TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Christina Jõesaar

ELEKTROONILISE SIDE ANDMETE SÄILITAMINE JA KASUTAMINE KRIMINAALMENETLUSES

Magistritöö

Juhendaja
Prof Jaan Ginter

Tartu
2019

Sisukord

Sissejuhatus

Viimastel aastatel on ühiskonnas üha enam arutletud selle üle, et riik jälgib inimesi rohkem, kui arvata osatakse. Paljud inimesed kardavad seetõttu, et neid pidevalt jälgitakse ning sekkutakse seekaudu nende õigusesse privaatsusele. Üheks jälgimise vormiks on elektroonilise side liiklus- ja asukohaandmete ehk metaandmete säilitamine ja ametiasutustele kättesaadavaks tegemine.[1] Metaandmed on andmed, mis vastavad konkreetse side toimumise kohta küsimustele kes, millal ja kuidas. Säilitatavad metaandmed hõlmavad üldiselt liiklusandmeid ehk andmeid selle kohta, kuidas side edastati, sealhulgas allikas, edastamise aeg, asukoht, sihtkoht, abonendi andmeid ehk abonentide identifitseerimisvahendeid ja kasutatava sideteenuse kohta käivaid andmeid ehk näiteks teenuse kasutamise pikkust, alla laaditud andmete hulka, arveldusteavet ja ümbersuunamisteenuseid.[2]

Ajakirjanduses on ilmunud mitmeid artikleid, mis juhivad inimeste tähelepanu sellele, kuidas Eestis säilitatakse elektroonilise side andmeid, kuigi Euroopa Kohtu praktikaga see kooskõlas ei ole.[3] Pärast Euroopa Kohtu poolt sideandmete säilitamist puudutavate lahendite tegemist ei ole liikmesriigid kiirustanud oma riigisiseste seaduste muutmisega. Seetõttu ei ole Eesti sugugi mitte ainus riik, kus toimub vastuolus Euroopa Kohtu praktikaga elektroonilise side andmete säilitamine ja kasutamine. Veel 2017. aasta septembris avaldatud aruande kohaselt ei olnud vaadeldud 21-st Euroopa Liidu liikmesriigist ühegi seadusandlus kooskõlas Euroopa Kohtu praktika ning inimõiguste standarditega.[4]

Reageeringuna Euroopa Kohtu otsustele andmete säilitamise ja kasutamise kohta on mitmed Euroopa Liidu liikmesriigid, sealhulgas Eesti Vabariik, esitanud Euroopa Kohtule eelotsusetaotlusi. Eelotsusetaotlustega soovivad liikmesriigid saada selgust, millistel tingimustel ja millisel määral võiks elektroonilise side andmete säilitamine ja kasutamine olla Euroopa Liidu õigusega kooskõlas.

---

[1] U. Lõhmus. Kolm suurt probleemi kodanike jälgimisega. – ERR 21.09.2018. Arvutivõrgus: https://www.err.ee/862981/uno-lohmus-kolm-suurt-probleemi-kodanike-jalgimisega (16.04.2019).

[2] National Data Retention Laws since the CJEU's Tele-2/Watson Judgment. A Concerning State of Play for the Right to Privacy in Europe. Privacy International. September 2017, lk 6. Arvutivõrgus: https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf (20.04.2019).

[3] Vt: K. Pruul. Riik lausjälgimisest loobuma ei rutta. – Äripäev 28.11.2018; Advokaadid: Eesti riik rikub elektroonilise side andmeid kogudes ja kasutades teadlikult ja räigelt inimõigusi. – Objektiiv, 20.11.2017.

[4] Press Release: New Privacy International Report Shows That 21 European Countries Are Unlawfully Retaining Personal Data. Privacy International. 6.09.2017. Arvutivõrgus: https://privacyinternational.org/press-release/634/press-release-new-privacy-international-report-shows-21-european-countries-are (19.04.2019).

Samas ei ole Eesti jäänud elektroonilise side andmete säilitamise ja kasutamise regulatsiooni Euroopa Liidu õigusega kooskõlla viimisel täiesti tegevusetuks. 2018. aasta lõpus avaldati elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus[5]. Seega on Eesti astunud esimesi samme, et kehtivat regulatsiooni muuta.

Varasemalt on elektroonilise side andmete säilitamise põhiseaduspärasust käsitlenud õiguskantsler Ülle Madise, kes, analüüsides elektroonilise side seaduse (edaspidi ESS)[6] regulatsiooni, leidis, et selles sisalduvad sätted ei ole põhiseadusega vastuolus.[7] Õiguskantsleri seisukohtadele on avaldanud kriitikat nii 2016. aastal magistritöö teemal „Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel“[8] kaitsnud Piret Schasmin kui ka Kätlin Helena Sehver, kes kaitses magistritöö teemal „Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel“[9].

Pärast eelpool nimetatud tööde avaldamist on aga Euroopa Kohtule esitatud uusi eelotsusetaotlusi seoses elektroonilise side andmete säilitamise ja kasutamisega ning tehtud on ka uusi otsuseid, mis antud olukorda täpsustavad. Samuti on alates 2017. aastast Euroopa Liidus menetluses uue e-privaatsuse määruse eelnõu[10] ning avaldatud on elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus. Seega on elektroonilise side andmete säilitamise ja kasutamise teema Eestis endiselt aktuaalne.

---

[5] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine). Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83?activity=1#fVKzRoTp (20.02.2019).

[6] Elektroonilise side seadus. – RT I, 12.12.2018, 33.

[7] Ü. Madise. Õiguskantsleri seisukoht elektroonilise side seaduse § 111^1 põhiseaduspärasuse kohta. 20.07.2015. Arvutivõrgus: https://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf (15.02.2019).

Ü. Madise. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus. 22.04.2016. Arvutivõrgus: https://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (15.02.2019).

[8] P. Schasmin. Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel. Magistritöö. Tallinn: Tartu Ülikool, 2016.

[9] K. H. Sehver. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. Tallinn: Tartu Ülikool, 2017.

[10] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). 10.01.2017. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010&qid=1550151482281 (14.02.2019).

Magistritöö eesmärgiks on välja selgitada, millistel tingimustel ja millises ulatuses on õigustatud elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses, muuhulgas uue e-privaatsuse määruse ettepaneku ning elektroonilise side seaduse väljatöötamiskavatsuse valguses.

Käesolevas magistritöös on püstitatud kaks hüpoteesi. Esimeseks hüpoteesiks on, et elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses oleks kavandatava e-privaatsuse määruse kehtima hakkamisel põhjendatud vaid piiratud tingimustel tulenevalt sideandmete säilitamise ja kasutamisega kaasnevast põhiõiguste riivest. Teiseks hüpoteesiks on, et elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses on elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsuse kohaselt kooskõlas kavandatava e-privaatsuse määrusega.

Hüpoteesi kontrollimist toetavad järgmised küsimused:

- missugune on tulenevalt Euroopa Liidu õigusest praegune seisukoht sideandmete säilitamise ja kasutamise kohta?
- millised on elektroonilise side andmete säilitamise ja kasutamisega kaasnevad põhiõiguste riived?
- missuguseid muudatusi soovitakse teha Euroopa Liidu õiguses ning Eesti õiguses seoses sideandmete säilitamise ja kasutamisega?
- millistes küsimustes on Euroopa Liidu liikmesriigid soovinud eelotsusetaotluste esitamise abil selgust saada ning millised on Eesti seisukohad neis küsimustes?

Käesolev magistritöö koosneb kahest peatükist. Esimeses peatükis käsitletakse seda, kuidas on reguleeritud elektroonilise side andmete säilitamine Euroopa Liidu õiguses, kuidas on seda muutnud Euroopa Kohtu praktika ning milliseid muudatusi tooks uue e-privaatsuse määruse kehtestamine. Vaadeldakse, milliste elektroonilise side andmete säilitamine on Eestis kehtiva õiguse järgi kohustuslik ning milliseid muudatusi plaanitakse seadustes teha. Samuti käsitletakse esimeses peatükis elektroonilise side andmete säilitamise ja kasutamisega riivatavaid põhiõigusi.

Teises peatükis analüüsitakse Euroopa Kohtu praktikat elektroonilise side andmete kasutamise kohta, e-privaatsuse määruse ettepanekut ning Euroopa Inimõiguste Kohtu lahendeid seoses side massiandmete kogumisega. Teise peatüki kolmandas alapeatükis vaadeldakse Euroopa Liidu liikmesriikide reaktsioone Euroopa Kohtu lahenditele elektroonilise side andmete

säilitamise ja kasutamise kohta, sealhulgas riikide poolt hiljuti esitatud eelotsusetaotlusi, mis puudutavad side metaandmete säilitamist ja kasutamist. Samuti käsitletakse elektroonilise side andmete kasutamist kriminaalmenetluses ning ESS väljatöötamiskavatsust osas, mis puudutab sideandmete kasutamist.

Magistritöö põhilisteks allikateks on Euroopa Kohtu ja Euroopa Inimõiguste Kohtu lahendid, Euroopa Liidu ja Eesti õigusaktid, elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, kavandatava e-privaatsuse määruse ettepanek ning õiguskirjandus. Käesolevas töös kasutatakse analüütilist, võrdlevat ja süsteemset meetodit.

Märksõnad: Euroopa Liidu õigus, metaandmed, telekommunikatsioon, elektrooniline kommunikatsioon, kriminaalmenetlus.

1. Elektroonilise side andmete säilitamine

1.1. Elektroonilise side andmete säilitamine Euroopa Liidu õiguses

1.1.1. Elektroonilise side andmete säilitamine Euroopa Liidu õigusaktide ja Euroopa Kohtu praktika kohaselt

2006. aastal hakkas kehtima direktiiv 2006/24/EÜ[11], mis käsitles üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist. Andmete säilitamise direktiivi artikli 1 lg 1 järgi oli direktiivi eesmärgiks ühtlustada liikmesriikide sätted elektroonilise side andmete säilitamise kohta, et need oleksid kättesaadavad pädevatele asutustele riiklikus õiguses määratletud raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks. Direktiivi artikkel 5 nägi ette vastavate andmete liigid, mille puhul liikmesriigid pidid tagama andmete säilitamise. Direktiivi artikli 6 järgi pidid liikmesriigid neid andmeid säilitama mitte vähem kui kuue kuu, kuid mitte rohkem kui kahe aasta jooksul side toimumisest. Andmete säilitamise direktiivi kehtivusaeg jäi aga lühikeseks.

2012. aastal esitasid Iirimaa ja Austria kohtud Euroopa Kohtusse eelotsusetaotlused seoses andmete säilitamise direktiivi kooskõlaga Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni[12] ja Euroopa Liidu põhiõiguste harta[13] nõuetega. Euroopa Kohus liitis kohtuasjad ja tegi 2014. aasta aprillis asjas *Digital Rights Ireland* otsuse, millega tunnistati andmete säilitamise direktiiv kehtetuks. Kohus leidis, et andmete säilitamine saavutamaks direktiiviga taotletavat eesmärki – andmete kättesaadavust iga liikmesriigi riiklikus õiguses määratletud raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks – on sobiv meede. Siiski ei piirduta andmete säilitamisel direktiivis sätestatu kohaselt eesmärgi saavutamiseks vaid vältimatult vajalikuga. Sellest tulenevalt järeldas kohus, et andmete säilitamise direktiivi vastuvõtmisega ületas liidu seadusandja proportsionaalsuse põhimõttest tulenevaid piire.[14]

---

[11] 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. – ELT L 105, 13.04.2006.

[12] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.

[13] Euroopa Liidu põhiõiguste harta. – ELT C 326, 26.10.2012.

[14] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland*, p-d 22, 41, 49, 65, 69.

Vahetult pärast andmete säilitamise direktiivi kehtetuks tunnistamist reguleeris isikuandmete valdkonda direktiiv 95/46/EÜ üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.[15] Alates 25. maist 2018. aastast on direktiiv 95/46/EÜ tunnistatud kehtetuks ning kohaldatakse määrust (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta.[16] Lisaks reguleerib pärast andmete säilitamise direktiivi kehtetuks tunnistamist sideandmete kogumist direktiiv 2002/58/EÜ[17], mis käsitleb isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris.

Euroopa riikides põhjustas aga küsimusi see, kuidas mõjutab *Digital Rights Ireland*'i kohtuotsus ning andmete säilitamise direktiivi kehtetuks tunnistamine riigisisese õiguse norme, mis reguleerivad elektroonilise side liiklus- ja asukohaandmete säilitamist ja pädevatele asutustele kättesaadavaks tegemist. Ebaselgest olukorrast tulenevalt esitasid Rootsi ja Ühendkuningriigid Euroopa Kohtusse eelotsusetaotlused, mis liideti üheks kohtuasjaks.[18] Selles asjas jõudis Euroopa Kohus järeldusele, et e-privaatsuse direktiivi 2002/58/EÜ artikli 15 lg 1 alusel võivad liikmesriigid piirata andmete konfidentsiaalsust, kuid piiranguid tuleb tõlgendada kitsalt, et erand andmete konfidentsiaalsuse põhimõttest ei muutuks reegliks.[19]

Rootsi riigisisesed õigusnormid nägid ette kõigi klientide ja registreeritud kasutajate kõikide liiklus- ja asukohaandmete säilitamise, olenemata seejuures kasutatud elektroonilise sidevahendi liigist ning nägemata ette erandeid. Kohus märkis, et need andmed koosvõetuna võimaldavad teha väga täpseid järeldusi isikute eraelu kohta, nende igapäevaelu harjumuste, alalise või ajutise elukoha, liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad.[20] Nimetatud õigusnormid toovad kaasa põhiõiguste riive, mida on võimalik põhjendada vaid võitlusega raskete kuritegude vastu, kuid üksnes sellise üldist huvi pakkuva eesmärgiga ei saa põhjendada norme, millega kohustatakse säilitama kõiki liiklus- ja

[15] Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995.

[16] Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.05.2016.

[17] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, 31.07.2002.

[18] EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige*.

[19] *Ibid*, p 89.

[20] *Ibid*, p 99.

asukohaandmeid.[21] Kohus tõdes, et Rootsi õigusnormid ei näinud ette mittemingisuguseid eristamisi, piiranguid või erandeid, mistõttu puudutavad need normid ka isikuid, kelle kohta ei esine tõendeid, et nende käitumisel oleks seos raske kuritegevusega.[22] Kohus leidis, et Rootsi ja kõigi teiste riikide sarnased normid väljuvad rangelt vajaliku piiridest ning neid ei saa pidada demokraatlikus ühiskonnas põhjendatuks.[23]

See, et üldiselt kõikide elektroonilise side liiklus- ja asukohaandmete säilitamine ei ole põhjendatud, ei tähenda, et selliste andmete säilitamine oleks täiesti välistatud. Euroopa Kohus tõi lahendis *Tele2 Sverige* välja teatud tingimused, mida järgides on võimalus liikmesriikidel raskete kuritegude vastu võitlemise eesmärgil säilitada liiklus- ja asukohaandmeid. Andmete säilitamiseks peab säilitamine olema piiratud säilitatavate andmete liigi, asjassepuutuvate sidevahendite ja isikute ning säilitamise kestuse osas rangelt vajalikuga. Selleks peavad normid ette nägema, missugustel asjaoludel ning tingimustel võib andmeid ennetavalt säilitada. Andmete säilitamise tingimused peavad võimaldama praktikas meetme ulatust ning puudutatud isikute ringi piirata. Isikute ringi piiramine on võimalik, kui andmete säilitamist rakendatakse nende isikute puhul, kellega seotud andmetest avaldub kasvõi kaudne seos raskete kuritegudega. Euroopa Kohus leidis, et piirangu võib saavutada ka geograafilise kriteeriumi abil, kui objektiivsete asjaolude pinnalt leitakse, et mõnes piirkonnas esineb eriti suur oht raskete kuritegude ettevalmistamiseks või toimepanemiseks.[24]

Eristada tuleb nõudeid sideandmete säilitamisele ning säilitatud andmetele juurdepääsuks. Lahendiga *Tele2 Sverige* andis Euroopa Kohus selge hinnangu, et kõigi elektroonilise side andmete üldine säilitamine ei ole vajalik ega põhjendatud. Liikmesriikidel on seega kohustus piirata säilitatavaid andmeid ning kehtestada normid, milles nähakse ette tingimused andmete säilitamiseks. Kuigi otsusest *Tele2 Sverige* võis jääda mulje, et rõhutati andmete säilitamise eesmärgina just raskete kuritegude vastu võitlemist[25], selgitas kohus otsuses *Ministerio Fiscal*[26] elektroonilise side andmete säilitamist ja kasutamist põhjendavat eesmärki selgemalt.[27]

---

[21] *Ibid*, p-d 102, 103.

[22] *Ibid*, p-d 105, 106.

[23] *Ibid*, p 107.

[24] *Ibid*, p-d 108-111.

[25] Järeldusele, et Euroopa Kohus on pidanud sideandmete säilitamist ja kasutamist põhjendatuks vaid raskete kuritegude uurimise, avastamise ja menetlemisega, on jõudnud oma magistritöös ka K. H. Sehver. (Vt viide 5, lk 64.)

[26] EKo 2.10.2018, C-207/16, *Ministerio Fiscal*.

[27] Vt käesoleva töö alapeatükk 2.1.1.

1.1.2. Elektroonilise side andmete säilitamine kavandatava e-privaatsuse määruse kohaselt

Arvestades järeldusi, milleni Euroopa Kohus lahendites jõudis, e-privaatsuse direktiivi sätete mõningast ajale jalgu jäämist ning uut isikuandmete kaitse üldmäärust, tekkis vajadus uue õigusakti järele, mis reguleeriks elektroonilise side andmete kaitset Euroopa Liidus. Vähem kui kuu aega pärast Euroopa Kohtu otsuse tegemist asjas *Tele2 Sverige*, tegigi komisjon Euroopa Parlamendile ja nõukogule ettepaneku võtta vastu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ.[28]

Nimelt leiti õigusloome kvaliteedi ja tulemuslikkuse programmi raames e-privaatsuse direktiivi uurides, et tulemuslikkuse ja tõhususe seisukohast ei ole direktiiv oma eesmärke täielikult täitnud – mõned sätted on ebaselgelt sõnastatud ning õiguskontseptsioonid mitmetimõistetavad.[29] Määruse ettepaneku põhjenduses 6 märgitakse, et kuigi e-privaatsuse direktiivi sätted on üldiselt veel otstarbekad, siis ei ole direktiiv pidanud sammu tehnoloogia ja turu tegeliku arenguga.[30] Seepärast ei ole privaatsuse kaitse ja konfidentsiaalsus elektroonilise side puhul piisavalt järjepidev ja tõhus ning sel põhjusel tuleks e-privaatsuse direktiiv kehtetuks tunnistada.[31]

Määruse ettepaneku põhjenduses 1 märgitakse, et elektroonilise side konfidentsiaalsuse abil tagatakse, et poolte vahetatud teavet ja side väliseid elemente ei avaldata kellelegi peale sides osalejate ning konfidentsiaalsuse põhimõtet tuleks kohaldada nii praegu kasutusel olevate kui ka tulevikus kasutusele võetavate sidevahendite suhtes.[32] Seega aitaks määrus kaasa sellele, et konfidentsiaalseks peetakse ka neid side metaandmeid, mis kaasnevad tehnoloogia arenedes kasutusele võetavate uute sidevahendite kasutamisega.

---

[28] Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). 10.01.2017. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010&qid=1550151482281 (14.02.2019).

[29] *Ibid*, lk 5.

[30] Näiteks märgitakse määruse ettepaneku põhjenduses 11, et traditsiooniliste telefonikõnede, tekstsõnumite ja elektronposti edastamise teenuste asemel kasutatakse üha enam internetipõhiseid teenuseid, millel on samaväärsed funktsioonid, näiteks IP-kõnesid, sõnumiteenuseid ja veebipõhiseid meiliteenuseid.

[31] Ettepanek, lk 12.

[32] *Ibid*, lk 11.

Kavandatava määruse põhjendus 2 toob sisuliselt välja seisukoha, mida Euroopa Kohus väljendas otsuses *Tele2 Sverige* ning *Digital Rights Ireland*.[33] See on ka põhjus, miks tuleb pidada elektroonilist sidet ning selle väliseid elemente konfidentsiaalseks nagu on mainitud ettepaneku põhjenduses 1. Nimelt nagu elektroonilise side sisu võib anda sides osalevate füüsiliste isikute kohta väga tundlikku teavet, võivad väga tundlikku ja isiklikku teavet anda ka elektroonilisest sidest saadud metaandmed. Need metaandmed võimaldavad teha täpseid järeldusi elektroonilises sides osalevate inimeste eraelu, näiteks nende sotsiaalsete suhete, igapäevaste harjumuste ja tegevuste, huvide ning eelistuste kohta.[34]

Määruse ettepaneku seletuskirja kohaselt ei sisalda ettepanek konkreetseid sätteid andmete säilitamise kohta. Samas on liikmesriikidel võimalik säilitada või luua riiklikke andmete säilitamise raamistikke. Seletuskirja kohaselt on selliste raamistike abil võimalik liikmesriikidel kehtestada muu hulgas sideandmete sihtotstarbelise säilitamise meetmed, mis vastavad Euroopa Liidu õigusele, võttes arvesse Euroopa Kohtu otsuseid e-privaatsuse direktiivi ning põhiõiguste harta tõlgendamise kohta. Ka ettepaneku põhjenduse 7 kohaselt tuleb liikmesriikidele anda võimalus säilitada määrusega lubatud piirides riiklikke sätteid, millega täpsustatakse või selgitatakse määruse õigusnormide kohaldamist.[35]

Määruse ettepaneku seletuskirjas öeldust võib seega järeldada, et Euroopa Liidu tasandil elektroonilise side andmete säilitamist enam reguleerima ei hakata. Liikmesriigid peavad aga vastavad sätted andmete säilitamise kohta siseriiklikus õiguses kehtestama. Selliste sätete puhul peavad liikmesriigid arvestama, et need ei oleks vastuolus Euroopa Liidu õigusega, sealhulgas Euroopa Kohtu otsustega. Seega peaksid liikmesriigid ilmselt lähtuma eelkõige otsustes *Digital Rights Ireland* ja *Tele2 Sverige* kirjeldatud põhimõtetest sideandmete säilitamise kohta.

