinger,Christof Tschohl jt.

110. EIKo 4.12.2015, 47143/06 *Roman Zakharov v. Russia*
111. EIKo 12.01.2016, *37138/14 Szabó And Vissy v. Hungary*

Muud Allikad:

112. United Nations General Assembly. Summary of the Human Rights Council panel discussion on the right to privacy in the digital age. www.un.org/en/ga/search/view_doc.asp?symbol=A/HRC/28/39
113. Ekert, A. A Very Brief History Of Secrecy Www.Arturekert.Org/Crypto/History.Pdf
114. Inimõiguste instituut. Privaatsusõigus inimõigusena ja igapäevatehnoloogiad www.humanrightsestonia.ee/wp/wp-content/uploads/2014/11/EST-Uuringu-I-osa-Saateks1.pdf
115. Tuulik, M-E., Sellest aastast on kõik Eesti seadused inglise keeles kättesaadavad. Justiitsministeerium. www.just.ee/et/uudised/sellest-aastast-koik-eesti-seadused-inglise-keeles-kattesaadavad
116. Riigi peaprokuröri ülevaade Riigikogu põhiseaduskomisjonile seadusega prokuratuurile pandud ülesannete täitmise kohta 2012. Aastal. www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/riigi_peaprokuri_ettekanne_pohiseaduskomisjonile_2013_0.pdfl
117. FinFisher – Customers www.wikileaks.org/spyfiles4/customers
118. Paulus, S. Teadlane: sõnumisaladust aitab kaitsta kvantkrüptograafia. Eesti Rahvusringhääling. http://novaator.err.ee/v/yhiskond/bea946cf-9c59-4df3-80ac-2aa46035d48b/teadlane-sonumisaladust-aitab-kaitsta-kvantkruptograafia
119. Kaye, D. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session29/Documents/A.HRC.29.32_AEV.doc.
120. Justiitsministeerium. Aruanne jälitusstatistikast 2015. aastal. Kriminaalpoliitika analüüs nr2/2016 www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/jalitusstatistika_aruanne_2015.pdf
121. Trehver, J. Digitaalsete tõendite kasutamise võimaldamine http://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf
122. Trehver, J. Arvamus Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõule (295 SE) https://www.riigikogu.ee/download/28f38ff9-5083-4d44-9838-b9b0b467a29a

123. Ginter, J., Plekksepp, A., Soo, A., Kairjak, M., Kangur, A., Mets,T., Analüüs isikute põhiõiguste tagamisest ja eeluurimise kiirusest kriminaalmenetluses. Tartu Ülikool 2013.www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/analuus_isikute_pohioiguste_tagamisest_ja_eeluurimise_kiirusest_kriminaalmenetluses.pdf

124. Fondamentaux, M. D. D. Commentary of the charter of fundamental rights of the european union. http://ec.europa.eu/justice/fundamental-rights/files/networkcommentaryfinal_en.pdf

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

126. Tuulik, M-E. Anvelt: sideandmete kasutamine ei tohi tulla isikute põhiõiguste arvel, Justiitsministeerium. www.just.ee/et/uudised/anvelt-sideandmete-kasutamine-ei-tohi-tulla-isikute-pohioiguste-arvel

127. Madise, Ü. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus. www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf

128. Andmekaitse inspektsioon. Metaandmed ja privaatsus Juhis organisatsioonidele ja kodukasutajale seaduse rakendamisel. www.aki.ee/sites/www.aki.ee/files/elfinder/article_files/Juhised/Metaandmed.pdf

129. Strandberg, M., Rahumägi, J. Rahumägi ja Strandberg: kas ja miks meid pealt kuulatakse? Postimees, 2007. arvamus.postimees.ee/1726661/rahumagi-ja-strandberg-kas-ja-miks-meid-pealt-kuulatakse

130. The Constitution of the Republic of Estonia. Translation published: 21.05.2015 www.riigiteataja.ee/en/eli/521052015001/consolide

131. Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf

132. Aas, N. Riigi peaprokuröri ülevaade Riigikogu põhiseaduskomisjonile seadusega prokuratuurile pandud ülesannete täitmise kohta 2012. Aasta. Eesti prokuratuur, 2013, lk 16 www.prokuratuur.ee/sites/www.prokuratuur.ee/files/elfinder/article_files/riigi_peaprokuri_ettekanne_pohiseaduskomisjonile_2013_0.pdf

133. Glikman, L. Igikestev mure põhiõiguste kaitstuse pärast. Eesti Päevaleht 2016. epl.delfi.ee/news/arvamus/igikestev-mure-pohioiguste-kaitstuse-parast?id=75525191

134. Siitam-Nyiri, K. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 175 www.riigikogu.ee/download/0eb6bebb-9abf-470f-9842-abe51795206a

135. La Rue, F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/HRC/23/40 2011 www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

136. Aasmäe, K. Siseministeerium ei kinnitanud ega lükanud ümber Finfisheri nuhkvara võimalikku kasutamist. Postimees 2012. majandus24.postimees.ee/941996/siseministeerium-ei-kinnitanud-ega-lukanud-umber-finfisheri-nuhkvara-voimalikku-kasutamist?_ga=1.137999731.2113773778.1491122744

137. Teder, I. Arvamus eelnõule Kriminaalmenetluse seadustiku jt seaduste muutmise eelnõu (295 SE) www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_arvamus_eelnoule_kriminaalmenetluse_seadustiku_jt_seaduste_muutmise_eelnou_295_se.pdf

138. Trehver, J. Arvamus Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõule (295 SE) https://www.riigikogu.ee/download/28f38ff9-5083-4d44-9838-b9b0b467a29a

139.

140. Maruste, R. Rait Maruste: Kas prokuratuur ja kapo suudavad tõrjuda mõjuvõimu ärakasutamise kahtlustusi? Eesti Päevaleht 2012 epl.delfi.ee/news/arvamus/rait-maruste-kas-prokuratuur-ja-kapo-suudavad-torjuda-mojuvoimu-arakasutamise-kahtlustusi?id=63833640

141. Reps, M. Kriminaalmenetluse seadustiku ja teiste seaduste muutmise seaduse eelnõu 295 SE. https://www.riigikogu.ee/download/7457e622-fe01-4d20-9af1-cd6cda20829d

142. Komisjoni Teatis Euroopa Parlamendile, Euroopa Ülemkogule Ja Nõukogule Neljas Eduaruanne Tulemusliku Ja Tegeliku Julgeolekuliidu Suunas Liikumise Kohta. 2017 Eur-Lex.Europa.Eu/Legal-Content/Et/Txt/Pdf/?Uri=Celex:52017dc0041&From=Et

143. Osula, A-M. Remote search and seizure Of extraterritorial data. Tartu Ülikool. dspace.ut.ee/bitstream/handle/10062/55683/osula_anna_maria.pdf?sequence=1&isAllowed=y

144. Digitaleurope views on Law Enforcement Access to Digital Evidence http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2299&language=en-US&PortalId=0&TabId=353

145. Reinthal, T. Küberkuritegevuse kohtupraktika Eestis. Riigikohus, 2009. www.riigikohus.ee/vfs/1275/Kyberkuritegevus%202009.pdf

146. Nixon, R. U.S. Postal Service Logging All Mail for Law Enforcement- www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html?pagewanted=all

147. Kegandberg, E. Eriarvamus Riigikohtu kriminaalkolleegiumi 20. novembri 2015. aasta otsuse 3-1-1-93-15 juurde. www.riigikohus.ee/?id=11&tekst=222579511