Määruse ettepaneku artikkel 5 sätestab elektroonilise side andmete[36] konfidentsiaalsuse ning keelab elektroonilise side andmetega seotud mis tahes sekkumised – kuulamine, pealtkuulamine, salvestamine, seire, skannimine või muud liiki infopüük, järelevalve või töötlemine – muude isikute kui lõppkasutajate poolt, kuid lubab määrusega ette näha keelu

[33] EKo *Tele2 Sverige*, p 99; EKo *Digital Rights Ireland*, p 27.

[34] Ettepanek, lk 11.

[35] *Ibid*, lk 3, 12.

[36] Ettepaneku artikli 4 lg 3 punkti a kohaselt tähistab mõiste „elektroonilise side andmed“ elektroonilise side sisu ja elektroonilise side metaandmeid (*Ibid*, lk 24).

suhtes ka erandeid.[37] Seega on e-privaatsuse määruse ettepaneku artikli 5 sisu üldjoontes samasugune nagu see on praegu kehtiva e-privaatsuse direktiivi artikli 5 lg-s 1.

Artiklis 5 mainitud eranditeks elektroonilise side andmete konfidentsiaalsuse suhtes on muuhulgas määruse ettepaneku artiklites 6 ja 7 sätestatu. Artikkel 7 reguleerib elektroonilise side andmete salvestamist ja kustutamist. Selle artikli lõike 2 kohaselt oleks elektroonilise side teenuse osutaja kohustatud elektroonilise side metaandmed kustutama või need andmed anonüümseks muutma pärast seda, kui need ei ole enam side edastamise jaoks vajalikud. Seejuures ei piira artikkel 7 lg 2 artikli 6 lg 2 punktide a ja c kohaldamist, mis näevad ette sideteenuste osutajate õiguse töödelda side metaandmeid vajaliku aja vältel, et täita kohustuslikke teenuse kvaliteedi nõudeid või kui asjaomane lõppkasutaja on andnud nõusoleku oma side metaandmete kindlaksmääratud otstarbel töötlemiseks. Artikli 7 lg 3 kohaselt võib juhul, kui elektroonilise side metaandmeid töödeldakse arveldamise eesmärgil, asjakohaseid metaandmeid säilitada kuni selle ajavahemiku lõpuni, mille vältel võib arve seaduslikult vaidlustada või riigi õiguse kohaselt nõuda selle tasumist.[38]

Nagu on näha artiklist 7 koostoimes artikliga 5, siis otseselt ei anna kavandatav määrus liikmesriikidele võimalust metaandmete kohustuslikuks säilitamiseks. Vastupidi, artiklist 7 lähtuvalt tuleks metaandmed kustutada, kui need pole enam side edastamiseks vajalikud või kui on möödunud ajavahemik, mille jooksul võib arve vaidlustada või nõuda selle tasumist. Seega oleks elektroonilise side metaandmete säilitamine kavandatava määruse kohaselt lubatud vaid väga piiratud juhtudel ja piiratud ajavahemiku jooksul. Siiski, nagu selgub määruse ettepaneku artiklist 11, võib tulevikus liikmesriikidel olla võimalik säilitada sideandmeid ka üldiste huvide kaitseks austades seejuures põhiõiguste ja -vabaduste olemust.[39]

[37] *Ibid*, lk 25.

[38] *Ibid*, lk 25-28.

[39] Kavandatava määruse artikli 11 ning selles viidatud piirangut õigustavate eesmärkide kohta vt käesoleva töö peatükki 2.1.2.

1.2. Elektroonilise side andmete säilitamine Eesti siseriiklikus õiguses

1.2.1. Elektroonilise side andmete säilitamine kehtiva õiguse kohaselt

Eesti siseriiklikus õiguses annab aluse elektroonilise side andmete säilitamiseks ESS. Selles seaduses sätestatud elektroonilise side andmete säilitamist ja kasutamist reguleerivad normid kehtestati võtmaks Eesti õigusesse üle 2006. aastal Euroopa Parlamendi ja nõukogu poolt vastu võetud direktiivi 2006/24/EÜ, mis käsitles elektrooniliste sideteenuste ja sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist.

Andmete säilitamise direktiivi artikli 1 lg 1 järgi oli direktiivi eesmärgiks ühtlustada liikmesriikide sätted elektroonilise side andmete säilitamise kohta, et sideandmed oleksid kättesaadavad pädevatele asutustele riiklikus õiguses määratletud raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks. Direktiivi artikkel 5 nägi ette vastavate andmete liigid, mille puhul liikmesriigid pidid tagama andmete säilitamise. Direktiivi artikli 6 järgi pidid liikmesriigid neid andmeid säilitama mitte vähem kui kuue kuu, kuid mitte rohkem kui kahe aasta jooksul side toimumisest. Seadusandja võttis andmete säilitamise direktiivi Eesti õigusesse üle elektroonilise side seaduse ja rahvatervise seaduse muutmise seadusega[40] 15. novembril 2007. aastal.

Põhiline säte sideettevõtja poolt andmete säilitamise kohustuse kohta sisaldub ESS §-s 111^1. Loetelu andmete kohta, mida sideettevõtjad on kohustatud säilitama, on sätestatud ESS § 111^1 lõigetes 2 ja 3.

ESS § 111^1 lg 2 alusel on telefoni- ja mobiiltelefoniteenuse ning telefoni- ja mobiiltelefonivõrgu teenuse osutaja kohustatud säilitama muuhulgas:

- helistaja numbri ning kliendi nime ja aadressi;
- vastuvõtja numbri ning kliendi nime ja aadressi;
- lisateenuse, sealhulgas kõne suunamise või edastamise kasutamise korral valitud numbri ning kliendi nime ja aadressi;
- kõne alguse ja lõpu kuupäeva ning kellaaja;
- kasutatud telefoni- või mobiiltelefoniteenuse;

[40] Elektroonilise side seaduse ja rahvatervise seaduse muutmise seadus. – RT I 2007, 63, 397.

- helistaja ja vastuvõtja rahvusvahelise mobiilside tunnuse ja nende rahvusvahelise mobiilside terminalseadme tunnuse;
- kärjetunnuse kõne alustamise ajal;
- andmed, mis määratlevad tugijaama geograafilise asukoha viitega kärjetunnusele;
- anonüümse ettemakstud mobiiltelefoniteenuse korral teenuse esmase aktiveerimise kuupäeva, kellaaja ning kärjetunnuse, millest teenus aktiveeriti.

Sama paragrahvi lõike 3 järgi on Interneti-ühenduse, elektronposti ja Interneti-telefoni teenuse osutaja kohustatud säilitama:

- sideettevõtja poolt eraldatud kasutajatunnused;
- telefoni- või mobiiltelefonivõrku siseneva side kasutajatunnuse ja telefoninumbri;
- kliendi nime ja aadressi, kelle nimele Interneti-protokolli aadress, kasutajatunnus või number olid side toimumise ajal eraldatud;
- Interneti-telefoni kõne kavandatud vastuvõtja kasutajatunnuse või numbri;
- kavandatud vastuvõtva kliendi nime, aadressi ja kasutajatunnuse elektronposti ning Interneti-telefoni teenuse korral;
- Interneti-seansi alguse ja lõpu kuupäeva ning kellaaja konkreetse ajavööndi järgi koos Interneti-protokolli aadressiga, mille on kasutajale eraldanud Interneti-teenuse osutaja, ja kasutajatunnusega;
- elektronposti või Interneti-telefoni teenuse kasutamise alguse ja lõpu kuupäeva ning kellaaja konkreetse ajavööndi järgi;
- kasutatud Interneti-teenuse elektronposti ja Interneti-telefoni teenuse korral;
- helistaja numbri sissehelistamisega Interneti-ühenduse korral;
- digitaalse kliendiliini või mõni muu tunnuse side algataja kohta.

Nagu näha, tuleb nimetatud sätete alusel sideteenust pakkuvatel ettevõtjatel säilitada teatud andmeid nii telefoni- ja mobiiltelefoniteenuse, elektronposti, Interneti-telefoni kui ka Internetiühenduse kasutamise kohta. Seega säilitatakse nimetatud lõigete alusel vaid elektroonilise side liiklus- ja asukohaandmeid[41], kuid mitte elektroonilise side abil edastatavate sõnumite sisu. Sideettevõtjal on kohustus tagada, et side sisu kajastavad andmed jäetaks säilitamata. See kohustus tuleneb sideettevõtetele ESS § 111[1] lg 9 p-st 4.

[41] Direktiivi 2002/58/EÜ artikkel 2 punkti b kohaselt on liiklusandmed andmed, mida töödeldakse side edastamiseks elektroonilises sidevõrgus või sellise edastamisega seotud arveldamiseks. Sama artikli punkti c järgi on asukohaandmed elektroonilises sidevõrgus töödeldavad andmed, mis näitavad üldkasutatavate elektrooniliste sideteenuste kasutaja lõppseadme geograafilist asukohta.

Hoolimata sellest, et andmete säilitamise direktiiv tunnistati juba 2014. aastal Euroopa Kohtu poolt kehtetuks, ei ole Eestis siiani muudetud ESS sätteid, millega direktiiv riigisisesesse õigusesse üle võeti. Olenemata direktiivi kehtetusest tuleb ESS alusel endiselt valimatult säilitada elektroonilise side andmeid, et need oleks vajadusel võimalik teha vastavatele asutustele kättesaadavaks.

Sarnaselt Rootsi õigusnormidele, mida käsitleti otsuses *Tele2 Sverige*, sätestab ka kehtiv ESS § 111[1] kõikide liiklus- ja asukohaandmete säilitamise ning ei näe ette eristamisi, piiranguid ega erandeid. Seega ei saa käsitletud Euroopa Kohtu lahendist *Tele2 Sverige* tulenevalt pidada ka ESS-s sisalduvaid vastavaid õigusnorme demokraatlikus ühiskonnas põhjendatuks.

1.2.2. Elektroonilise side andmete säilitamine eelnõu väljatöötamiskavatsuses

Tulenevalt sellest, et ESS-s sätestatud elektroonilise side andmete säilitamist käsitlevad õigusnormid on vastuolus Euroopa Kohtu praktikaga, tekkis vajadus tegutseda selle nimel, et muuta elektroonilise side seadust. Juba Vabariigi Valitsuse tegevusprogrammis aastateks 2015-2019 punktis 12.22 on välja toodud vajadus elektroonilise side seaduse eelnõu väljatöötamiskavatsuse järele.[42] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsuse kooskõlastamine algatati 5. novembril 2018. aastal ning käesoleva töö kirjutamise ajaks on seaduseelnõu kooskõlastamise etapp lõppenud.[43]

Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsuses leitakse, et sideandmete säilitamine on vajalik mitmel eesmärgil: süütegude avastamiseks, ennetamiseks, tõkestamiseks ja kohtus menetlemiseks, muude menetluste raames vajaliku tõendusteabe saamiseks, erinevates loamenetlustes ning riikliku julgeoleku tagamiseks.[44] Muude menetluste raames vajaliku tõendusteabe saamiseks ja erinevate loamenetluste tarvis elektroonilise side andmete säilitamist ei saa *Tele2 Sverige*

[42] Vabariigi Valitsuse tegevusprogramm 2015-2019. Vabariigi Valitsuse 29. mai 2015. a korraldus nr 231. Arvutivõrgus: https://www.riigiteataja.ee/aktilisa/3030/6201/5006/231klisa.pdf (19.02.2019).

[43] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine). Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83?activity=1#fVKzRoTp (20.02.2019).

[44] *Ibid*, lk 2.

lahendit silmas pidades proportsionaalseks pidada. Kui Euroopa Kohus pidas isegi raske kuritegevuse vastu võitlemise eesmärgil põhjendatuks andmete ennetavat säilitamist vaid piiratuna rangelt vajalikuga, siis ei ole põhjust arvata, et põhjendatud oleks elektroonilise side andmete ennetav säilitamine muude menetluste raames või loamenetluses kasutamiseks.

Väljatöötamiskavatsuse koostamisel on kaalutud ka varianti säilitada olemasolev regulatsioon. Justiitsministeerium on arutanud sideandmete säilitamise ja kasutamise probleemi erinevate asutuste ja huvigruppidega ning arutelude käigus on selgunud, et „kehtiva olukorra säilitamine ei ole antud juhul võimalik ega asjakohane“. Samuti leitakse väljatöötamiskavatsuses, et „kehtiva õiguse parem selgitamine ja tõhusam rakendamine“ ei annaks soovitud tulemust, sest riivatakse ulatuslikult isikute põhiõigusi, nõudmised sideandmete säilitamisele ja kasutamisele on muutunud kõrgemaks ning kehtiv regulatsioon on killustatud ning ebaselge.[45]

Kehtivale regulatsioonile killustatuse etteheitmine on mõistetav. Kuigi pädevad asutused, kellele sideettevõtjad on kohustatud andmeid edastama, on loetletud ESS § 111^1 lg-s 11, siis iga menetlusliigi kohta käivad regulatsioonid paiknevad mitmetes erinevates seadustes[46]. Eriseadustes on sätestatud, millistel tingimustel on võimalik andmetele juurdepääs, kuidas toimub juurdepääsuks lubade andmine ning millistel eesmärkidel võib andmeid kasutada.

Kuna väljatöötamiskavatsuses jõuti järeldusele, et mitteregulatiivsed meetmed ei ole piisavad, et saavutada soovitud tulemust, on väljatöötamiskavatsuses analüüsitud ka regulatiivseid lahendusi ja nende mõjusid. ESS-s kavandatavate muudatuste eesmärgiks on sätestada täpsemad ja selgemad sideandmete säilitamist ning andmetele juurdepääsu võimaldamist puudutavad reeglid ning näha ette „andmete senisest täpsem ning valikuline säilitamine“. Eelnõu väljatöötamiskavatsuse alusel on plaanis sideandmete säilitamisel selgelt eristada, mis eesmärkidel andmeid töödeldakse – kas korrakaitselisel, kriminaalmenetluslikul või riigi julgeoleku tagamise eesmärgil. Väljatöötamiskavatsuse kohaselt on plaanis kehtestada „erinevad reeglid lähtuvalt andmete säilitamise ja töötlemise eesmärgist“. Siiski on plaanis riigi julgeoleku tagamise eesmärgil kõikide elektroonilise side andmete säilitamine. Seega plaanitakse sisuliselt säilitada kõiki elektroonilise side metaandmeid ja piirata vaid erinevatele andmetele juurdepääsu sõltuvalt kasutamise eesmärgist. Taoline elektroonilise side andmete üldine säilitamine ja vaid kasutamise eesmärkide ja säilitamistähtaegade osas piirangute

[45] *Ibid*, lk 9, 10.

[46] Vastavate eriseaduste kohta vaata käesoleva töö alapeatükki 2.4.

seadmine ei oleks käesoleva töö autori arvates kooskõlas kohtuotsuses *Tele2 Sverige* välja toodud põhimõttega, et üldine kõikide sideandmete säilitamine ei ole põhjendatud ning liikmesriigid peavad piirama säilitatavaid andmeid nende liigi, asjassepuutuvate sidevahendite, isikute ning säilitamise kestuse osas.[47]

Andmete valikulisel säilitamisel on vajalik hinnata selle võimalikkust lähtuvalt erinevatest kriteeriumidest, kuid samal ajal tuleb arvestada, et hoidutaks isikute diskrimineerimisest. Andmete säilitamisel nähakse teoorias nelja erinevat kriteeriumit, mille alusel põhimõtteliselt saaks säilitatavaid andmeid diferentseerida:

- isikuline – valiku aluseks on isiku vanus, sugu, rahvus, religioon, varasemate karistuste olemasolu jne;
- geograafiline – valiku aluseks on teatud piirkonnad;
- seadmepõhine – valiku aluseks on teatud liiki seadmete kasutamine;
- teenustepõhine – andmete säilitamise valiku aluseks on teatud liiki teenuste kasutamine.[48]

Eelnimetatud kriteeriumide puhul on Justiitsministeerium aga leidnud, et need ei oleks tulenevalt seatud eesmärgist efektiivsed ning looksid aluse diskrimineerimiseks. Diskrimineerivaks peetakse ka võimalust panna statistiliste andmete põhjal kokku keskmise kurjategija profiil ning kõrgema kuritegevusega piirkondade väljatoomist Eestis. Samuti nähakse selliste kriteeriumide puhul ohtu, et isikud võivad hakata andmete säilitamisest kõrvale hoiduma. Seetõttu on peetud parimaks lahenduseks kehtestada erinevad säilitamis- ja kasutamisreeglid erinevate andmekategooriate kaupa. Seaduses tuleks ette näha andmete kategooriad konkreetsete menetluste ning asutuste suhtes. Seejuures tuleks erinevatele andmekategooriatele kehtestada ka erinevad säilitamistähtajad.[49]

Sideandmete säilitamisel kriminaalmenetluses tõendite kogumise eesmärgil tuleks eristada, millise kuriteo menetlust päring puudutab. Kriminaalmenetluses tuleb tagada menetlejatele võimalus saada teavet, mida sideettevõtjad säilitavad oma ärilistel eesmärkidel. Sellisele teabele peab olema juurdepääs kindlustatud kogu ajaperioodi vältel, mil sideettevõtja neid andmeid säilitab ning kõikide andmete osas, mida sideettevõtja ärilistel eesmärkidel on kogunud. Juurdepääs sellistele andmetele on kooskõlas ka kriminaalmenetluse seadustiku

[47] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 12, 16; EKo *Tele2 Sverige*, p-d 108-111.

[48] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 14.

[49] *Ibid*, lk 14, 15.

(KrMS)[50] § 215 lg-ga 1, mille järgi on uurimisasutuse ja prokuratuuri määrused kriminaalmenetluses kohustuslikud.[51] Töö autori hinnangul püütakse sellisel viisil ilmselt laiendada andmekategooriate ringi, millele menetlejatel on kohtueelses kriminaalmenetluses juurdepääs.

Kui sideettevõtja ärist tulenevatel eesmärkidel enam mingeid andmekategooriaid ei säilita, siis on väljatöötamiskavatsuses ette nähtud, et edasi peab kriminaalmenetluses „olema võimalik juurdepääs ainult neile andmetele, mille säilitamise eesmärk on kriminaalmenetlus sõltuvalt kuriteo raskusest“. Olenemata sellest, et riigi julgeoleku tagamise eesmärgil planeeritakse säilitada kõiki andmeid pikema perioodi jooksul, siis kriminaalmenetluse eesmärgil plaanitakse säilitada teatud andmeid sõltuvalt kuriteo raskusest. Seega kuigi säilitatakse kõiki andmeid, siis kriminaalmenetluse eesmärgil oleks sõltuvalt kuriteo raskusest ette nähtud vaid teatud andmekategooriate säilitamise kohustus.[52]

Lisaks soovitakse teha muudatusi ka andmete säilitamise tähtaegade osas. Kui praegu kehtiva ESS-i kohaselt tuleb kõiki andmeid säilitada ühe aasta jooksul alates sideseansi toimumisest, siis tulevikus soovitakse eristada andmete säilitamise tähtajad lähtudes andmekategooriatest ja andmete säilitamise eesmärkidest. Riigi julgeoleku tagamise eesmärgil soovitakse andmete säilitamiseks võimalikult pikka tähtaega ning leitakse, et ühe aasta pikkune tähtaeg võib olla isegi liiga lühike. Kriminaalmenetluse puhul soovitakse aga eristada, milliseid andmeid säilitatakse mis perioodi jooksul. Samuti leitakse väljatöötamiskavatsuses, et lähtuvalt säilitatavate andmete kategooriast peaksid kehtima erinevad reeglid. Näiteks numbri kasutaja andmeid, mis on väiksema riive ulatusega andmed, tuleks säilitada kauem, tundlikumaid andmeid, näiteks asukohaandmeid, aga lühema perioodi jooksul.[53]

Nagu juba eelpool märgitud, kavatsetakse riigi julgeoleku tagamise eesmärgil säilitada kõiki elektroonilise side metaandmeid. Sel eesmärgil säilitatud andmetele soovitakse ka võimalikult pikka säilitamistähtaega. Olenemata sellest, et kriminaalmenetluse eesmärgil säilitatavate andmekategooriate hulk oleks piiratud ning kriminaalmenetluse eesmärgil säilitataks neid erineva perioodi vältel sõltuvalt andmekategooriast, siis reaalselt tuleks

[50] Kriminaalmenetluse seadustik. – RT I, 13.03.2019, 7.

[51] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 15, 16.

[52] *Ibid*, lk 16.

[53] *Ibid*, lk 16.

väljatöötamiskavatsusest lähtuvalt endiselt edaspidigi säilitada kõiki side metaandmeid ja seda võimalikult pika säilitamistähtaja jooksul. Väljatöötamiskavatsuses plaanitav kõikide elektroonilise side andmete säilitamine ei oleks kooskõlas ka kavandatava e-privaatsuse määrusega, mille järgi tuleb liikmesriikidel arvestada Euroopa Kohtu otsuseid e-privaatsuse direktiivi tõlgendamise kohta.

Säilitamiskohustust analüüsides on väljatöötamiskavatsuses nähtud ka võimalust kohustada sideettevõtjaid säilitama vaid neid andmekoosseise, mida sideettevõtja ärilistel eesmärkidel ei vaja. Väljatöötamiskavatsuses on peetud küsitavaks vajadust kohustada sideettevõtjaid säilitama neid andmeid, mida ettevõtjad säilitavad niigi igal juhul oma ärilistest eesmärkidest tulenevalt. Samas on aga jõutud järeldusele, et kõik sideettevõtjad ei pruugi säilitada ärilistel eesmärkidel samu andmekoosseise ning lisaks võib erineda ka ajaperiood, mille vältel need ettevõtted ärilistel eesmärkidel vajalikke andmeid säilitavad.[54]

Väljatöötamiskavatsuses on tähelepanu pööratud isikutevahelist sidet võimaldavatele internetipõhistele teenustele ehk nn OTT-teenustele. Eelnõu väljatöötamiskavatsuse kohaselt ei laiene praegu kehtiv ESS nimetatud teenustele, kuid tänapäeval on OTT-teenused väga laia kasutusulatusega, mistõttu „sideandmete säilitamise reeglite kohaldamisel OTT-teenustele on mitmeid eeliseid, sealhulgas kõrvaldaks see õigustamatu diferentseerimise nn klassikalise sideteenuse pakkuja ja OTT-teenuse pakkuja vahel“. Lõpuks on väljatöötamiskavatsuses siiski jõutud järeldusele, et kuna Euroopa Liit ei ole nende teenuste osas veel reegleid ühtlustanud, siis ei ole kuni e-privaatsuse määruse rakendamiseni veel asjakohane viia ESS-i sisse OTT-teenuse osutajaid puudutavaid muudatusi ning laiendada neile sideandmete säilitamise kohustust.[55]

Kuigi eelnõu väljatöötamiskavatsuse kohaselt praegu kehtiv ESS OTT-teenustele ei kehti, on käesoleva töö autor arvamusel, et osaliselt reguleerib ka praegu kehtiv ESS OTT-teenuseid. Nimelt on ESS § 111^1 lg 3 kohaselt kohustatud ka Interneti-telefoni teenuse osutaja säilitama lõikes nimetatud andmed. Interneti-telefoni teenus on aga samuti üks OTT-teenustest.[56]

[54] *Ibid*, lk 13.

[55] *Ibid*, lk 13.

[56] ICT Regulation Toolkit. Regulating 'Over-the-Top' Services. Arvutivõrgus: http://www.ictregulationtoolkit.org/toolkit/2.5 (20.04.2019).

Sideandmete säilitamise reeglite kohaldamine kõigile OTT-teenustele oleks ilmselt põhjendatud. Lisaks õigustamatu eristamise kaotamisele erinevate teenusepakkujate vahel, aitaks see ka vältida olukordi, kus tingituna sellest, et klassikalise sideteenuse pakkuja poolt pakutavate sideteenuste kasutamisel side metaandmed säilitatakse, hakatakse kasutama rohkem OTT-teenuseid. Sideandmete säilitamise reeglite OTT-teenustele mitte kohaldamine võib kaasa tuua ka olukorra, kus kurjategijad, püüdes vältida sideandmete säilitamist, hakkavad kuritegude toimepanemisel kasutama OTT-teenuseid.

Eelnõu väljatöötamiskavatsuses on justiitsministeerium pidanud asjakohaseks kaaluda, kas Eestis tuleks loobuda isikustamata kõnekaartidest ning nõuda, et kaardi omaniku isik oleks tuvastatud. Isikustamata kõnekaartide korral ei saa kindlaks teha numbri omanikku. Seetõttu on selliseid kõnekaarte võimalik ära kasutada kurjategijatel ebaseaduslike tegevuste eesmärgil. Sellest tulenevalt on ka mitmed Euroopa Liidu liikmesriigid (näiteks Belgia, Hispaania, Kreeka ja Prantsusmaa) kaotanud võimaluse anonüümsete kõnekaartide kasutamiseks ning kõnekaardi soetamine neis riikides eeldab kõnekaardi ostja isiku tuvastamist. Kuna praegu kehtiva ESS § 111^1 lg 2 p 10 järgi on sideteenuse osutajad kohustatud kõnekaartide puhul säilitama vaid teenuse esmase aktiveerimise kuupäeva ja kellaaja ning kärjetunnuse, millest teenus aktiveeriti, siis peetakse asjakohaseks hinnata, kas ka Eestis oleks vajalik nõuda kaardi omaniku isiku tuvastamist.[57]

Kõnekaardi ostmisel isiku tuvastamine aitaks eeldatavasti kaasa kurjategijate avastamisele, kes kasutavad neid ära süütegude toimepanemisel. Samas aga võib kõnekaartide isikustamisel tekkida olukord, kus ebaseaduslikeks tegevusteks hakatakse kõnekaarte vähem kasutama ning leitakse suhtlemise tarbeks teistsugused vahendid.

1.3. Elektroonilise side andmete säilitamise ja kasutamisega riivatavad põhiõigused

Elektroonilise side andmete säilitamise ja kasutamisega võivad kaasneda mitmesugused põhiõiguste riived. Nendeks on eelkõige perekonna- ja eraelu puutumatuse, kodu puutumatuse ja sõnumite saladuse põhiõiguste riived, samuti sõnavabaduse riive.

[57] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 14.

Inimõiguste ja põhivabaduste kaitse konventsiooni artikkel 8 lg 1 näeb ette nelja eelpool nimetatud inimõiguse kaitse: era- ja perekonnaelu puutumatuse, kodu puutumatuse ja sõnumite saladuse kaitse. Isikuandmete kaitset, mis põhiõiguste hartas on sätestatud artiklis 8, käsitletakse inimõiguste konventsioonis eraelu osana.[58] Seejuures on inimõiguste konventsiooni artikli 8 lõike 2 kohaselt võimalik era- ja perekonnaelu ning kodu puutumatust ja sõnumite saladust piirata, kui see on vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.[59]

Põhiõiguste harta artikkel 7 sätestab samuti igaühe õiguse, et austataks era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust. Harta ingliskeelses versioonis kasutatakse sõnumite kaitse puhul mõistet „communication", mis ei viita vaid edastatavatele sõnumitele ehk kommunikatsiooniprotsessis olevatele sõnumitele ning millega soovitakse privaatsust sõnumite saladuse osas laiemalt kaitsta.[60] Lisaks näeb harta artikkel 8 ette õiguse isikuandmete kaitsele. Seejuures ongi Euroopa Kohus viidanud lahendis *Digital Rights Ireland* sellele, et side metaandmete säilitamine ja vajadusel riigiasutustele kättesaadavaks tegemine riivab harta artikliga 7 tagatud põhiõigust eraelu puutumatusele ning nende andmete töötlemine riivab artikliga 8 tagatud õigust isikuandmete kaitsele.[61]

Põhiõiguste harta selgituste kohaselt vastavad harta artikliga 7 tagatud põhiõigused inimõiguste konventsiooni artiklis 8 nimetatutele ning neil on samasugune tähendus ja ulatus. Seetõttu on piirangud, mida võib neile põhiõigustele kehtestada, samasugused nagu inimõiguste konventsiooni artikli 8 lg-s 2 lubatud piirangud.[62]

---

[58] EIKo 04.12.2008, 30562/04, 30566/04, *S. ja Marper vs. Ühendkuningriik*, p 67.

[59] Isikuandmete kogumist ja töötlemist puudutavat informatsioonilist privaatsust, isikute füüsilise puutumatusega seonduvat kehalist privaatsust, sõnumite saladust puudutavat kommunikatsiooni privaatsust ja kodu puutumatust puudutavat territoriaalset privaatsust on peetud privaatsusõiguse neljaks komponendiks. (D. Banisar, S. Davies. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. – The John Marshall Journal of Information Technology & Privacy Law. 1999/1, lk 6.)

[60] Riigikohus on põhiseaduse § 43 osas, mille sõnastuse kohaselt on igaühel õigus „edastatavate sõnumite saladusele", leidnud, et põhiseaduse § 43 kaitsealas on vaid kommunikatsiooniprotsessis olevad sõnumid. Kohale jõudnud sõnumid on põhiseaduse § 26 kaitsealas. (RKKKo 20.11.2015, 3-1-1-93-15, p 100, RKKKo 30.06.2014, 3-1-1-14-14, p 816.)

[61] EKo *Digital Rights Ireland*, p-d 34-36.

[62] Selgitused põhiõiguste harta kohta. – ELT C 303, 14.12.2007, lk 20.

Eesti Vabariigi põhiseadus[63] sisaldab inimõiguste konventsiooni artikliga 8 sarnaseid põhiõigusi, kuid nii era- ja perekonnaelu puutumatus, kodu puutumatus kui ka sõnumite saladuse kaitse on sätestatud eri paragrahvides. Igaüheõiguse perekonna- ja eraelu puutumatusele tagab põhiseaduse § 26, kodu puutumatust käsitleb § 33 ning õigust edastatavate sõnumite saladusele § 43. Seejuures on erinevad ka nende põhiõiguste riivet õigustavad eesmärgid.

Põhiseaduse § 26 teine lause annab õiguse sekkuda perekonna- ja eraellu tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. §-s 33 sätestatud kodu puutumatust võib piirata samadel eesmärkidel kui era- ja perekonnaelu puutumatust, kuid esinevad ka kaks erisust. Kodu puutumatust võib piirata tõe väljaselgitamiseks kriminaalmenetluses, kuid kõlblust § 33 eraldi eesmärgina ei sätesta. Kolmest eelpool nimetatud põhiseaduse paragrahvist annab põhiseadus kõige kitsamad võimalused sõnumite saladuse riiveks. Nimelt võib põhiseaduse § 43 teise lause kohaselt teha erandeid vaid kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks.

Infotehnoloogia areng loob aga järjest enam olukordi, kus on raske piiritleda eraelu ja kodu puutumatuse ning sõnumite saladuse kaitsealasid. Inimõiguste konventsiooni ja põhiõiguste harta kohaldamisel ei olegi eriti oluline iga kord kindlaks teha, millise konkreetse põhiõiguse rikkumisega on tegemist, kuna riivet õigustavad eesmärgid kattuvad. Kuna põhiõiguste riivet õigustavad eesmärgid on Eesti põhiseaduses erinevad, siis on põhiõiguste tõhusa kohtuliku kontrolli eelduseks, et tehakse kindlaks, kas tegemist on § 26, § 33 või § 43 kaitsealas oleva teo või situatsiooniga.[64]

Elektroonilise side metaandmete säilitamise ja kasutamise kontekstis on eriti oluline sõnumite saladuse kaitseala ulatuse kindlaks tegemine. Euroopa inimõiguste konventsioonis ega põhiõiguste hartas sõnumi edastamise viise ei mainita. Eesti põhiseaduses on aga antud lahtine loetelu sõnumite edastamise viiside kohta. Siiski räägib põhiseadus õigusest sõnumite saladusele, mida edastatakse üksnes üldkasutataval teel. Põhiseaduse § 43 eesmärgipärase tõlgenduse korral on leitud, et säte kaitseb sõnumite vahetust hoolimata selle iseloomust,

[63] Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.

[64] U. Lõhmus. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014, lk 310.

kitsama tõlgenduse puhul on leitud, et muul viisil kui üldkasutataval teel edastatud sõnumid kuuluvad eraelu puutumatuse kaitsealasse.[65]

Eriti probleemne on aga sõnumi mõiste maht. Kui sõnumi sisu suhtes ollakse üksmeelel, et see kuulub sõnumi saladuse kaitsealasse, siis sidega kaasnevate metaandmete puhul selline üksmeel puudub.[66] Näiteks ei kaitse Saksa Liidukonstitutsioonikohtu otsuse kohaselt Saksa põhiseaduse §-s 10 sätestatud õigus korrespondentsi, posti ja telekommunikatsiooni privaatsusele üksnes kommunikatsiooni sisu, vaid ka kommunikatsiooniga seotud andmeid. Samuti on ÜRO inimõiguste nõukogu raportis väljendusvabaduse kaitse ja edendamise kohta leitud, et kommunikatsiooniandmed on teave isiku suhtluse kohta, identiteet, kontod, aadressid, külastatud veebilehed, raamatud ja teised loetud, vaadatud või kuulatud materjalid, otsingud ning liiklus-ja asukohaandmed.[67]

Euroopa Inimõiguste Kohtu praktika kohaselt kuuluvad samuti nii sõnumite sisu kui ka metaandmed sõnumite saladuse kaitsealasse. Asjas *Copland vs. Ühendkuningriik* on inimõiguste kohus leidnud, et telefoni, elektronposti ning internetikasutusega seotud andmete kogumise ja säilitamisega sekkutakse isiku õigusesse eraelu ja korrespondentsi austamisele.[68] Oluline on tähelepanu pöörata sellele, et kasutatud on mõistet „korrespondents", mis ei ole samastatav sõnumi sisuga.[69]

Nii inimõiguste konventsiooni kui ka Euroopa Liidu põhiõiguste harta inglis- ja prantsuskeelses versioonis[70] kasutatakse vastavalt mõisteid „korrespondents" ja „kommunikatsioon". Erinevalt inimõiguste konventsiooni uuendatud eestikeelsest tõlkest, mis kasutab mõistet sõnumite saladus, oli ka inimõiguste konventsiooni varasemas eestikeelses versioonis[71] kasutusel termin „korrespondents". „Kommunikatsioon" ja „korrespondents" tähendavad teate edastamist ja vastuvõtmist. Need on laiema tähendusulatusega mõisted, mis hõlmavad nii teate sisu kui ka

[65] U. Lõhmus. Põhiõigused kriminaalmenetluses, lk 328, 329; RKKKo 21.03.2003, 3-1-1-25-03, p 8.2.

[66] *Ibid*, lk 330.

[67] U. Lõhmus. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. – Juridica III/2016, lk 179; F. La Rue. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 17.04.2013. A/HRC/23/40, lk 3. Arvutivõrgus: www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/23/40 (21.04.2019).

[68] EIKo 03.04.2007, 62617/00, *Copland vs. Ühendkuningriik*, p 44.

[69] U. Lõhmus. Põhiõigused kriminaalmenetluses, lk 331.

[70] Inimõiguste ja põhivabaduste kaitse konventsiooni inglis- ja prantsuskeelne variant on kättesaadavad Euroopa Inimõiguste Kohtu kodulehelt. Arvutivõrgus: https://www.echr.coe.int/Pages/home.aspx?p=basictexts/convention (12.04.2019).

[71] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2000, 11, 57.

selle liikumise kohta käivaid andmeid ehk metaandmeid. „Sõnum“ seevastu tähistab ainuüksi teadet. Terminite erinev tähendus võib ka olla üheks põhjuseks, miks erinevad inimõiguste konventsiooni ja Eesti põhiseaduse kohaldamispraktika.[72]

Nimelt on Eesti seadusandja välistanud sõnumite saladuse kaitse sätestava põhiseaduse § 43 kohaldamisalast side metaandmed. Sellele järeldusele on muuhulgas jõutud kriminaalmenetluse seadustiku muutmise eelnõu seletuskirjas, kus tulenevalt sellest, et sõnumite edastamise faktiga seotud asjaolude kohta päringu tegemisel ei ole vajalik kohtu luba, on järeldatud, et ESS § 111^1 toodud andmed ei ole põhiseaduse § 43 kaitsealas, kuna viimane eeldab sõnumisaladuse õiguse piiramiseks kohtu luba.[73] Ka põhiseaduse kommenteeritud väljaandes on toodud välja, et kuna metaandmetest ei selgu sõnumi sisu, siis kuulub selliste andmete kogumine valitseva arvamuse kohaselt eraelu ehk põhiseaduse § 26 kaitsealasse.[74]

Riigikohtu praktika kinnitab samuti side metaandmete kuulumist põhiseaduse § 26 kaitsealasse. 2015. aastal tehtud Riigikohtu otsuses leiti, et elektroonilise side võrgu operaatorilt või posti- või elektroonilise side teenuse osutajalt üldkasutatava elektroonilise side võrgu kaudu edastatavate sõnumite kohta andmete kogumine, säilitamine ja kriminaalmenetluses kasutamine, et kindlaks teha sõnumi edastamise fakt, kestus, viis, vorm ja sõnumi edastaja või vastuvõtja isikuandmed ning asukoht, riivavad õigust eraelu puutumatusele.[75] A. Lott on viidanud ka sellele, et põhiseaduse § 43 järgi õigustab kriminaalmenetluse kõrval sõnumisaladuse riivet ainult kuriteo tõkestamise eesmärk. Seetõttu metaandmete arvamisel sõnumisaladuse kaitsealasse seaks see olulisi piiranguid, kuna kehtiva õiguse järgi saab metaandmete kohta päringuid teha isegi väärteomenetluses.[76]

Põhiseaduse kommentaaride järgi on õigus sõnumite saladusele kujunenud ajalooliselt vajaduse tõttu tagada puutumatus vahendaja kaudu liikuvatele sõnumitele ja luua usaldust teenuse osutaja suhtes.[77] A. Lott on seisukohal, et seadusandja otsus käsitada päringute tegemist

[72] U. Lõhmus. Põhiõigused kriminaalmenetluses, lk 328, 331, 332.

[73] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 175 SE. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, lk 4. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0 (02.04.2019).

[74] S. Laos, H. Sepp. PõhiSK § 43/10. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 4. vlj. Tallinn: Juura 2017.

[75] RKKKo 23.02.2015, 3-1-1-51-14, p-d 19, 20.

[76] A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Tartu, 2015, lk 26, 27.

[77] S. Laos, H. Sepp. PõhiSK § 43/4.

metaandmete kohta väljaspool põhiseaduse §-i 43 võib olla vastuolus sõnumite saladuse kaitseala eesmärgiga ning metaandmete kaitsetaseme vähendamise asemel oleks vajalik pigem selle tugevdamine või säilitamine.[78] Ka põhiseaduse kommentaarides on nenditud, et vajadus sõnumi sisu ja metaandmete eristamise järele on vähenenud infoühiskonna ja tehniliste võimaluste arengu tõttu.[79] Sõnumi sisu ja metaandmeid mitte eristades ja mõlemad põhiseaduse § 43 kaitsealasse arvates tekiks aga olukord, kus nii sõnumi sisu kui ka metaandmete saladuse riivet õigustaks vaid kuriteo tõkestamise või kriminaalmenetluses tõe väljaselgitamise eesmärk.

Seega on elektroonilise side metaandmete säilitamine ja kasutamine Euroopa Kohtu ja Euroopa Inimõiguste kohtu praktika kohaselt vastavalt põhiõiguste harta artikli 7 ja inimõiguste konventsiooni artikli 8 kaitsealas, mis tagavad era- ja perekonnaelu puutumatuse, kodu puutumatuse ja sõnumite saladuse kaitse. Seevastu Eesti põhiseaduse kohaldamispraktika näitab, et põhiseaduse § 43 kaitsealas on vaid sõnumi sisu, side metaandmed on aga eraelu puutumatust sätestava põhiseaduse § 26 kaitsealas.

Lisaks on Euroopa Kohus viidanud lahendis *Tele2 Sverige* sellele, et elektroonilise side teenuste osutajate kohustus säilitada side metaandmeid, et need vajadusel liikmesriigi ametiasutustele kättesaadavaks teha, võib riivata harta artikliga 11 tagatud sõnavabadust.[80] Põhiõiguste harta artikli 11 lg 1 järgi on igaühel õigus sõnavabadusele, mis kätkeb arvamusvabadust, vabadust saada ja levitada teavet ja ideid ilma avaliku võimu sekkumiseta. Põhiõiguste harta selgituste kohaselt vastab artikkel 11 inimõiguste konventsiooni artiklile 10, mis on oma sõnastuselt vägagi sarnane põhiõiguste harta artikliga 11.[81]

Sõnavabaduse kohta on Euroopa Kohus öelnud, et see on üks demokraatliku ja pluralistliku ühiskonna põhialus ning väärtus, millele Euroopa Liit rajaneb.[82] Elektroonilise side metaandmete säilitamine võib aga mõjutada elektrooniliste sidevahendite kasutamist ja seetõttu mõjutada ka sõnavabaduse teostamist.[83] Kahjuks ei ole aga lahendites *Digital Rights Ireland* ja *Tele2 Sverige* sõnavabaduse riivet põhjalikumalt analüüsitud ning piirdutud on vaid eelpool

[78] A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis, lk 27.
[79] S. Laos, H. Sepp. PõhiSK § 43/10.
[80] EKo *Tele2 Sverige*, p 92.
[81] Selgitused põhiõiguste harta kohta, lk 21.
[82] EKo *Tele2 Sverige*, p 93; EKo 06.09.2011, C-163/10, *Patriciello*, p 31.
[83] EKo *Tele2 Sverige*, p 101, EKo *Digital Rights Ireland*, p 28.

välja toodud tõdemustega. Siiski näitab lahendites leitu seda, et isikute teadmine sideandmete säilitamisest mõjutab ka sõnavabaduse kasutamist.

Ka elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsuses pööratakse tähelepanu põhiõiguste kaitsele ning riivatavatele põhiõigustele. Väljatöötamiskavatsuse kohaselt puudutab kavandatav regulatsioon mitmeid põhiõigusi ja -vabadusi. Muuhulgas puudutab see põhiseaduse §-st 11 tulenevat põhimõtet, et õigusi ja vabadusi tohib piirata vaid kooskõlas põhiseadusega ning piirangud peavad olema demokraatlikus ühiskonnas vajalikud ja ei tohi moonutada piiratavate õiguste ja vabaduste olemust. Samuti puudutab see põhiseaduse §-st 19 tulenevat õigust vabale eneseteostusele ning informatsioonilisele enesemääramisele, mis hõlmab isiku õigust otsustada, kas ja kui palju tema kohta andmeid kogutakse ja salvestatakse, põhiseaduse §-st 26 tulenevat õigust perekonna- ja eraelu puutumatusele, §-st 33 tulenevat õigust kodu puutumatusele ning §-st 43 tulenevat igaühe õigust tema poolt või temale üldkasutataval teel edastatavate sõnumite saladusele.[84]

Eelnõu väljatöötamiskavatsuses on nenditud ka väljatöötatava regulatsiooni seotust inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8, mille järgi on igaühel õigus era- ja perekonnaelu, kodu ning sõnumite saladuse austamisele. Samuti puudutab kavandatav regulatsioon Euroopa Liidu põhiõiguste harta artiklit 7, mille järgi on igaühel õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust ning artikliga 8, mis sätestab õiguse isikuandmete kaitsele. Seega näib, et eelnõu väljatöötamisel pööratakse tähelepanu põhiõigustele, mida elektroonilise side andmete säilitamise ja kasutamisega eelkõige riivatakse.[85]

[84] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 22.
[85] *Ibid*, lk 22, 23.

2. Elektroonilise side andmete kasutamine

2.1. Elektroonilise side andmete kasutamine Euroopa Liidu õiguses

2.1.1. Euroopa Kohtu praktika elektroonilise side andmete kasutamise kohta

2018. aasta oktoobris tegi Euroopa Kohus otsuse asjas *Ministerio Fiscal,* kus Hispaania kohus esitas eelotsusetaotluse seoses direktiivi 2002/58 artikli 15 lõike 1 tõlgendamisega. Täpsemalt soovis eelotsusetaotluse esitanud kohus teada, kas avaliku võimu juurdepääs perekonnanimele, eesnimele ja vajaduse korral ka aadressile, millega saab tuvastada varastatud mobiiltelefonis avatud SIM-kaartide omanikke, kujutab endast harta artiklitega 7 ja 8 tagatud põhiõiguste riivet, mis on nii raske, et kuritegude ennetamisel, uurimisel, avastamisel ja menetlemisel tuleks juurdepääsu sellistele andmetele piirata võitlusega raske kuritegevuse vastu ning milliste kriteeriumide alusel tuleb sellisel juhul kuriteo raskust hinnata.[86]

Euroopa Kohus täpsustas otsuses *Ministerio Fiscal*, mida tuleb võtta arvesse hindamaks, kas kuriteod on piisavalt rasked, et põhjendada elektroonilise side andmetele juurdepääsuga kaasnevat sekkumist põhiõigustesse. Kohus nentis, et avaliku võimu juurdepääs neile andmetele riivab põhiõigust eraelu austamisele olenemata sellest, kas eraelulised andmed on delikaatsed või kas puudutatud isikud on pidanud riive pärast taluma ebamugavusi ning riivab ka põhiõigust isikuandmete kaitsele. Euroopa Kohus märkis, et direktiivi 2002/58 artikli 15 lg 1 lauses 1 toodud eesmärkide loetelu on ammendav, mistõttu saab juurdepääs elektroonilise side teenuste osutajate säilitatavatele andmetele toimuda ainult neil eesmärkidel. Nimetatud lause sõnastus aga peab silmas kuritegusid üldiselt ning ei piira kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärki võitlusega vaid raskete kuritegude vastu.[87]

Otsuses *Ministerio Fiscal* viidati otsuse *Tele2 Sverige* punktile 99, milles Euroopa Kohus leidis, et juurdepääsu andmine sideteenuste osutajate säilitatavatele isikuandmetele, mis üheskoos võimaldavad teha täpseid järeldusi nende isikute eraelu kohta, kelle andmeid säilitatakse, saab põhjendada ainult võitlusega raske kuritegevuse vastu. Samuti leiti otsuses *Ministerio Fiscal,* viidates otsuse *Tele2 Sverige* punktile 115, et kohus olevat põhjendanud eelnimetatud

[86] EKo *Ministerio Fiscal,* p 48.
[87] *Ibid,* p-d 51-53.

tõlgendust asjaoluga, et juurdepääsu reguleerivate normidega taotletav eesmärk peab olema proportsioonis selle tegevusega kaasneva põhiõiguste riive raskusega.[88]

Otsuse *Tele2 Sverige* punktist 115 aga esmapilgul sellist muljet ei jää. Nimelt leidis seal Euroopa Kohus, et liikmesriigi õigusnormidega taotletav eesmärk peab olema proportsioonis andmetele juurdepääsuga kaasneva põhiõiguste riive raskusega, millest järelduvalt saab kuritegude ennetamise, uurimise, avastamise ja menetlemise puhul säilitatavatele andmetele juurdepääsu andmist põhjendada ainult võitlusega raske kuritegevuse vastu.[89] Lisaks leidis otsuses *Tele2 Sverige* Euroopa Kohus, et „kuritegevuse vastu võitlemise eesmärgil [tohib] anda juurdepääsu ainult nende isikute andmetele, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või eelnevas toimepanemises või niisuguse kuriteoga ühel või teisel viisil seotud olemises".[90] Seega tõi kohus küll välja proportsionaalsuse hindamise kohustuse, kuid samas leidis, et säilitatavatele andmetele juurdepääsu andmist saab põhjendada vaid võitlusega raske kuritegevuse vastu.

Otsuses *Ministerio Fiscal* selgitas kohus nimetatud proportsionaalsuse põhimõtet. Proportsionaalsuse põhimõtte alusel saab rasket riivet kuritegude ennetamisel, uurimisel, avastamisel ja menetlemisel põhjendada üksnes võitlusega sellise kuritegevuse vastu, mida tuleb pidada raskeks.[91] Vastupidisel juhul, kui andmetele juurdepääsuga kaasnev riive ei ole raske, võib juurdepääsu põhjendada üldiselt kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga.[92] Seega selgitas kohus selles otsuses proportsionaalsuse põhimõtet selgelt ja üheselt arusaadavalt.

Samas kohtuasjas võttis Euroopa Kohus arvesse põhikohtuasja asjaolusid ning hindas, kas arvestades seda, millistele andmetele taotles kriminaalpolitsei juurdepääsu, on tegemist põhiõiguste raske riivega. Andmed, millele politsei juurdepääsu soovis, võimaldasid tuvastada vaid SIM-kaardi omanike identiteeti, kelle SIM-kaart avati teatud ajavahemiku jooksul varastatud mobiiltelefonis. Kui andmeid, millele juurdepääsu taotleti, ei võrrelda SIM-kaartidelt lähtuva side andmetega ja asukohaandmetega, siis ei saa teada SIM-kaardilt või SIM-kaartidelt lähtuva side kuupäeva, kellaaega, kestust ega adressaati, side toimumise kohta ega

[88] *Ibid*, p-d 54, 55.
[89] EKo *Tele2 Sverige*, p 115.
[90] *Ibid*, p 119.
[91] EKo *Ministerio Fiscal*, p 56.
[92] *Ibid*, p 57.

side sagedust teatud isikutega kindla ajavahemiku vältel. Seetõttu ei saa taotletud andmete pinnalt teha täpseid järeldusi nende isikute eraelu kohta, kelle andmetele juurdepääsu sooviti. Eelneva põhjal tegi kohus järelduse, et isikute, kelle andmetele juurdepääsu taotleti, põhiõiguste riivet ei saa pidada raskeks.[93] Kuna põhikohtuasjas taotletud andmetele juurdepääsuga kaasnevat riivet ei saanud pidada raskeks, siis tulenevalt proportsionaalsuse põhimõttest sai konkreetsel juhul andmetele juurdepääsu põhjendada üldiselt kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga.[94]

Sellest ilmneb lahendite *Ministerio Fiscal* ja *Tele2 Sverige* vahel mõningane ebakõla ning tekib küsimus, kas Euroopa Kohus võib pidada seaduslikuks selliste andmete kasutamist, mille säilitamine on seadusega vastuolus. *Ministerio Fiscal* lahendi põhjal olid Hispaania elektroonilise sideteenuse pakkujad kohustatud säilitama „nende poolt elektroonilise side teenuste või üldkasutatavate sidevõrkude teenuste osutamisel loodavaid või töödeldavaid andmeid".[95] Kohus ei analüüsinud ega viidanud sellele, et üleüldiselt kõigi metaandmete säilitamise vastuolu tõttu Euroopa Liidu õiguse ja põhiõigustega, oleks nendele andmetele juurdepääs samuti keelatud. Otsuses tõdeti vaid, et eelotsusetaotlus puudutab vaid küsimust, kas ja millises ulatuses saab vaidlusaluste normide eesmärgiga põhjendada kriminaalpolitsei juurdepääsu elektroonilise side andmetele.[96] Seega ei pidanud kohus vajalikuks eelnevalt analüüsida sideandmete säilitamise seaduspärasust. Seetõttu on võimalik, et Euroopa Kohus lubab juurdepääsu andmetele, mille säilitamine *Tele2 Sverige* otsuse põhjal on Euroopa Liidu õigusega vastuolus ning ebaseaduslik.

Kuna Euroopa Kohtu hinnangul ei olnud asjas *Ministerio Fiscal* põhiõiguste riive raske, siis ei selgitanud Euroopa Kohus seda, milliste kriteeriumide alusel tuleb kuriteo raskust hinnata. Seega ei ole teada, milliste kriteeriumide abil tuleb kindlaks teha kuriteo raskus juhul, kui asjaomased asutused taotlevad juurdepääsu elektroonilise side andmetele, millega kaasneb raske põhiõiguste riive.

Kuriteo raskuse iseloomustamiseks kriteeriumide kindlaksmääramist on käsitlenud aga kohtujurist oma ettepanekus otsusele *Ministerio Fiscal*.[97] Kohtujurist oli arvamusel, et mõiste

[93] *Ibid*, p-d 60, 61.
[94] *Ibid*, p 62.
[95] *Ibid*, p 12.
[96] *Ibid*, p 49.
[97] EK C-207/16, *Ministerio Fiscal*, kohtujurist H. Saugmandsgaard Øe ettepanek.

„raske kuritegu“ ei kujuta endast liidu õiguse autonoomset mõistet, mille sisustamine oleks Euroopa Kohtu pädevuses, kuna karistusõiguse ja kriminaalmenetluse normid kuuluvad liikmesriikide pädevusse ning on liikmesriigi pädevate asutuste määrata. Teise võimalusena oli kohtujurist arvamusel, et kui Euroopa Kohtu arvates on tegemist autonoomse mõistega, siis ei tuleks kuriteo raskust mõõta kuriteo eest ette nähtud karistusest lähtudes, vaid tuleks arvestada ka teisi hindamiskriteeriume. Teiste hindamiskriteeriumidena toob kohtujurist välja näiteks väidetava kuriteo toimepanemise asjaolud – kas tegemist oli tahtliku süülise käitumisega, kas esines raskendavaid asjaolusid ja kas tegemist oli korduva süüteo toimepanemisega – ning kui olulisi ühiskondlikke huve võis toimepanija kahjustada ja millist liiki ja kui suurt kahju sellega põhjustati kannatanule.[98]

Lisaks käsitles kohtujurist võimalust, et kuriteo raskus tuleb kindlaks määrata võttes arvesse vaid selle eest ette nähtud karistust. Sellisel juhul ei saa karistuse raskust, mille põhjal käsitada kuritegu raskena, kogu Euroopa Liidu territooriumil ühte moodi kindlaks määrata. Seetõttu võivad liikmesriigid ise kindlaks määrata minimaalse karistuse, mille alusel pidada kuritegusid raskeks, kui liikmesriigid teevad seda kooskõlas nõudega, et põhiõiguste harta artiklites 7 ja 8 tagatud põhiõiguste riive peab olema erandlik ja kooskõlas proportsionaalsuse põhimõttega.[99]

2.1.2. Elektroonilise side andmete kasutamine kavandatava e-privaatsuse määruse kohaselt

E-privaatsuse määruse ettepaneku seletuskirja kohaselt säilitatakse e-privaatsuse määruses e-privaatsuse direktiivi artikli 15 sisu ja see viiakse isikuandmete kaitse üldmääruse artikli 23 sõnastusega vastavusse.[100] Kuna e-privaatsuse direktiivi artiklis 15 on sätestatud teatud tingimused, mille alusel võib piirata muuhulgas side konfidentsiaalsusest tulenevaid õiguseid ja kohustusi, on sellega sisuliselt seotud ettepaneku põhjendus 26. Määruse ettepaneku põhjenduse 26 kohaselt tuleb määruses ette näha võimalus, et Euroopa Liit või selle liikmesriigid võivad teatud tingimustel õigusaktidega piirata teatavaid kohustusi ja õigusi, et kaitsta avalikke huve, muuhulgas avalikku julgeolekut ning kuritegude tõkestamist, uurimist ja avastamist või nende eest vastutusele võtmist. Seejuures tuleb arvestada, et liikmesriikide

[98] *Ibid*, p-d 93-96, 102-105.
[99] *Ibid*, p-d 109, 111, 113-115, 121.
[100] Ettepanek, lk 3.

võetavad meetmed oleksid vajalikud ja proportsionaalsed avaliku huvi kaitsmiseks kooskõlas Euroopa Liidu põhiõiguste hartaga ning Euroopa inimõiguste ja põhivabaduste kaitse konventsiooniga, arvestades Euroopa Liidu Kohtu ja Euroopa Inimõiguste Kohtu tõlgendusi.[101]

Ettepaneku artiklis 11 sisaldub erand sideandmete konfidentsiaalsusest, mille tegemine on lubatud side konfidentsiaalsust sätestava artikli 5 alusel. Nimetatud erand on sarnane e-privaatsuse direktiivi artiklis 15 sätestatud erandile, mille sisu säilitamist uues e-privaatsuse määruses lubati ka ettepaneku seletuskirjas. Ettepaneku artikli 11 lg 1 järgi võib Euroopa Liidu või liikmesriigi õigus piirata muuhulgas artiklis 5 sätestatud kohustuste ja õiguste ulatust, kui sellise piirangu puhul austatakse põhiõiguste ja -vabaduste olemust. Lisaks on eelduseks see, et piirang on vajalik, asjakohane ja proportsionaalne meede demokraatlikus ühiskonnas üldise avaliku huvi kaitsmiseks, millele on osutatud määruse 2016/679 artikli 23 lõike 1 punktides a-e, või jälgimise, kontrolli või regulatiivsete ülesannete täitmiseks, mis on seotud avaliku võimu teostamisega selliste huvide jaoks.[102]

Isikuandmete kaitse üldmääruse artikkel 23 lg 1 punktid a-e, millele viidati ettepaneku artiklis 11, näevad ette võimaluse õiguste ja kohustuste piiramiseks, et tagada riigi julgeolek, riigikaitse, avalik julgeolek, süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine või kriminaalkaristuste täitmisele pööramine, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmine ja nende ennetamine. Samuti on piiramine lubatud, et tagada liidu või liikmesriigi muud üldist avalikku huvi pakkuvad olulised eesmärgid, eelkõige liidu või liikmesriigi oluline majanduslik või finantshuvi, sealhulgas rahandus-, eelarve- ja maksuküsimused, rahvatervis ja sotsiaalkindlustus.

Euroopa Parlamendi seadusandliku resolutsiooni projektis[103] on toodud muudatusettepanek määruse ettepaneku artikli 11 kohta. Muudatusettepaneku artikkel 11b lg 1 punktid a-c näevad sarnaselt isikuandmete kaitse üldmääruse artikkel 23 lg 1 punktidele a-c ette, et määruse ettepaneku artiklis 5 sätestatud õiguste piiramine on lubatud riigi julgeoleku, riigikaitse ja avaliku julgeoleku kaitsmiseks. Sama muudatusettepaneku artikkel 11b lg 1 punkt d sätestab aga, et artiklis 5 kirjeldatud õiguste piiramine on õigustatud raskete kuritegude tõkestamise,

[101] *Ibid*, lk 18.

[102] *Ibid*, lk 28.

[103] Raport ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). Menetlus 2017/0003(COD). Muudatusettepanek nr 119-121.

uurimise, avastamise või nende eest vastutusele võtmise, elektroonilise sidesüsteemi volitamata kasutamise või kriminaalkaristuste täitmisele pööramise, sealhulgas avalikku julgeolekut ähvardavate ohtude eest kaitsmise ja nende ennetamiseks. Seega on muudatusettepanekus soovitud kitsendada eesmärki, mille alusel saab elektroonilise side andmetesse sekkumine olla põhjendatud, võitlusega vaid raske kuritegevuse vastu.

Seega on e-privaatsuse määruse ettepanekus soovitud sideandmete kasutamise eesmärki muuta tulevikus kitsamaks kui seda lubati tulenevalt proportsionaalsuse põhimõttest Euroopa Kohtu lahendis *Ministerio Fiscal*. Nagu eelpool käsitletud, tuleb sellest lahendist tulenevalt arvestada proportsionaalsuse põhimõtet, mille järgi juhul, kui õiguste riive ei ole raske, ei ole põhjendatud ka andmetele juurdepääsu piiramine vaid raskete kuritegude tõkestamise, uurimise ja avastamisega. Seetõttu võib kohtupraktika kohaselt juhul, kui õiguste riive ei ole raske, olla põhjendatud sideandmetele juurdepääs ka üldiselt kuritegude tõkestamiseks, uurimiseks ja avastamiseks. Kavandatava e-privaatsuse määruse kohaselt oleks muudatusettepanekut arvesse võttes õiguste piiramine ning sideandmete säilitamine ja kasutamine põhjendatud vaid võitlusega raske kuritegevuse vastu.

Seega juhul kui nimetatud muudatusettepanekut võetakse arvesse ja see hakkab tulevikus e-privaatsuse määruse jõustumisel kehtima, siis oleks liikmesriikidel võimalik side metaandmete säilitamine ja neile juurdepääs vaid piiratud tingimustel – kuritegude tõkestamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks ainult raskete kuritegude puhul. E-privaatsuse määruse ettepanekus ei ole kuritegude raskuse hindamiseks kriteeriume antud. Nagu eelpool käsitletud, siis ei ole ka Euroopa Kohus selgitanud, mille alusel kuritegude raskust hinnata. Tõenäoliselt jääks see liikmesriikide endi hinnata. Liikmesriikidel tuleks seejuures ilmselt arvestada ka *Tele2 Sverige* lahendist tuleneva põhimõttega, et erand andmete säilitamise keelust ei tohi saada reegliks.[104]

[104] EKo *Tele2 Sverige*, p 89.

2.2. Euroopa Inimõiguste Kohtu hiljutine praktika

2016. aasta otsuses asjas *Figueiredo Teixeira vs. Andorra* on Euroopa Inimõiguste Kohus analüüsinud elektroonilise side metaandmete säilitamise ja kohtule edastamise vastavust inimõiguste konventsiooni artiklile 8. Esmalt hindas kohus, kas andmete säilitamine ja edastamine olid ettenähtavad. Kohus leidis, et selline sekkumine põhiõigustesse oli Andorras seadusega ette nähtud. Lisaks võttis inimõiguste kohus arvesse , et Andorra kriminaalmenetluse seadustik nõudis kohtutelt põhjendatud otsuse esitamist, milles selgitatakse meetme vajalikkust ja proportsionaalsust ning kogutud tõendeid ja uuritava kuriteo raskust. Kohus rõhutas, et sätestatud olid mitmed kuritarvituste vastased kaitsemeetmed. Näiteks kohtuniku poolt eelneva loa andmine, kohaldamine vaid väga raskete kuritegude puhul, meetme kasutamist piirav tähtaeg ning võimalus vaidlustada menetluse käigus kogutud tõendite õiguspärasus. Kohus leidis, et siseriikliku õiguse kohaldamine oli inimõiguste konventsiooni artikli 8 lg 2 tähenduses ettenähtav.[105]

Põhiõigustesse sekkumise õigustatuse ja proportsionaalsuse osas leidis kohus, et põhiõigustesse sekkumine oli õigustatud, kuna see oli vajalik kuritegevuse ennetamiseks, mis on üheks inimõiguste konventsiooni artikli 8 lõikes 2 loetletud õigustavaks eesmärgiks. Samuti leidis kohus, et meede oli proportsionaalne, kuna Andorra ametivõimud olid järginud, et eriuurimismeetodite kasutamine ja sellega taotletav eesmärk oleksid omavahel proportsionaalsed ning kasutanud vähem põhiõigustesse sekkuvat meetodit, et võimaldada kuriteo avastamist, ennetamist ja selle eest vastutusele võtmist.[106]

Euroopa Inimõiguste Kohus on otsuses *Ben Faiza vs. Prantsusmaa* teinud vahet isiku asukoha sideteenuse osutajalt saadud andmete abil tagantjärele kindlaks tegemisel ning isiku asukoha jälgimisel reaalajas. Inimõiguste kohus analüüsis mobiilsideoperaatorile antud korraldust sissetulevate ja väljaminevate kõnede nimekirja esitamiseks nelja mobiiltelefoni kohta koos mobiilimastide nimekirjaga, mille levialas need mobiiltelefonid on olnud. Prantsusmaa õigusaktide kohaselt võisid prokurörid või uurijad prokuratuurilt loa saamisel nõuda ettevõtetelt, organisatsioonidelt, isikutelt, institutsioonidelt ja ametiasutustelt nende valduses olevaid dokumente, mis on vajalikud uurimise läbiviimiseks. Kohus märkis, et Prantsusmaa

[105] EIKo 8.11.2016, 72384/14, *Figueiredo Teixeira vs. Andorra*, p-d 38, 39, 42, 43, 47.
[106] *Ibid*, p 48-51.

kassatsioonikohtu praktika kohaselt kasutatakse seda sätet ka telefonioperaatoritelt isikuandmete taotlemiseks, mis ei hõlma side sisu.[107]

Inimõiguste kohus leidis, et seaduses olid olemas mitmed tagatised kuritarvituste vastu. Päringu esitamiseks oli vajalik prokuratuuri eelnev luba, sellest kohustusest ei saanud kõrvale kalduda ilma, et see muudaks toimingu tühiseks. Päringu õiguspärasust sai tagantjärele hinnata kohus kriminaalmenetluses vastava isiku suhtes ning juhul, kui päring oli õigusvastane, oli kohtul võimalik sellisel teel saadud tõendid välja jätta. Kokkuvõttes leidis kohus, et sideandmete nõudmine sideettevõtjatelt oli seadusega kooskõlas, seadus andis kuritarvituste vastu ka mitmed tagatised, samuti oli põhiõigusesse sekkumine õigustatud ning demokraatlikus ühiskonnas vajalik, mistõttu kohus ei tuvastanud konventsiooni artikli 8 rikkumist.[108]

Euroopa Inimõiguste Kohus on seega pidanud inimõiguste konventsiooni artikliga 8 kooskõlas olevaks sideoperaatorite poolt säilitatud metaandmetele juurdepääsu taotlemist, et viia läbi kriminaalmenetlust. Side metaandmete säilitamise ja kasutamise puhul on kohus üheks eelduseks pidanud säilitamise ja kasutamise ettenähtavust seadusest. Seejuures on inimõiguste kohus hinnanud ka kuritarvitamise vastaste tagatiste olemasolu, sealhulgas eelneva loa taotlemist ning päringu õiguspärasusele tagantjärele hinnangu andmist kohtu poolt.

Seoses sideandmete säilitamise ja kasutamisega tegi Euroopa Inimõiguste Kohus järgmise lahendi 19. juunil 2018. aastal. Lisaks sellele, et Rootsi poolt sideandmete säilitamist ja kasutamist on analüüsinud Euroopa Kohus lahendis *Tele2 Sverige*, on Rootsi seadusandlust massilise kommunikatsiooniandmete kogumise kohta signaalluures analüüsinud inimõiguste kohus otsuses *Centrum för Rättvisa vs. Rootsi*. Selles kaasuses esitas Rootsis inimõigusi kaitsev mittetulundusorganisatsioon kaebuse, milles väitis, et Rootsi õigusnormid signaalluure valdkonnas rikuvad inimõiguste ja põhivabaduste kaitse konventsiooni artiklis 8 sätestatud õigusi. Kaebaja arvates esines oht, et tema teabeedastust on pealt kuulatud ja seda uuritakse signaalluure abil.[109]

Rootsi õigusnormide kohaselt on signaalluure üks välisluure vormidest, mida kasutatakse vaid riikliku julgeoleku tagamise eesmärgil. Teabevahetust, mille puhul nii edastaja kui ka

[107] EIKo 8.02.2018, 31446/12, *Ben Faiza vs. Prantsusmaa*, p-d 7, 70, 72, 74.
[108] *Ibid*, p-d 73, 77-80.
[109] EIKo 19.06.2018, 35252/08, *Centrum för Rättvisa vs. Rootsi*, p-d 3, 6.

vastuvõtja asuvad Rootsis, pealt ei kuulata. Signaalluure abil informatsiooni kogumine on lubatud vaid side puhul, mis ületab Rootsi riigipiire. Seejuures kogutakse signaalluure abil informatsiooni nii side sisu kui ka side metaandmete kohta. Signaalluure abil teabe saamiseks on vajalik eelnev luba spetsiaalse välisluure kohtu poolt.[110]

Euroopa Inimõiguste Kohtu argumentatsioon, hinnates Rootsi välisluure seaduse alusel era- ja perekonnaelu austamise põhiõigusesse sekkumist, põhines kohtu varasemale otsusele asjas *Roman Zakharov vs. Venemaa*[111]. Kohus hindas, kas asjas *Centrum för Rättvisa* oli nimetatud põhiõigusesse sekkumine kooskõlas seadusega ja demokraatlikus ühiskonnas vajalik. Lahendis *Roman Zakharov vs. Venemaa* oli kohus selgitanud, et kooskõla seadusega tähendab, et seadus peab olema asjaomasele isikule ligipääsetav ning selle mõju peab olema ettenähtav. Õiguspärase eesmärgi saavutamiseks era- ja perekonnaelu austamise põhiõigusesse sekkumise vajalikkuse kohta demokraatlikus ühiskonnas on kohus öelnud, et tasakaalustamaks riigi huve riigi julgeoleku kaitsmisel salajase jälgimise abil ja isikutele konventsiooni artiklist 8 tuleneva põhiõiguse riivet, on riigil teatav kaalutlusruum valida vahendid õiguspärase eesmärgi, riigi julgeoleku tagamise, saavutamiseks. Riikliku julgeoleku tagamiseks teostatav salajane jälgimine võib aga demokraatiat selle kaitsmise asemel hoopis kahjustada. Seetõttu on inimõiguste kohus leidnud, et vajalikkuse kriteeriumi täitmiseks peavad olema kehtestatud piisavad ja efektiivsed kaitsemeetmed ja garantiid võimu kuritarvitamise vastu.[112]

Olukord, kus isikute sideandmeid massiliselt kogutakse ja salaja jälgitakse, tekitab võimu kuritarvitamiseks soodsad võimalused. Seda eriti juhul, kus inimesed ei ole teadlikud, et nende sidet, sealhulgas side metaandmeid, võidakse salaja jälgida. Seetõttu on vägagi põhjendatud Euroopa Inimõiguste Kohtu seisukoht, et isikutele, kelle sideandmeid kogutakse ja jälgitakse, peab olema seadus ligipääsetav, selle mõju ettenähtav ning tagatud piisavad ja efektiivsed kaitsemeetmed.

Piisavate ja tõhusate kaitsemeetmete ja garantiide olemasolu, et jälgimisrežiimid oleksid ettenähtavad ja vähendaksid võimu kuritarvitamise riski, hindas Euroopa Inimõiguste Kohus kuue kaitsemeetme kaudu.[113] Need minimaalsed kaitsemeetmed, mis peavad olema seaduses kehtestatud, on:

---

[110] *Ibid*, p-d 7-9, 15, 18.

[111] EIKo 4.12.2015, 47143/06, *Roman Zakharov vs. Venemaa*.

[112] *Ibid*, p-d 227, 228, 232; EIKo *Centrum för Rättvisa vs. Rootsi,* p-d 99-101, 104.

[113] EIKo *Centrum för Rättvisa vs. Rootsi,* p 113.

- pealtkuulamise korralduse andmise aluseks olevate õigusrikkumiste kirjeldus;
- nende isikukategooriate kirjeldus, kelle teabevahetust võib pealt kuulata;
- meetmete kasutamise kestuse piirang;
- kord, mida peab järgima saadud andmete uurimisel, kasutamisel ja säilitamisel;
- ettevaatusabinõud, mida tuleb järgida andmete edastamisel teistele osapooltele;
- asjaolud, mille korral salvestised võib või peab kustutama või hävitama.[114]

Lisaks neile asjaoludele hindas kohus ka loa andmist jälgimismeetmete kasutamiseks, jälgimismeetme rakendamise üle teostatavat järelevalvet, teavitamismehhanisme isikute teavitamiseks nende pealtkuulamise kohta ning siseriiklike õigusaktidega ette nähtud õiguskaitsevahendite olemasolu.[115] Eelnevast võib järeldada, et inimõiguste kohus peab nii side sisu kui ka metaandmeid inimõiguste konventsiooni artikli 8 kaitsealasse kuuluvaks, kuid eristab riivamise lubatavuse aluseid. Kui side sisu pealtkuulamiseks peavad kuritarvituste vältimiseks kehtima mitmed erinevad kaitsemeetmed, siis metaandmete puhul, nagu on näha eelpool käsitletud asjades *Figueiredo Teixeira vs. Andorra* ja *Ben Faiza vs. Prantsusmaa* tehtud lahenditest, on kohus hinnanud artikli 8 riivet palju pealiskaudsemalt.

Kohus jõudis otsuses *Centrum för Rättvisa* järeldusele, et kuigi mõnes valdkonnas esineb puudusi – sealhulgas andmete teistele riikidele ja rahvusvahelistele organisatsioonidele edastamise regulatsioonis, samuti puudub isikutel võimalus saada teada, kas nende sidet on pealt kuulatud ning individuaalsete kaebuste läbivaatamise järel ei esitata põhjendatud otsuseid – on üldiselt signaalluure puhul seadused kooskõlas eespool nimetatud printsiipidega ning proportsionaalsed eesmärgi saavutamiseks, mistõttu ei esine konventsiooni artikli 8 rikkumist.[116]

Puudusi, mille olemasolule Rootsi õiguses küll Euroopa Inimõiguste Kohus viitas, kuid millest hoolimata jõudis siiski järeldusele, et ei esine konventsiooni artikli 8 rikkumist, on kritiseeritud ka kirjanduses. Näiteks on välja toodud kohtu seisukoht, et andmete edastamine kolmandatele osapooltele ei kujuta endast isikutele võimalikku kahju, sest seaduse rakendamise üle on olemas tugev järelevalve. Samas on kohus jätnud tähelepanuta selle, et vastavat järelevalvet teostatakse riigisiseselt, kuid kuritarvitused kolmandate osapoolte poolt on endiselt võimalikud. Lisaks on

[114] *Ibid,* p 103.
[115] *Ibid,* p 114.
[116] *Ibid,* p-d 177, 180, 181.

väidetud, et kuna isikuid ei ole kunagi kordagi teavitatud sellest, et nende sidet on jälgitud, siis on reaalselt võimalus õiguskaitsevahendite kasutamiseks vaid neil isikutel, kes on sellisest massjälgimise praktikast teadlikud.[117]

2018. aasta septembris avaldas Euroopa Inimõiguste Kohus otsuse *Big Brother Watch jt vs. Ühendkuningriik*. Selles asjas esitati kaebused kohtule pärast seda, kui Edward Snowden oli lekitanud informatsiooni Ühendkuningriigi ja USA poolt kasutatavate elektrooniliste jälgimissüsteemide ja teabe jagamise kohta.[118]

Inimõiguste kohus leidis, et Ühendkuningriik on rikkunud riigipiiri ületavate sidealaste massandmete jälgimisega konventsiooni artiklit 8. Kohus tõi välja, et iseenesest ei ole sidealaste massandmete jälgimine konventsiooniga vastuolus, kuid see peab vastama teatud tingimustele.[119] Kohus viitas muuhulgas otsusele *Weber ja Saravia vs. Saksamaa*[120], kus selgitati, millised kaitsemeetmed peavad olema seaduses määratletud. Kuigi varasemas kohtupraktikas on neid põhimõtteid kasutatud edastatava teabe pealtkuulamise suhtes kriminaalmenetluses, siis on kohus kinnitanud, et samad põhimõtted kehtivad ka riigi julgeoleku eesmärgil teostatava jälgimise puhul.[121] Samadele kaitsemeetmetele viitas Euroopa Inimõiguste Kohus ka otsuses *Centrum för Rättvisa*, mida käsitleti ülalpool.[122]

Muuhulgas heitis Euroopa Inimõiguste Kohus seoses sidealaste massandmete jälgimisega Ühendkuningriigile ette, et side metaandmed olid jäetud täielikult kaitseta. Kohus leidis, et jättes side metaandmed täielikult välja side sisu suhtes kohaldatavatest kaitsemeetmetest, ei ole ametivõimud saavutanud õiglast tasakaalu avalike ja erahuvide vahel.[123] Kohus ei olnud veendunud, et elektroonilise side metaandmete omandamine on vähem riivav kui side sisu hõivamine. Elektroonilise side sisu ei pruugi paljastada midagi selle saatja või saaja kohta, kuid side metaandmed võivad näidata saatja ja saaja identiteeti, asukohta ning seadmeid, mille kaudu

---

[117] Strasbourg Observers. "Bulk interception of communications in Sweden meets Convention standards": the latest addition to mass surveillance case law by the European Court of Human Rights. 9.07.2018. Arvutivõrgus: https://strasbourgobservers.com/2018/07/09/bulk-interception-of-communications-in-sweden-meets-convention-standards-the-latest-addition-to-mass-surveillance-case-law-by-the-european-court-of-human-rights/ (20.03.2019).

[118] EIKo 13.09.2018, 58170/13, 62322/14, 24960/15. *Big Brother Watch jt vs. Ühendkuningriik*, p-d 7, 8.

[119] *Ibid*, p 303.

[120] EIKo 29.06.2006, 54934/00, *Weber ja Saravia vs. Saksamaa*.

[121] EIKo *Big Brother Watch jt vs. Ühendkuningriik*, p 307; EIKo *Roman Zakharov vs. Venemaa*, p 231.

[122] EIKo *Centrum för Rättvisa vs. Rootsi*, p 103.

[123] EIKo *Big Brother Watch jt vs. Ühendkuningriik*, p 357.

side edastati. Lisaks väljendas kohus sama seisukohta, milleni varem oli jõudnud ka Euroopa Kohus otsustes *Digital Rights Ireland* ja *Tele2 Sverige*.[124] Nimelt massilise andmete kogumisega kaasneb suurem riive, kuna ilmsiks tulevad mustrid võivad maalida isikust intiimse pildi läbi sotsiaalvõrgustike kaardistamise, asukoha ning internetilehekülgede sirvimise jälgimise, suhtlemisharjumuste kaardistamise ning näidates, kellega inimene on suhelnud.[125]

Seega, kuigi Euroopa Inimõiguste Kohus on aktsepteerinud teatud tingimustel üldist elektroonilise side massandmete kogumist, on siiski arvestatud sellega, et ka side metaandmete kogumisel ja kasutamisel peavad eksisteerima kaitsemeetmed. Veelgi enam, inimõiguste kohus on võtnud Euroopa Kohtuga sarnase positsiooni ning rõhutanud, et side metaandmed võivad paljastada inimeste kohta rohkemgi kui side sisu.

Lahendis *Big Brother Watch jt* analüüsis Euroopa Inimõiguste Kohus veel ka konventsiooni artikli 8 rikkumist seoses sideandmete nõudmisega elektroonilise side teenuse pakkujatelt. Esiteks viitas kohus oma otsusele asjas *Ben Faiza vs. Prantsusmaa*, kus samuti analüüsiti muuhulgas elektroonilise side metaandmete taotlemist mobiilsideoperaatoritelt. Seejärel viitas kohus Euroopa Kohtu praktikale asjades *Digital Rights Ireland* ja *Tele2 Sverige*, mille järgi juurdepääs sideandmetele peab olema piiratud eesmärgi saavutamiseks rangelt vajalikuga ning kui eesmärgiks on kuritegevuse vastu võitlemine, siis peaks see piirduma raskete kuritegude vastu võitlemisega. Samuti selgitati seal, et andmetele juurdepääs peaks alluma kohtu või sõltumatu haldusasutuse eelnevale kontrollile.[126]

Euroopa Inimõiguste Kohus oli seisukohal, et Euroopa Liidu õigus on Ühendkuningriigi õiguskorra osa. Juhul kui riigi õigus ja Euroopa Liidu õigus on omavahel vastuolus, siis on viimane riigi õiguse suhtes ülimuslik. Ühendkuningriigi kohus oli käsitletud sätete osas aga leidnud, et need ei ole kooskõlas Euroopa Liidu õigusega, sest juurdepääs säilitatud metaandmetele ei olnud piiratud eesmärgiga võitlusega raske kuritegevuse vastu ning juurdepääsuks andmetele ei olnud vaja kohtu ega sõltumatu haldusasutuse eelnevat luba. Seega tõlgendatuna Ühendkuningriigi kohtu poolt Euroopa Kohtu lahendite valguses, pidi riigi õigus nõudma, et juurdepääs sideandmetele oleks piiratud raske kuritegevuse vastu võitlemise eesmärgiga ning juurdepääsule pidi eelnema kontroll kohtu või sõltumatu haldusasutuse poolt.

[124] EKo *Digital Rights Ireland*, p 27; EKo *Tele2 Sverige*, p 99.
[125] EIKo *Big Brother Watch jt vs. Ühendkuningriik*, p 356.
[126] *Ibid*, p-d 461, 463.

Kuna Ühendkuningriigi kehtiv õigus selliseid tingimusi ei seadnud, siis ei olnud see ka kooskõlas konventsiooni artikliga 8. Seetõttu leidis inimõiguste kohus, et on toimunud rikkumine konventsiooni artikli 8 suhtes.[127]

Kohtuotsused asjades *Centrum för Rättvisa vs. Rootsi* ning *Big Brother Watch* ei ole siiski veel jõustunud. Kohtuasjade pooled on taotlenud asja üleandmist suurkojale.[128]

2.3. Liikmesriikide reageeringud Euroopa Kohtu lahenditele sideandmete säilitamise ja kasutamise kohta

2.3.1. Ühendkuningriigi eelotsusetaotlus Euroopa Kohtule

2017. aasta oktoobris on Ühendkuningriik esitanud Euroopa Kohtule eelotsusetaotluse sideandmete säilitamise ja kasutamise kohta. Eelotsusetaotluses soovitakse teada saada, kas e-privaatsuse direktiiv kohaldub liikmesriigi julgeoleku- ja luureagentuuridele sidealaste massandmete edastamisele arvestades seda, et Euroopa Liidu lepingu artikli 4 järgi austab Euroopa Liit riigi põhifunktsioone, sealhulgas riigi julgeoleku kaitsmist, nii et riigi julgeolek jääb iga liikmesriigi ainuvastutusse. Juhul kui liidu õigus on kohaldatav, soovis eelotsusetaotluse esitanud kohus teada, kas ja millisel määral tuleb kohaldada otsuses *Tele2 Sverige* sätestatud nõudeid sidealaste massandmete säilitamise ja kasutamise kohta riigi julgeolekutegevusele. Praeguseks veel antud asjas kohus otsust teinud ei ole.[129]

Eesti on esitanud selles asjas Euroopa Kohtule seisukoha. Esitatud seisukohas leidis Eesti, et liikmesriigi julgeoleku- ja luureagentuuridele sidealaste massandmete edastamisele ei kohaldu Euroopa Liidu õigus vastavalt Euroopa Liidu lepingu artiklitele 4 ja 5. Riigi julgeolek on iga liikmesriigi ainuvastutuses. Seejuures tuleb e-privaatsuse direktiivis sisalduvat kohaldamisala erandit seoses julgeoleku tagamisega tõlgendada aluslepingu artikleid arvesse võttes. Juhul kui Euroopa Kohus leiab, et liidu õigus on kohaldatav, on Eesti seisukohal, et lisaks inimõiguste

[127] *Ibid*, p-d 465-468.

[128] European Court of Human Rights. Hearings, Cases pending before the Grand Chamber. Arvutivõrgus: https://www.echr.coe.int/Pages/home.aspx?p=hearings/gcpending&c (3.04.2019).

[129] EK C-623/17, *Privacy International versus Secretary of State for Foreign and Commonwealth Affairs jt*, eelotsusetaotlus.

konventsiooniga kehtestatud nõuetele *Tele2 Sverige* lahendis toodud nõuded ei kohaldu, sest seal analüüsiti kitsalt raske kuritegevuse vastu võitlemise eesmärgil side massandmete säilitamise ja kasutamise regulatsiooni kooskõla põhiõiguste hartaga, mistõttu need nõuded saavad kohalduda vaid sel eesmärgil andmete edastamisele.[130]

Euroopa Liidu pädevus liikmesriikide julgeoleku küsimustes on piiratud. Juhul, kui Euroopa Kohus leiab liidu õiguse siiski kohaldatava olevat, ei saa täielikult nõustuda Eesti seisukohaga osas, mis puudutab *Tele2 Sverige* lahendis toodud nõuete mittekohaldamist. Sellisel juhul peab arvestama, et Euroopa Liidu Kohus on alati püüdnud vältida olukordi, kus liikmesriikidel on tulenevalt põhiõiguste hartast ja inimõiguste konventsioonist vastuolulised kohustused ning kohandanud oma otsuseid Euroopa Inimõiguste Kohtu kohtupraktikaga nii palju kui võimalik.[131] Euroopa Kohtu ja inimõiguste kohtu poolt esitatavad nõuded sideandmete säilitamisele ja kasutamisele on kohtupraktikas olnud küllaltki sarnased. Kuna inimõiguste kohus laiendas oma varasemas kohtupraktikas kriminaalmenetluses sideandmete jälgimise suhtes kohaldatud põhimõtteid ka riigi julgeoleku eesmärgil teostatavale jälgimisele[132], siis on võimalik, et Euroopa Kohus käitub sarnasel viisil ning kohaldab vähemalt teatud ulatuses *Tele2 Sverige* lahendis toodud nõudeid riigi julgeoleku tagamise eesmärgil sideandmete säilitamisele ning võtab arvesse ka inimõiguste kohtu seisukohti.

2.3.2. Reaktsioonid Belgias ning eelotsusetaotlus Euroopa Kohtule

Pärast lahendi tegemist asjas *Tele2 Sverige*, seisis Belgia konstitutsioonikohus vastamisi taotlustega tühistada andmete säilitamise regulatsioon, mis on taotluse kohaselt põhiseadusega vastuolus. Kaebajate arvates koheldakse side metaandmete säilitamise osas põhjendamatult ühtmoodi elektrooniliste telekommunikatsiooni- või sideteenuste kasutajaid, kellel on ametisaladuse hoidmise kohustus, ja teisi nende teenuste kasutajaid. Selline olukord on kahjustav muuhulgas nii advokaatidele, kellel on konfidentsiaalsuskohustus, kui ka

[130] Ülevaade Eesti osalemisest Euroopa Liidu Kohtu ja EFTA kohtu menetlustes, Eesti vastu algatatud rikkumismenetlustest ja projekti „EU Pilot“ päringutest aastal 2018. Välisministeerium, juriidiline osakond, Euroopa Liidu õiguse büroo, 2019. Lk 18.

[131] Reconsidering the blanket-data-retention-taboo, for human rights' sake? – European Law Blog. 1.10.2018. Arvutivõrgus: http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/ (20.03.2019).

[132] EIKo *Big Brother Watch jt vs. Ühendkuningriik*, p 307; EIKo *Roman Zakharov vs. Venemaa*, p 231.

õigussubjektidele. Näiteks on võimalik side metaandmete järgi kindlaks teha, kas isik, keda kahtlustatakse süüteo toimepanemises, on võtnud ühendust advokaadiga ning millal ta seda on teinud.[133]

Muuhulgas on kaebajad seisukohal, et säilitatud andmetele juurdepääsu ei ole piiratud vaid ametivõimudega, kes tegelevad raske kuritegevuse vastu võitlemisega. Sideandmetele juurdepääsu puhul olid täiendavad tagatised ametisaladuse asjus Belgia õigusega tagatud vaid advokaatidele, arstidele ja ajakirjanikele, kuigi ametisaladus hõlmab rohkemaid kui nende kolme kutseala esindajaid. Samuti ei sisaldanud Belgia seadused kaebajate arvates täpset kirjeldust andmetele juurdepääsu lubamise asjaolude ega tingimuste kohta.[134]

Kohtulahendis, mis tehti Belgia konstitutsioonikohtu poolt eelotsuse küsimiseks, jõudsid kohtunikud arvamusele, et nende, kes vaidlustasid Belgia sideandmete säilitamise seaduse põhiseaduspärasust, ning Belgia valitsuse, kes seadust põhjendatuks pidas, puhul oli tegemist erinevate lahendi *Tele2 Sverige* tõlgendustega. Seaduse tühistamist soovinute arvates ei olnud kahtlust, et üldine kõigi inimeste kõigi sideandmete säilitamine on ebaproportsionaalne ning Euroopa Kohus lubaks andmete säilitamist vaid teatud gruppide või geograafiliste piirkondade suhtes, mille puhul on selged viited, et andmete kogumiseks esineb alus – võitlus raske kuritegevuse või terrorismi vastu.[135]

Belgia valitsus seevastu oli seisukohal, et Euroopa Kohus oli välja toonud mitmeid puudusi, mis koos võetuna muutsid kogu süsteemi ebaproportsionaalseks, kuna esinesid privaatsuse ning andmete säilitamise õiguse rikkumised. Proportsionaalsuse põhimõtte kontrollimine eeldab terviklikku lähenemisviisi, mistõttu Belgia valitsuse arvates oli vale välja tuua üks puudus ja öelda, et see iseenesest muudab meetme ebaproportsionaalseks.[136]

Belgia seadusandja on pidanud võimatuks kehtestada diferentseeritud säilitamiskohustus. Selle asemel on otsustatud üldise säilitamiskohustuse kasuks ning ette nähtud ranged tagatised nii säilitamise kui ka juurdepääsu tasandil, et piirata eraelu puutumatusesse sekkumist. Belgia

[133] Eelotsusetaotluse kokkuvõte vastavalt Euroopa Kohtu kodukorra artikli 98 lõikele 1. Kohtuasi C-520/18, p-d 24, 26-28. Arvutivõrgus: https://eelnoud.valitsus.ee/main/mount/docList/0226101f-9cd8-46e9-b80c-7dcd6ae7ccf8 (22.03.2019).

[134] *Ibid*, p-d 50, 51, 53.

[135] Reconsidering the blanket-data-retention-taboo, (viide 131).

[136] Eelotsusetaotluse kokkuvõte vastavalt Euroopa Kohtu kodukorra, p-d 72, 73.

valitsus on rõhutanud, et andmete säilitamisel on võimatu ette näha eristamist isikute, ajaperioodide või piirkondade järgi.[137]

Belgia kohtu poolt esitatud esimeses küsimuses soovitaksegi teada, kas üldine andmete säilitamise kohustus, mille puhul on tagatud turvameetmed andmete säilitamiseks ja juurdepääsuks, on kooskõlas Euroopa Liidu õigusega, kui see ei ole mõeldud vaid võitluseks raske kuritegevusega, aga ka riigi julgeoleku, kaitse ja avaliku julgeoleku tagamiseks ning muude kuritegude ennetamiseks, uurimiseks, avastamiseks ja nende eest vastutusele võtmiseks.[138]

Seega soovib Belgia kohus sisuliselt välja selgitada, kas sideandmete üldine säilitamine on põhjendatud vaid võitlusega raske kuritegevuse vastu isegi siis, kui on tagatud andmete säilitamiseks ja neile juurdepääsuks turvameetmed. Arvestada tuleb aga seda, et otsuses *Tele2 Sverige* selgitas Euroopa Kohus, et niisugused riigisisesed õigusnormid, milles on ette nähtud üldiselt ja vahet tegemata kõigi elektroonilise side andmete säilitamine, on vastuolus e-privaatsuse direktiivi artikli 15 lg-ga 1 ning põhiõiguste harta artiklitega 7, 8, 11 ja 52 lg-ga 1.[139] Samas otsuses Euroopa Kohus küll rõhutas, et liikmesriigid peavad sätestama õigusnormid, mis võimaldavad andmeid kuritarvitamise ohu eest kaitsta – vastavate turvameetmete tagamisele viitas ka Belgia kohus eelotsusetaotluses – kuid esimeseks tingimuseks oli siiski see, et andmete säilitamine on piiratud vältimatult vajalikuga. Belgia kohus on aga viidanud üldisele andmete säilitamise kohustusele, mille puhul ei ole andmete säilitamine piiratud. Kuigi käesoleva töö kirjutamise ajaks ei ole Belgia eelotsusetaotluse osas avaldatud isegi veel kohtujuristi ettepanekut, on tulevikus kindlasti huvitav näha, eriti arvestades Eestis plaanitavat sarnast lähenemist andmete säilitamisele ja juurdepääsetavusele, kas Euroopa Kohus taganeb otsuses *Tele2 Sverige* esitatud seisukohast või jääb endiselt selle juurde.

Belgia eelotsusetaotluse kohta on Eesti esitanud ka oma seisukohad Euroopa Kohtule. Seejuures on Eesti pidanud vajalikuks vastata kahele esimesele eelotsusetaotluses esitatud küsimusele. Esimesele küsimusele vastates on leitud, et kuritegevuse vastane tõhus võitlus, riigikaitse ja julgeoleku tagamine on võimalik vaid siis, kui kohustuse puhul sideandmeid

[137] *Ibid*, p 81.

[138] EK C-520/18, *Ordre des barreaux francophones et germanophone jt versus Conseil des ministres*, eelotsusetaotlus, p 1.

[139] EKo *Tele2 Sverige*, p-d 99-105, 107.

säilitada ei eristata andmesubjekte, sidevahendeid ega säilitatavaid andmekategooriaid, sest eesmärgi saavutamise tagab üksnes üldine säilitamiskohustus. Eesti hinnangul tooks sideandmete säilitamisel säilitatavate andmete mahu või puudutatud seadmete ringi piiritlemine kaasa kriminaalmenetluse edukuse vähenemise ja mõjutaks negatiivselt ühiskonna turvatunnet. Lisaks on Eesti viidanud sarnaselt väljatöötamiskavatsuses esitatud põhjendustele, et säilitamiskohustust geograafiliselt või teatud seadmetega piirates tooks see kaasa kuritegevuse liikumise teise piirkonda või seadmete ja tehnoloogiate kasutuselevõtu, millele säilitamiskohustus ei laiene. Isikuline piiramine tooks paratamatult kaasa diskrimineerimise. Seega on Belgia esimesele küsimusele vastates leitud, et Euroopa Liidu õigus lubab kehtestada üldise kohustuse sideandmete säilitamiseks, kui riigisiseses õiguses on kehtestatud kindlad juurdepääsureeglid ning erinevad õiguskaitsevahendid.[140]

Teiseks on Belgia kohus küsinud, kas e-privaatsuse direktiivi artikli 15 lg-ga 1 ja põhiõiguste hartaga on vastuolus riigisisesed õigusnormid, millega on ette nähtud üldine kohustus säilitada liiklus- ja asukohaandmeid, kui nende õigusnormide eesmärgiks on riigi positiivsete kohustuste täitmine, mis tulenevad harta artiklitest 4 ja 8[141], milleks on kehtestada õiguslik raamistik, mis võimaldab tõhusat kriminaaluurimist, laste seksuaalse kuritarvitamise karistamist ning kuriteo toimepanija tuvastamist isegi kui viimased on kasutanud elektroonilisi sidevahendeid.[142]

Kõige huvitavamaks aspektiks Belgia diskussiooni puhul peetaksegi inimõiguste kasutamist argumendina sideandmete säilitamise poolt. Euroopa Inimõiguste Kohtu väljakujunenud kohtupraktikast ilmneb, et andmete säilitamine ja õiguskaitseasutuste juurdepääs neile andmetele võib olla vajalik selleks, et tagada liikmesriikide poolt teatavate põhiõiguste tõhus kaitse, eriti kuriteoohvrite puhul.[143]

Vastates Belgia eelotsusetaotluse teisele küsimusele on Eesti oma seisukohas leidnud, et kuriteod, sealhulgas need, mis on toime pandud sidevahendi vahendusel, riivavad oluliselt isikute põhiõigusi. Riigi kohustus on tagada elanike turvalisus ja nende põhiõiguste kaitse, et isikute põhiõigusi riivavad tegevused, sealhulgas laste seksuaalne ärakasutamine ning

[140] Eesti seisukohad Euroopa Kohtule liidetud eelotsusetaotluste C-511/18 ja C-512/18 (French Data Network) ja eelotsusetaotluse C-520/18 (Ordre des barreaux francophones et germanophone) kohta. Eelnõu toimik nr 18-1233. Arvutivõrgus: https://eelnoud.valitsus.ee/main/mount/docList/0226101f-9cd8-46e9-b80c-7dcd6ae7ccf8 (22.03.2019).

[141] Põhiõiguste harta artikkel 4 sätestab piinamise ning ebainimlikult või alandavalt kohtlemise ja karistamise keelu ning artikkel 8 isikuandmete kaitse.

[142] EK *Ordre des barreaux francophones et germanophone jt*, p 2.

[143] Reconsidering the blanket-data-retention-taboo, (viide 131).

lapsporno käitlemisega seotud kuriteod, oleks tõhusalt menetletud ning toimepanijad kindlaks tehtud. Sidevahendi vahendusel toime pandud kuritegude korral ei oleks nende menetlemine paljudel juhtudel üldse võimalik, kui sideandmeid ei säilitataks.

Eesti on viidanud sellele, et ilma juurdepääsuta sideandmetele jääks väga suur osa laste vastu suunatud kuritegudest avastamata ja lahendamata, eriti laste seksuaalse ärakasutamise juhtumites, kus kurjategija otsib ohvreid ja paneb kuriteod toime küberruumis. See aga oleks muuhulgas vastuolus liikmesriikidele Euroopa Liidu õigusest tulenevate kohustustega, kuna Euroopa Parlamendi ja nõukogu direktiivi 2011/92/EL, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lapsporno vastast võitlust ja mis asendab nõukogu raamotsuse 2004/68/JSK[144], artikli 15 lg 3 järgi peavad direktiivis viidatud süütegude uurimiseks ja süüdistuse esitamiseks olema pädevatele asutustele kättesaadavad tõhusad uurimismeetodid. Sama artikli lõige 4 kohustab liikmesriike kasutama lapsohvrite tuvastamiseks andmeid, sealhulgas neid, mis on teatavaks tehtud info- ja kommunikatsioonitehnoloogia abil. Kokkuvõttes leidis Eesti, et riigil lasuvad kohustused annavad aluse sätestada riigisiseses õiguses sideteenuse pakkujate kohustuse säilitada sideandmeid.[145]

Ka raportis Euroopa Parlamendi ja nõukogu 13. detsembri 2011. aasta direktiivi 2011/93/EL, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust, rakendamise kohta on Euroopa Parlament rõhutanud, et üheks peamiseks õiguskaitse- ja kohtuasutuste ees seisvaks probleemiks laste internetis toime pandud seksuaalse kuritarvitamise süütegude uurimisel ja nende eest süüdistuse esitamisel tuleneb paljude uurimiste sõltuvusest elektroonilistest tõenditest.[146] Olukorras, kus riigil ei ole lubatud kõiki elektroonilise side andmeid säilitada ja kriminaaluurimise eesmärgil kasutada, võib kindlasti olla kahjustatud ka laste seksuaalse kuritarvitamise süütegude uurimine, toimepanijate tuvastamine ja nende karistamine. Seda eelkõige seetõttu, et selliste kuritegude toimepanemine võib õiguskaitseasutustele teatavaks saada alles peale nende toimepanemist, mistõttu andmete piiratud säilitamisel ei pruugi vajalikke andmeid olla säilitatud. See võib omakorda raskendada

[144] Euroopa Parlamendi ja nõukogu direktiiv 2011/92/EL, 13. detsember 2011, mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust ja mis asendab nõukogu raamotsuse 2004/68/JSK. – ELT L 335, 17.12.2011.

[145] Eesti seisukohad Euroopa Kohtule, lk 10, 11.

[146] Raport Euroopa Parlamendi ja nõukogu 13. detsembri 2011. aasta direktiivi 2011/93/EL (mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust) rakendamise kohta. Menetlus (2015/2129(INI)). Euroopa Parlamendi resolutsiooni ettepanek, p 20.

või koguni välistada süütegude toimepanijate kindlaks tegemist ja nende vastutusele võtmist. Seetõttu tuleks pooldada Eesti seisukohta, et liikmesriikidel peaks olema õigus kehtestada reeglid kohustamaks teenusepakkujaid kõiki sideandmeid säilitama.

Kolmandaks soovib Belgia konstitutsioonikohus teada, et juhul, kui Belgia seadus eirab ühte või mitut eelmistes küsimustes nimetatud Euroopa Liidu õigusnormidest tulenevat kohustust, siis kas võib seadusest andmete kogumise ja säilitamise kohta tulenevad õiguslikud tagajärjed ajutiselt jõusse jätta, et vältida õiguslikku ebakindlust ning võimaldada varem säilitatud andmete kasutamist seaduses ette nähtud eesmärkidel.[147] On leitud, et sellele küsimusele antav vastus avaldab suurt praktilist mõju, kui Euroopa Kohus peaks sõnaselgelt uuesti kinnitama seda, et sideandmete üldine säilitamine on keelatud – vastus sellele küsimusele näitaks, kas tõendeid võib kasutada nende ebaseaduslikust kogumisest hoolimata.[148] Euroopa Inimõiguste Kohus on liikmesriikidele andnud inimõiguste konventsiooni artiklit 8 rikkudes kogutud teabe tõendina kasutamiseks piisava vabaduse, kuid Euroopa Kohus on kasutanud tõhususe argumenti, et välistada põhiõigusi rikkuvate tõendite kasutamine.[149] Näiteks on Euroopa Kohus asjas *WebMindLicenses*[150] jõudnud järeldusele, et tõendid, mis on saadud põhiõigusi rikkudes, tuleb siseriiklikul kohtul jätta arvestamata, samuti tuleb tõendid jätta arvesse võtmata, kui siseriiklik kohus ei ole pädev kontrollima, kas tõendid on kriminaalmenetluse käigus kogutud kooskõlas liidu õigusega või ei saa kohtu poolt võistlevas menetluses läbi viidud kontrolli põhjal öelda, et tõendid on saadud kooskõlas selle õigusega.

2.3.3. Prantsusmaa eelotsusetaotlus Euroopa Kohtule

Conseil d'État[151] on Euroopa Kohtule eelotsusetaotlused esitanud 2018. aasta augustis.[152] Neis eelotsusetaotlustes on kaebajad vaidlustanud nende hinnangul Euroopa Liidu põhiõiguste harta ja Euroopa Liidu kohtupraktikaga vastuolus olevad Prantsusmaa seadused, mis kohustavad

[147] EK *Ordre des barreaux francophones et germanophone jt*, p 3.

[148] Reconsidering the blanket-data-retention-taboo, (viide 131).

[149] *Ibid*.

[150] EKo 17.12.2015, C-419/14, *WebMindLicenses*, p-d 87-91.

[151] Conseil d'État on Prantsusmaa kõrgeim halduskohus. (The Conceil d'État. Arvutivõrgus: http://english.conseil-etat.fr/ (18.04.2019).)

[152] EK C-511/18, *La Quadrature du Net jt*, eelotsusetaotlus; EK C-512/18, *French Data Network jt*, eelotsusetaotlus.

sideteenuse pakkujaid piiratud aja jooksul sideandmeid säilitama ja mis annavad julgeolekuasutustele võimaluse saada neile andmetele juurdepääs.[153]

Esimeses küsimuses soovib Conseil d'État teada, kas sideteenuste pakkujatele e-privaatsuse direktiivi artikli 15 lg 1 alusel pandud üldist andmete säilitamise kohustust tuleks tõsiste ja pidevate ohtude korral riigi julgeolekule, mis seisnevad eelkõige terrorismiohus, käsitada riivena, mis on põhjendatud Euroopa Liidu põhiõiguste harta artikliga 6 tagatud õigusega turvalisusele ja riigi julgeoleku kaitsmise vajadusega, mille eest vastutavad Euroopa Liidu lepingu[154] artikli 4 kohaselt ainult liikmesriigid.[155] Eesti on vastuses sellele küsimusele leidnud, et riikliku julgeoleku tagamine on liikmesriikide endi pädevuses, sest liikmesriigid ei ole riigi põhifunktsioone seoses riigi julgeolekuga liidule üle andnud. Seetõttu ei saa riigi julgeoleku tagamist reguleerida Euroopa Liidu õigus ega e-privaatsuse direktiiv. Kuna riigi julgeoleku tagamine on liikmesriikide ainuvastutuses, siis saavad liikmesriigid otsustada, kas panna sideteenuste pakkujatele andmete säilitamise kohustus riigi julgeoleku tagamise eesmärgil või mitte.[156]

Juhul, kui Euroopa Kohus otsustab, et riigi julgeoleku tagamine ning seda reguleerivad normid kuuluvad liidu õiguse kohaldamisalasse, on Eesti seisukohal, et sideettevõtjate kohustamine kõigi sideandmete üldiseks säilitamiseks ei ole vastuolus e-privaatsuse direktiiviga, kuna direktiiv lubab kehtestada sellise kohustuse muu hulgas riigi julgeoleku tagamise eesmärgil. Eesti hinnangul on selline kohustus vajalik, otstarbekas ja proportsionaalne, kuna aitab kaasa riigi julgeolekupoliitiliste otsuste tegemiseks informatsiooni kogumisele ning võimaldab anda hoiatusi võimalike riigivastaste, sõjaliste ja terrorirünnakute kohta.[157]

Teiseks on Prantsusmaa kohus küsinud, kas e-privaatsuse direktiivi tuleb tõlgendada nii, et see lubab meetmeid nagu kindlaksmääratud isikute kohta liiklus- ja asukohaandmete kogumist reaalajas, mis puudutavad elektrooniliste sideteenuste osutajate õigusi ja kohustusi, kuid millega ei kohustata neid oma andmete säilitamiseks.[158] Sisuliselt soovitakse teada, kas e-

[153] Ärakirjad eelotsusetaotlustest eesti keeles on kättesaadavad eelnõude infosüsteemist, vt viide 133.

[154] Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid. – ELT 2016/C 202/01, 7.06.2016.

[155] EK *La Quadrature du Net jt*, p 1.

[156] Eesti seisukohad Euroopa Kohtule, lk 5, 6.

[157] *Ibid*, lk 6.

[158] EK *La Quadrature du Net jt*, p 2.

privaatsuse direktiivi ja põhiõiguste hartaga on kooskõlas reaalajas side metaandmete kogumine kindlaksmääratud isikute kohta.

Eesti on oma seisukohas sellele küsimusele leidnud, et sellise meetme puhul tuleb hinnata, kas see on kooskõlas Euroopa Liidu õigusega, kui see on kehtestatud riigi julgeoleku tagamiseks ja Euroopa Kohus leiab, et riigi julgeoleku tagamine kuulub liidu õiguse kohaldamisalasse või kui meedet kasutatakse seoses avaliku korra, kriminaalkuritegude ennetamise, uurimise, avastamise või menetlemisega. Eesti hinnangul on e-privaatsuse direktiiviga kooskõlas riigisisesed õigusnormid, mille alusel on võimalik koguda konkreetsete isikute kohta teavet reaalajas. Reaalajas liiklus- ja asukohaandmete kogumine on menetlustoiming, mida kasutatakse muuhulgas kriminaalmenetluses ja mis riivab tugevalt põhiõigusi. See võib olla aga proportsionaalne ja vajalik meede, kui seda reguleerivad õigusaktid tagavad põhiõiguste kaitse isikute suhtes, keda jälgitakse, ning kui täiendavalt hindab tõendite kogumise õiguspärasust kohus.[159]

Kuigi lahendis *Tele2 Sverige* analüüsis kohus sideandmete säilitamist, mitte isikute reaalajas jälgimist, jõuti seal järeldusele, et andmete säilitamine peaks olema piiratud andmete liigi, asjassepuutuvate sidevahendite ja isikute ning säilitamise kestuse osas. Eelotsuseküsimusest lähtuvalt oleks meede piiratud asjassepuutuvate isikute ja sellest tulenevalt ka sidevahenditega. Kuna eelotsusetaotlus puudutab just konkreetsete isikute osas reaalajas andmete kogumist, siis võiks arvata, et Euroopa Kohus võiks e-privaatsuse direktiivist ja põhiõiguste hartast ja senisest kohtupraktikast lähtuvalt sellist meedet mitte keelata. Siiski, nagu tõi oma seisukohas välja ka Eesti, peaks põhiõiguste tagamiseks olema selline tegevus riigisiseselt reguleeritud. Kindlasti peaks liiklus- ja asukohaandmete reaalajas kogumiseks konkreetsete isikute suhtes andma loa sõltumatu ametiasutus, sellise loa kehtivus peaks olema ajaliselt piiratud ning selliste andmete kogumine peaks ka tagantjärele alluma kohtu kontrollile. Sel viisil oleks tagatud, et isikute, kelle kohta liiklus-ja asukohaandmeid reaalajas kogutakse, põhiõiguste riive oleks proportsionaalne.

Kolmanda küsimusega soovitakse teada, kas e-privaatsuse direktiivi tuleb põhiõiguste hartat arvestades tõlgendada nii, et sideandmete kogumise menetluse õiguspärasuse eelduseks on see, et asjasse puutuvat isikut informeeritakse, kui see ei kahjusta enam pädevate ametiasutuste poolt läbi viidavat uurimist, või saab selliseid menetlusi käsitada õiguspärastena, võttes arvesse

[159] Eesti seisukohad Euroopa Kohtule, lk 6, 7.

teisi olemasolevaid menetluslikke tagatisi, mis tagavad õiguskaitsevahendite kasutamise võimaluse.[160]

Seisukohas sellele küsimusele on Eesti leidnud, et isikute teavitamine on üks võimalik tagatis, mis annab võimaluse kasutada meetmeid põhiõiguste kaitseks. Selle puhul tuleb arvestada teavitamise mõjuga isikute põhiõigustele, kuna teavitamine võib kaasa tuua täiendava privaatsuspõhiõiguse riive. Selline olukord võib tekkida näiteks juhul, kui on vajalik koguda andmesubjektide kohta lisainformatsiooni teavitamiskohustuse täitmiseks. Eesti arvamuse kohaselt on võimalik rakendada ka teisi õiguskaitsevahendeid peale teavitamise, mis aitaksid tagada andmesubjekti õigusi, näiteks töötlemise piiramine või kustutamine. Õiguskaitsevahendid, mida erinevates olukordades kasutatakse, tuleks seaduses sätestada.[161]

Ka Euroopa Inimõiguste Kohus on asjas *Centrum för Rättvisa* nentinud, et alati ei ole praktikas võimalik nõuda isikute hilisemat teavitamist. Kohus võttis seejuures arvesse, et eksisteerivad teised õiguskaitsevahendid, mille abil on võimalik kontrollida teabevahetuse pealtkuulamise õiguspärasust.[162] Seega on vähemalt Euroopa Inimõiguste Kohus seisukohal, et arvesse tuleb võtta ka teisi menetluslikke tagatisi peale isikute informeerimise. Töö autor pooldab nii inimõiguste kohtu kui ka Eesti väljendatud seisukohta, kuna alati ei ole mõistlik muutmaks sideandmete kogumise menetlust õiguspäraseks, inimesi nende kohta kogutud andmetest teavitada. Kuna sageli ei töödelda kogutud andmeid üldse, siis eeldaks isikute teavitamine vastavate isikute kindlakstegemist, mis riivaks nende põhiõigusi veelgi. Isikute põhiõiguste tagamist on võimalik kindlustada näiteks seeläbi, et seaduses nähakse ette juhtumid, mil on lubatud andmeid töödelda, kohtu või sõltumatu asutuse eelnev luba andmetele juurdepääsuks, tõhus kontroll asutuste üle, kes sideandmeid säilitavad ja kasutavad ning andmete säilitamise ja kustutamise tingimused.

Siiski tuleb tõdeda, et eelnimetatud vahendid ei taga isikutele õigust tõhusatele õiguskaitsevahenditele. Neil viisidel on võimalik vähendada põhiõiguste riivete ulatust, kuid ilma isikuid teavitamata on keeruline kui mitte võimatu tagada, et isikud saavad kasutada oma õiguste kaitseks tõhusaid vahendeid.

[160] EK *La Quadrature du Net jt*, p 3.
[161] Eesti seisukohad Euroopa Kohtule, lk 8, 9.
[162] EIKo *Centrum för Rättvisa*, p-d 164, 178.

Kohtuasjas C-512/18 esitatud esimene küsimus kattub asjas C-511/18 esitatud esimese küsimusega. Teise küsimusega soovib aga eelotsusetaotluse esitanud Prantsusmaa kohus teada, kas elektroonilise kaubanduse direktiivi[163] sätteid tuleks Euroopa Liidu põhiõiguste harta artikleid 6, 7, 8 ja 11 ning artikli 52 lg 1 arvestades tõlgendada viisil, et need lubavad kehtestada riigisisesed normid, millega pannakse isikutele, kes pakuvad juurdepääsu interneti teel üldsusele andmete edastamise teenustele, ning füüsilistele ja juriidilistele isikutele, kes tagavad interneti teel üldsusele andmete edastamise teenuste kaudu üldsusele edastamise eesmärgil nende teenuste kasutajate poolt edastatud signaalide, tekstide, piltide, helide või mis tahes liiki sõnumite salvestamise, kohustus säilitada andmeid, mis võimaldavad tuvastada kõik nende poolt osutatavate teenuste sisu või selle osa loomises osalenud isikud, et kohus saaks vajadusel nõuda andmete esitamist tsiviil- või karistusõiguslikku vastutust reguleerivate õigusnormide kohaldamiseks.[164]

Kokkuvõttes soovib kohus teada, kas isikuid, kes pakuvad interneti teel üldsusele andmete edastamise teenust ning edastatud andmete salvestamist, saab kohustada andmeid säilitama, et tuvastada nende teenuste kasutajad muuhulgas karistusõiguslikku vastutust reguleerivate sätete kohaldamiseks. Eesti selle küsimuse kohta oma seisukohta esitanud ei ole, kuna Eestis vastav regulatsioon puudub.[165] Elektroonilise kaubanduse direktiivis ei ole sätestatud andmete säilitamise keeldu. Samas ei kuuluks selliste andmete säilitamine ka e-privaatsuse direktiivi kohaldamisalasse, kuna seda kohaldatakse artikli 3 lg 1 kohaselt vaid seoses üldkasutatavate elektrooniliste sideteenuste osutamisega üldkasutatavates sidevõrkudes. Elektroonilise kaubanduse direktiivi artikli 15 lg 2 kohaselt võivad küll liikmesriigid kehtestada teenuse osutajatele kohustuse edastada pädevatele asutustele nende taotluse põhjal teavet, mis võimaldab identifitseerida teenuse saajaid, kellega teenuseosutajal on talletamise kohta lepingud. Sellist võimalust ei nähta aga selgesõnaliselt ette juhuks, mil teenus seisneb vaid teabe edastamises.

Töö autori arvates võiks ka selliste teenuste puhul olla liikmesriikidel võimalus sätestada õigusnormid, mis kohustavad isikute tuvastamiseks vajalikke andmeid säilitama ja annavad võimaluse neid andmeid kriminaalmenetluse läbiviimise tarbeks kasutada. Siiski peaksid

[163] Euroopa Parlamendi ja nõukogu direktiiv 2000/31/EÜ, 8. juuni 2000, infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta). – ELT L 178, 17.07.2000.

[164] EK *French Data Network*, p-d 1, 2.

[165] Eesti seisukohad Euroopa Kohtule, lk 5.

eksisteerima sarnased tagatised, näiteks andmetele juurdepääsuks prokuratuuri poolt loa andmine, nagu muude elektrooniliste sideandmete säilitamise ja kasutamise puhulgi, et oleks tagatud isikute põhiõiguste kaitse.

2.3.4. Eesti eelotsusetaotlus Euroopa Kohtule

Hiljuti on ka Riigikohus esitanud Euroopa Kohtule eelotsusetaotluse seoses ESS § 111[1] vastavusega Euroopa Liidu õigusele.[166] Selles kriminaalasjas leidis ringkonnakohtu otsuse peale kassatsiooni esitanud kaitsja, et sideettevõtjalt saadud andmeid kajastavad protokollid ei ole lubatavad tõendid ning nende alusel süüdistatava süüditunnistamine on põhjendamatu, kuna õigusnormid, mis kohustavad sideettevõtjaid säilitama sideandmeid, on vastuolus direktiivi 2002/58/EÜ artikli 15 lg-ga 1.[167]

Riigikohtu kolleegium arvestas oma seisukohas sellega, et Euroopa Liidu õigus on ülimuslik, mistõttu tuleb riigisisest õigust tõlgendada kooskõlas Euroopa Liidu õigusega.[168] Eelotsusetaotluses esitatud esimese küsimusega soovib Riigikohus välja selgitada, kas direktiivi 2002/58/EÜ tuleb tõlgendada nii, et riigiasutuste juurdepääs andmetele, mis võimaldavad kindlaks teha kahtlustatava telefoni ja mobiiltelefoni side lähte- ja sihtkoha, kuupäeva, kellaaja ja kestuse, sideteenuse liigi, kasutatud seadme ja mobiilsideseadme kasutamise asukoha, kujutab endast harta viidatud artiklitega tagatud põhiõiguste riivet, mis on alati nii raske, et sellist juurdepääsu tuleks piirata võitlusega raske kuritegevuse vastu, sõltumata sellest, millise ajavahemiku kohta säilitatud andmetele on riigiasutustel juurdepääs. Kolleegium viitas nimelt sellele, et kui andmeid nõutakse lühikese ajavahemiku kohta, siis ei ole nende andmete põhjal võimalik teha ulatuslikke järeldusi isiku eraelu kohta, mistõttu ei saa sellisel juhul olla sideandmete nõudmine õigustatav üksnes võitlusega raske kuritegevuse vastu.[169]

Tuleb nõustuda, et mida pikema ajavahemiku kohta sideandmeid soovitakse, seda täpsemaid järeldusi saab teha isikute eraelu kohta ning seda suurem on ka põhiõiguste riive. Otsuses *Tele2 Sverige* on kohus rõhutanud, et liikmesriigid võivad lubada raske kuritegevuse vastu võitlemise

[166] RKKKm 12.11.2018, 1-16-6179.
[167] *Ibid*, p-d 8, 9.
[168] *Ibid*, p 18.
[169] *Ibid*, p 23.

eesmärgil elektroonilise side metaandmete eesmärgipärast ennetavat säilitamist. Andmetele juurdepääsu kohta nenditi samas lahendis, et kuritegevuse vastu võitlemise eesmärgil võib anda juurdepääsu ainult nende isikute andmetele, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või sellise kuriteoga seotud olemises.[170] Seega kui andmeid võib eesmärgipäraselt ennetavalt säilitada vaid raske kuritegevuse vastu võitlemise eesmärgil, siis peaks ka neile juurdepääs olema piiratud võitlusega raske kuritegevuse vastu olenemata sellest, kui pika ajavahemiku kohta andmeid nõutakse.

Teise eelotsusetaotluses esitatud küsimuse abil soovitakse täpsustada, kas Euroopa Kohtu otsuses *Ministerio Fiscal* väljendatud proportsionaalsuse põhimõte tähendab seda, et kui esimeses küsimuses viidatud andmete hulk, millele riigiasutusel on juurdepääs, ei ole suur, siis on sellega kaasnev põhiõiguste riive õigustatav üldiselt kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga ning mida raskem on kuritegu, seda intensiivsem põhiõiguste riive on lubatud.[171]

Lahendis *Ministerio Fiscal*, milles Euroopa Kohus analüüsis side metaandmetele juurdepääsu proportsionaalsust, toodi välja, et rasket põhiõiguste riivet saab põhjendada „üksnes võitlusega sellise kuritegevuse vastu, mida tuleb samuti pidada „raskeks““[172]. Seega võiks tõepoolest leida, et mida raskem on kuritegu, seda intensiivsem riive on lubatud. Arvesse võttes aga *Tele2 Sverige* otsust, kus kohus leidis, et kuritegevuse vastu võitlemise eesmärgil võib anda juurdepääsu ainult nende isikute andmetele, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või eelnevas toimepanemises või kuriteoga seotud olemises,[173] siis on tulevikus huvitav näha, kuidas vastab Euroopa Kohus sellele eelotsusetaotluse küsimusele.

Kolmanda küsimusega soovitakse selgitada välja, mida tähendab kohtuasjas *Tele2 Sverige* toodud nõue, et riigi pädevate asutuste juurdepääs säilitatud sideandmetele peab olema allutatud kohtu või sõltumatu haldusasutuse eelnevale kontrollile. Eesti kohus soovib teada, kas sõltumatu haldusasutusena on käsitletav ka prokuratuur, kes on seadusega kohustatud juhtima kohtueelset menetlust sõltumatult, kuid kes hiljem esindab kohtumenetluses riiklikku süüdistust olles ise kohtumenetluse pool.[174]

[170] EKo *Tele2 Sverige* p-d 108, 119
[171] *Ibid*, p 24.
[172] EKo *Ministerio Fiscal*, p 56.
[173] EKo *Tele2 Sverige*, p 119.
[174] RKKKm, p-d 26-28.

KrMS § 30 lõigetest 1 ja 2 tulenevalt peab prokurör kriminaalmenetluses teostama prokuratuuri volitusi sõltumatult, kuid peab kohtueelset menetlust juhtides tagama selle seaduslikkuse ja tulemuslikkuse ning esindama riiklikku süüdistust kohtus. Samuti tuleneb KrMS § 211 lg-st 2, et prokuratuur ja uurimisasutus selgitavad kohtueelses menetluses kahtlustatavat ja süüdistatavat süüstavad kui ka õigustavad asjaolud. Arvestades neid prokuratuurile pandud kohustusi võiks eeldada, et prokuratuur on käsitletav sõltumatu haldusasutusena. Lisaks tuleks arvestada sedagi, et kohtumenetluses, kus prokuratuur esindab riiklikku süüdistust, on KrMS § 90^1 lg 2 kohaselt õigus teha sideettevõtjale päring kohtu loal, mitte enam prokuratuuri loal. Euroopa Inimõiguste Kohus on samuti pidanud üheks andmetele juurdepääsu kuritarvitamise vastaseks tagatiseks sideettevõtjale päringu esitamiseks vajalikku prokuratuuri eelnevat luba.[175]

Liikmesriikide poolt esitatud eelotsusetaotlustest jääb kokkuvõttes mulje, et riigid soovivad endiselt säilitada valimatult kõiki elektroonilise side liiklus- ja asukohaandmeid. Otsides erinevaid tõlgendusvariante ning argumente soovitakse leida võimalus edaspidigi säilitada üldiselt kõiki metaandmeid. Samuti soovitakse säilitatud andmeid esitatud küsimuste põhjal kasutada nii riigi julgeoleku tagamise kui ka kuritegude ennetamise, uurimise ja avastamise eesmärgil.

2.4. Elektroonilise side andmete kasutamine kriminaalmenetluses

Eesti õiguses reguleerib ESS § 111^1 lg 11, missugustele pädevatele asutustele tuleb sama paragrahvi lõigete 2 ja 3 alusel säilitatavad andmed edastada. Näiteks tuleb ESS § 111^1 lg 11 punkti 2 alusel julgeolekuasutusele[176] ning punkti 6 järgi jälitusasutusele[177] kaitseväe korralduse seaduses[178], maksukorralduse seaduses[179], politsei ja piirivalve seaduses[180],

[175] EIKo *Ben Faiza vs. Prantsusmaa*, p 73.

[176] Julgeolekuasutuste seaduse § 5 alusel on julgeolekuasutused Kaitsepolitseiamet ja Välisluureamet. (Julgeolekuasutuste seadus. – RT I, 05.05.2017, 2.)

[177] Jälitusasutus on kriminaalmenetluse seadustiku § 126^2 lg 1 kohaselt Politsei- ja Piirivalveamet, Kaitsepolitseiamet, Maksu- ja Tolliamet, Sõjaväepolitsei ning Justiitsministeeriumi vanglate osakond ja vangla.

[178] Kaitseväe korralduse seadus. – RT I, 29.05.2018, 2.

[179] Maksukorralduse seadus. – RT I, 07.12.2018, 5.

[180] Politsei ja piirivalve seadus. – RT I, 05.02.2019, 3.

relvaseaduses[181], strateegilise kauba seaduses[182], tolliseaduses[183], tunnistajakaitse seaduses[184], turvaseaduses[185], vangistusseaduses[186] ja välismaalaste seaduses[187] sätestatud juhtudel. Muuhulgas tuleb ESS § 111[1] lg 11 punkti 1 järgi esitada säilitatavad andmed KrMS-i kohaselt uurimisasutusele, jälitusasutusele, prokuratuurile ja kohtule. See võimaldabki elektroonilise side andmete kasutamist kriminaalmenetluses.

Kui varasemalt kuulus ESS § 111[1] lg 2 ja 3 andmete päring KrMS-i kohaselt jälitustoimingute hulka, siis alates 1. jaanuarist 2013. aastast on tegemist tavalise menetlustoiminguga, mis on sätestatud KrMS §-s 90[1]. Eelnõu seletuskirja kohaselt arutati seda küsimust jälitustegevuse õigusliku regulatsiooni analüüsimiseks kokku kutsutud töörühmas, kus leiti, et elektroonilise side andmete päringud võib jälitustoimingute hulgast välja arvata.[188]

KrMS § 90[1] lg-s 1 on sätestatud omanikupäring, mille alusel võib menetleja teha päringu elektroonilise side ettevõtjale, et teha kindlaks elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja kindlaks tegemiseks vajalikud andmed. Identifitseerimistunnusteks võivad olla IMEI[189], IMSI[190], SIM[191], IP-aadress, kasutajatunnus ja teised lõppkasutaja tuvastamist võimaldavad identifitseerimistunnused.[192] KrMS § 90[1] lg 2 alusel on aga uurimisasutusel kohtueelses menetluses prokuratuuri loal või kohtumenetluses kohtu loal võimalus teha päring elektroonilise side ettevõtjale ESS § 111[1] lõigetes 2 ja 3 loetletud andmete kohta, mida ei ole nimetatud lõikes 1. Muuhulgas tuleb päringu tegemise loas märkida kuupäeva täpsusega ajavahemik, mille kohta andmeid võib nõuda. Seega on muu kui omanikupäringu tegemiseks kohtueelses kriminaalmenetluses vajalik prokuratuuri luba. Ka elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu

[181] Relvaseadus. – RT I, 12.12.2018, 4.

[182] Strateegilise kauba seadus. – RT I, 29.06.2018, 59.

[183] Tolliseadus. – RT I, 11.01.2018, 14.

[184] Tunnistajakaitse seadus. – RT I, 29.06.2012, 46.

[185] Turvaseadus. – RT I, 03.03.2017, 27.

[186] Vangistusseadus. – RT I, 09.03.2018, 19.

[187] Välismaalaste seadus. – RT I, 29.06.2018, 76.

[188] Kriminaalmenetluse seadustiku muutmise, lk 3.

[189] IMEI (*International Mobile Equipment Identity*) on helistaja ja vastuvõtja rahvusvaheline mobiilside terminalseadme tunnus. (ESS § 111[1] lg 2 p 7.)

[190] IMSI (*International Mobile Subscriber Identity*) on helistaja ja vastuvõtja rahvusvaheline mobiilside tunnus. (ESS § 111[1] lg 2 p 6.)

[191] SIM (*Subscriber Identification Module Card*) on kiipkaart, mis identifitseerib abonendi mobiilside teenusepakkuja võrgule. (The Tech Terms Computer Dictionary. SIM Card. Arvutivõrgus: https://techterms.com/definition/sim_card (19.04.2019).)

[192] *Ibid*, lk 4.

väljatöötamiskavatsuses ei ole Justiitsministeerium pidanud oluliseks, et kriminaalmenetluses oleks loaandjaks kohus.[193]

Päringu tegemine sideettevõtjale ei ole aga alati põhjendatud. Nimelt lubab KrMS § 90^1 lg 3 teha päringu üksnes siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Kuna päringu tegemine sideettevõtjale on menetlustoiming, tuleb selle puhul alati lähtuda proportsionaalsuse põhimõttest ehk menetlustoimingu võib teha siis, kui see on vajalik ja ainult põhjendatud ulatuses. Päringut ei või seega teha igas olukorras, vaid see peab olema põhjendatud. Seda, et päringu võib teha üksnes vältimatu vajaduse korral ning KrMS § 90^1 lg-s 2 nimetatud päringu võib kohtueelses kriminaalmenetluses teha prokuratuuri loal, on seaduse eelnõu seletuskirjas peetud piisavateks tagatisteks isikute õiguste ja vabaduste kaitseks.[194]

Kehtiv seadus ei piira säilitatud sideandmete juurdepääsu vaid võitlusega raske kuritegevuse vastu. Selle põhjendamiseks on eelnõu seletuskirjas viidatud praeguseks kehtetuks tunnistatud andmete säilitamise direktiivile ning leitud, et raske kuritegevuse mõiste on jäetud liikmesriikide endi sisustada.[195] Arvesse võttes Euroopa Kohtu kohtupraktikat asjades *Tele2 Sverige* ja *Ministerio Fiscal*, ei oleks Eestis kehtiv üldine andmete säilitamise kohustus ning andmetele juurdepääsu põhjendamine võitlusega igasuguse kuritegevuse vastu proportsionaalne.

Õiguskantsleri nõunik on sideandmetele juurdepääsu kohta tõdenud, et selle puhul on suur oht kahjustada eraelu puutumatust. Selleks, et teha ettepanekuid seaduse muutmiseks, on tema hinnangul vaja teada, milline on seaduse rakendamise praktika. Selle uurimine oli 2018. aasta oktoobri seisuga Õiguskantsleri Kantseleis pooleli.[196]

Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsuses on analüüsitud säilitatud elektroonilise side metaandmete kasutamist. Väljatöötamiskavatsuses leitakse, et säilitatud andmete kasutamise puhul on vajalik oluliselt piiritleda juhud, mil on lubatud erinevates menetlustes päringuid teha. Kõige suuremal määral

[193] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 18.

[194] Kriminaalmenetluse seadustiku muutmise, lk 3, 5, 6.

[195] *Ibid*, lk 6.

[196] Külli Taro: jälitamisest ja jälgimisest. 4.10.2018. Arvutivõrgus: https://www.err.ee/866452/kulli-taro-jalitamisest-ja-jalgimisest (19.04.2019).

plaanitakse lubada säilitatud andmete kasutamist riigi julgeoleku tagamise eesmärgil. Laiemat andmete kasutamist lubatakse kriminaalmenetluse puhul eelkõige raskete kuritegude korral. Seevastu kergemate kuritegude korral soovitakse päringute tegemist piirata.[197]

Side metaandmete kasutamine kriminaalmenetluses oleks väljatöötamiskavatsuse kohaselt seega kooskõlas e-privaatsuse määruse algse ettepanekuga, millega lubataks kõigi kuritegude tõkestamise, uurimise ja avastamise eesmärgil metaandmeid säilitada. Juhul, kui arvesse võetakse e-privaatsuse määruse muudatusettepanekut, mille kohaselt võib andmeid kasutada vaid raskete kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise puhul, siis ei ole elektroonilise side andmete kasutamisel kriminaalmenetluses väljatöötamiskavatsus kooskõlas kavandatava e-privaatsuse määrusega.

Väljatöötamiskavatsuses leiti, et andmete diferentseerimine säilitamisel ei oleks efektiivne ja looks aluse diskrimineerimiseks.[198] Neil põhjustel, nagu leiti ka sideandmete säilitamist käsitlenud osas, soovitakse Eestis edaspidigi säilitada kõiki elektroonilise side metaandmeid ning teha piiranguid vaid andmetele juurdepääsu osas. Selles sarnaneb ESS muutmise väljatöötamiskavatsus Belgiale arusaamale, kuna Belgia on samuti pidanud võimatuks kehtestada diferentseeritud säilitamiskohustus ning soovinud põhiõigusi tagada vaid side metaandmete säilitamiseks ja kasutamiseks rangete tagatiste sätestamise abil.[199]

Tähelepanuväärne on see, et kaalutakse sideandmete kasutamise ranget piiritlemist väärteomenetluse ning haldus- ja tsiviilmenetluse puhul. Sideandmete kasutamist väärteomenetluses peetakse üldiselt erandlikuks ning see peab olema selgelt põhistatud. Väärtegude menetlemisel peetakse üheks võimalikuks kriteeriumiks, mille alusel võiks sideandmete kasutamine olla lubatud, et väärtegu on toime pandud sidevahendi vastu või sidevahendi vahendusel. Leitakse, et tuleb piiritleda, milliseid andmeid võib väärteomenetluses kasutada, sealjuures kas asukohaandmete kasutamine väärteomenetluses on proportsionaalne ning millistel juhtudel.[200]

Kuna Euroopa Kohus on säilitatud sideandmete kasutamisse suhtunud rangelt ning ka andmetele juurdepääsu puhul leidnud, et tuleb hinnata põhiõiguste riive ja kuriteo raskuse

[197] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 17.
[198] *Ibid*, lk 14, 15.
[199] Vt käesoleva töö lk 41-42.
[200] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 17.

proportsionaalsust[201] siis ei oleks andmete kasutamine väärteomenetluses kindlasti proportsionaalne ning oleks vastuolus Euroopa Liidu õigusega. Ka kavandatavas e-privaatsuse määruse ettepanekus plaanitakse sideandmete kasutamist piirata üksnes raske kuritegevuse vastu võitlemisega. Arvestades väärtegude eest ette nähtud karistusi ning seda, et tegemist on justnimelt väärtegudega, kergema süüteoliigiga, ei saa nende vastu võitlemist pidada raske kuritegevuse vastu võitlemiseks.

Haldus- ja tsiviilmenetluse puhul soovitakse samuti rangelt piiritleda andmed, millele on võimalik saada juurdepääs, ning millised menetluses ette tulnud asjaolud või kahtlused annavad aluse andmete kasutamiseks. Lisaks plaanitakse andmete kasutamise lubamist väiksemas ulatuses ja lühema aja vältel, samuti püütakse vältida üldisi sõnastusi, mis ei võimalda hinnata normi ulatust ja mõju ning seda, kuidas on järgitud põhiseadusest ja Euroopa Liidu õigusest tulenevaid nõudeid põhiõiguste kaitsel.[202] Töö autori hinnangul ei saa haldus- ja tsiviilmenetluses andmete kasutamist pidada põhjendatuks. Kehtiva e-privaatsuse direktiivi, Euroopa Kohtu praktika ega ka kavandatava e-privaatsuse määruse põhjal ei saa sellisel eesmärgil elektroonilise side andmete kasutamist pidada põhjendatuks. Samas kui ka tulevikus lubatakse haldus- ja tsiviilmenetluse puhul metaandmetele juurdepääsu, siis andmete kasutamine väiksemas ulatuses ja lühema aja vältel vähendaks oluliselt isikute põhiõiguste riivet.

Kõik järgnevad tegurid mõjutavad andmete kasutamise proportsionaalsuse tagamist, mistõttu on väljatöötamiskavatsuses peetud vajalikuks reguleerida, milliseid meetmeid on vaja, et teostada tõhusat järelevalvet, kuidas toimub päringute tegemise dokumenteerimine, kuidas säilitatakse andmeid peale nende kasutamist, millal need kustutatakse ning kuidas reguleerida andmete edasist kasutamist. Kuna tähtsaks peetakse ka tõhusa järelevalve tagamist, siis peab tulevikus olema võimalik tuvastada, miks ja millise menetluse raames on päring tehtud, milliseid andmeid saadi, kas andmesubjekte on teavitatud ning kas andmed kajastuvad näiteks kriminaaltoimikus või on kustutatud.[203]

Tõhus järelevalve ning kasutatud andmete edasise käitlemise reguleerimine aitab tagada, et andmeid kasutatakse õiguspäraselt ning et nende töötlemine on proportsionaalne. Järelevalve

[201] EKo *Ministerio Fiscal*, p 56.
[202] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 17.
[203] *Ibid*, lk 18, 19.

tagamine aitab vähendada inimeste hulgas hirmu, et nende sideandmeid alusetult kasutatakse, samuti vähendab see reaalset andmete väärkasutamise ohtu ja sellest tulenevat põhiõiguste ebaproportsionaalset riivet.

Proportsionaalsuse põhimõttest kinnipidamise ja isikute põhiõiguste kaitse tagamiseks soovitakse väljatöötamiskavatsuse järgi tulevikus senisest rohkem tähelepanu pöörata sellele, milline asutus ja mis kaalutlustel annab loa sideandmete päringu esitamiseks. Praegu kehtiva seaduse järgi annab loa sideandmete kasutamiseks kriminaalmenetluses prokuratuur.[204] Väljatöötamiskavatsuse kohaselt ei ole Justiitsministeeriumi hinnangul oluline, et sideandmete kasutamiseks kriminaalmenetluses annaks loa kohus.[205] Küll aga soovitakse üle vaadata sätted, mis käsitlevad loa andmist andmete kasutamiseks muudes menetlustes, ning muuta loamenetluse reeglid menetluste lõikes võimalikult ühtseks ja selgeks.[206]

Nagu käsitletud alapeatükis 2.3.4 Eesti eelotsusetaotluses esitatud kolmanda küsimuse juures, võib ka prokuratuuri pidada sõltumatuks haldusasutuseks, kes on Euroopa Inimõiguste Kohtu praktikat arvesse võttes õigustatud kuritarvituste vältimiseks andma loa metaandmetele juurdepääsuks. Loamenetluse reeglite ühtlustamise ja selgeks muutmise osas tuleb tõdeda, et see aitaks kaasa põhiõiguste tagamisele, kuna selged ja üheselt mõistetavad normid hõlbustavad seaduste kohaldamist. Arusaamatuks jääb aga, kuidas aitab põhiõiguste tagamisele kaasa see, et side metaandmeid soovitakse säilitada ja kasutada erinevate menetluste tarbeks, kui Euroopa Kohus on lahendis *Tele2 Sverige* pidanud isegi raske kuritegevuse vastu võitlemise eesmärgil põhjendatuks andmete ennetavat säilitamist vaid piiratuna rangelt vajalikuga. Seega ei aitaks andmetele juurdepääsu reeglite ühtlustamine eriti kaasa põhiõiguste kaitsele, kui metaandmeid plaanitakse ka edaspidi säilitada lisaks kuritegevuse vastu võitlemisele ka mitmetes teistes menetlustes kasutamise eesmärgil, sest see oleks kohtupraktikat arvesse võttes nagunii rängalt ebaproportsionaalne ning põhiõigusi riivav.

Samuti soovitakse isikute põhiõiguste kaitse tagamiseks tulevikus tähelepanu pöörata isikute teavitamisele andmete kasutamisel või andmete kasutamise järgselt. Kriminaalmenetluses ei peeta kohaseks küll kõigi isikute teavitamist, kelle telefoninumbrid võivad olla kõneeristusel, sest selleks peaks andmeid täiendavalt töötlema, et leida telefoninumbri omanik ja tema

[204] KrMS § 90^1 lg 2.

[205] Riigikohtu poolt Euroopa Kohtule esitatud eelotsusetaotluse kohta, kus käsitletakse prokuratuuri poolt loa andmist sideandmete kasutamiseks vt peatükk 2.3.4.

[206] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus, lk 18.

kontaktandmed. Siiski soovitakse, et tulevikus teavitataks neid isikuid, kelle andmeid töödeldi ja kelle puhul on isiku teavitamine võimalik. Lisaks soovitakse üle vaadata andmete kasutamisest teavitamise ja andmete tutvustamise võimalused teiste menetluste puhul.[207]

Kuna andmete kasutamise proportsionaalsuse tagamist mõjutab ka päringute esitamise dokumenteerimine, tõhusa järelevalve teostamine, pädevate asutuste poolt andmete säilitamine pärast nende kasutamist ning andmete edasise kasutamise reeglid, siis tuleb väljatöötamiskavatsuse kohaselt seaduse tasandil kindlustada, et andmeid ei kasutataks õigustamata ning vältida olukorda, kus järelevalvemenetluses ei ole võimalik välja selgitada, miks, kellele ja millises olukorras andmeid edastati ja kuidas neid pärast edastamist kasutati. Arvestades seda, et kriminaalmenetluse raames võidakse töödelda ka nende isikute sideandmeid, kes ei ole menetlusega seotud, siis tuleb kindlustada, et neid isikuid puudutav teave hävitatakse kohe, kui tuleb välja, et isik ei ole menetletava asjaga seotud. Samuti tuleks kõneeristuste puhul tagada, et ei säilitataks ega töödeldaks menetluse kontekstis mitteasjakohaste kõne osapoolte andmeid.[208]

Isikute teavitamine pärast metaandmete kasutamist oleks kooskõlas *Tele2 Sverige* lahendiga. Selles otsuses leidis Euroopa Kohus, et ametiasutused, kellele on antud sideandmetele juurdepääs, peaksid asjassepuutuvaid isikuid teavitama kohe, kui teavitamine ei saa enam kahjustada menetluse läbiviimist. Eelkõige on otsuse kohaselt teavitamine tähtis selleks, et isikud saaksid oma õiguste rikkumise korral kasutada õiguskaitsevahendeid.[209] Samas ei saa teavitamiskohustust pidada tingimata vajalikuks juhtudel, kus teavitamiskohustuse täitmisega kaasneks täiendav põhiõiguste riive näiteks teavitatava isiku ja tema kontaktandmete kindlakstegemise vajaduse tõttu. Päringute dokumenteerimine ja järelevalve teostamine oleksid kooskõlas ka e-privaatsuse määruse ettepaneku artikliga 11 lg 2 lausega 2, mille kohaselt peaksid elektroonilise side teenuste osutajad esitama pädevatele järelevalveasutustele viimaste poolt taotluse esitamisel teabe saabunud taotluste arvu, viidatud õigusliku aluse ja oma vastuse kohta.[210]

[207] *Ibid*, lk 18.
[208] *Ibid*, lk 18, 19.
[209] EKo *Tele2 Sverige*, p 121.
[210] Ettepanek, lk 28.

Kokkuvõte

Töö eesmärgiks oli selgitada välja millistel tingimustel ja millises ulatuses on õigustatud elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses. Eesmärgiks oli sealhulgas välja selgitada, kuidas soovitakse elektroonilise side metaandmete säilitamist ja kasutamist reguleerida uue e-privaatsuse määruse ettepaneku ning elektroonilise side seaduse muutmise eelnõu väljatöötamiskavatsuse kohaselt.

Euroopa Kohus tunnistas 2014. aastal tehtud otsuses *Digital Rights Ireland* kehtetuks andmete säilitamise direktiivi, mille eesmärgiks oli ühtlustada liikmesriikide õigusnormid, millega reguleeriti elektroonilise side andmete säilitamist. Direktiiv tunnistati kehtetuks, sest selles ei piirdutud elektroonilise side andmete säilitamisel vaid vältimatult vajalikuga ning liidu seadusandja oli direktiivi vastuvõtmisega ületanud proportsionaalsuse põhimõttest tulenevaid piiranguid. Selles direktiivis sisaldunud sätted on Eesti riigisisesesse õigusesse üle võtnud elektroonilise side seaduses ning need kehtivad praeguse ajani.

Pärast direktiivi kehtetuks tunnistamist, esitasid Euroopa Kohtule eelotsusetaotlused Rootsi ja Ühendkuningriigi kohtud. Liidetud kohtuasjas *Tele2 Sverige* leidis Euroopa Kohus, et liikmesriikide õigusnorme, mis kohustavad sideettevõtjaid säilitama üldiselt kõiki elektroonilise side metaandmeid, ei saa pidada Euroopa Liidu õigusega kooskõlas olevaks. Siiski leidis kohus, et metaandmete säilitamine on raskete kuritegude menetlemise eesmärgil lubatav, kui andmete säilitamine on piiratud säilitatavate andmete liigi, asjassepuutuvate sidevahendite ja isikute ning säilitamise kestuse osas rangelt vajalikuga. Säilitatud side metaandmetele juurdepääsu kohta leiti samas otsuses, et kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgi puhul saab säilitatavatele andmetele juurdepääsu andmist põhjendada ainult võitlusega raske kuritegevuse vastu.

2018. aastal tegi Euroopa Kohus otsuse asjas *Ministerio Fiscal*, milles kohus selgitas elektroonilise side metaandmetele juurdepääsu tingimusi. Kohus leidis, et e-privaatsuse direktiivi artikli 15 lg 1 lause 1 sõnastus peab silmas kuritegusid üldiselt ega piira kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärki võitlusega vaid raskete kuritegude vastu. Kohus selgitas proportsionaalsuse põhimõtet, mille kohaselt peab liikmesriigi õigusnormidega taotletav eesmärk olema proportsioonis andmetele juurdepääsuga kaasneva põhiõiguste riive raskusega. Selgituse kohaselt, kui andmetele juurdepääsuga kaasnev riive ei

ole raske, võib juurdepääsu põhjendada üldiselt kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga. Seevastu kui riive on raske, siis saab ka juurdepääsu põhjendada vaid raskete kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga. Kuna kohus *Ministerio Fiscal*'i lahendis side metaandmete säilitamise õiguspärasust ei hinnanud, siis on võimalik, et Euroopa Kohus võib pidada õiguspäraseks ka ebaseaduslikult säilitatud andmetele juurdepääsu. Samas on varem Euroopa Kohus kasutanud tõhususe argumenti, et välistada põhiõigusi rikkuvate tõendite kasutamine.

Lahendi *Ministerio Fiscal* asjaolude kohaselt ei olnud tegemist põhiõiguste raske riivega, mistõttu sai juurdepääsu põhjendada üldiselt kuritegude menetlemise eesmärgiga. Sel põhjusel ei selgitanud kohus, mille alusel peaksid liikmesriigid juhul, kui põhiõiguste riive oleks raske, kuritegude raskust hindama. Tõenäoline on, et sellisel juhul tuleks liikmesriikidel endil kuriteo raskust hinnata võttes arvesse *Tele2 Sverige* lahendist tulenevat põhimõtet, et erand andmete säilitamise keelust ei või saada reegliks.

Elektroonilise side andmete säilitamise ja kasutamisega võivad kaasneda mitmesugused põhiõiguste riived. Nendeks on eelkõige perekonna- ja eraelu puutumatuse, kodu puutumatuse ja sõnumite saladuse põhiõiguste riived, samuti sõnavabaduse riive. Perekonna- ja eraelu puutumatus, kodu puutumatus ja sõnumite saladuse põhiõigus on sätestatud inimõiguste konventsiooni artikkel 8 lg-s 1 ning põhiõiguste harta artiklis 7. Eesmärgid, mille nimel neid põhiõigusi võib piirata on sätestatud inimõiguste konventsiooni artikkel 8 lg-s 2. Eesti põhiseaduses on nimetatud põhiõigused sätestatud eri paragrahvides ning nende riivet õigustavad eesmärgid on samuti erinevad. Konventsiooni artiklis 8 ja põhiõiguste harta artiklis 7 sätestatud sõnumite saladuse kaitse alla kuuluvad ka elektroonilise side metaandmed, kuid Eesti põhiseaduse § 43, mis sätestab samuti sõnumite saladuse kaitse, kaitsealasse metaandmed ei kuulu.

Euroopa Inimõiguste Kohtu praktikas on peetud inimõiguste ja põhivabaduste kaitse konventsiooni artikliga 8 kooskõlas olevaks sätteid, mis lubavad prokuratuuri või kohtu eelneval loal saada juurdepääsu sideteenuse osutaja säilitatavatele side metaandmetele. Seejuures on kohus arvesse võtnud kuritarvituste vastaste tagatiste olemasolu – eelnevat loa taotlemist ning loa andmise õiguspärasust tagantjärele hindava kohtu olemasolu.

Jälgimisrežiimide põhiõigustele vastavuse puhul on inimõiguste kohus arvesse võtnud piisavate ja tõhusate kaitsemeetmete ja garantiide olemasolu, mis muudavad režiimid ettenähtavaks ja

vähendavad võimu kuritarvitamise riski. Euroopa Inimõiguste Kohus on küll väljendanud seisukohta, et ta ei ole veendunud, et elektroonilise side metaandmete omandamine on vähem riivav kui side sisu hõivamine, kuid ei ole metaandmetele juurdepääsuks pidanud vajalikuks nii paljude kaitsemeetmete olemasolu kui side pealtkuulamise puhul.

Käesolevas magistritöös oli püstitatud kaks hüpoteesi. Esimeseks hüpoteesiks oli, et elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses oleks kavandatava e-privaatsuse määruse kehtima hakkamisel põhjendatud vaid piiratud tingimustel tulenevalt sideandmete säilitamise ja kasutamisega kaasnevast põhiõiguste riivest.

E-privaatsuse määruse ettepaneku kohaselt soovitakse sellega tagada side konfidentsiaalsuse põhimõtet ning kohaldada seda praegu kasutusel olevate kui ka tulevikus kasutusele võetavate sidevahendite suhtes. Konfidentsiaalseks peetakse nii elektroonilise side sisu kui ka metaandmeid. Määruse ettepaneku seletuskirja kohaselt Euroopa Liidu tasandil enam elektroonilise side metaandmete säilitamist reguleerima ei hakata. Määruse ettepanek ei sisalda konkreetseid sätteid andmete säilitamise kohta, kuid lubab liikmesriikidel luua riiklikke andmete säilitamise raamistikke. Liikmesriikide andmete säilitamise meetmed peavad vastama Euroopa Liidu õigusele, võttes arvesse e-privaatsuse direktiivi ja põhiõiguste harta tõlgendamise kohta käivaid Euroopa Kohtu otsuseid.

Kavandatav e-privaatsuse määrus ei anna otsesõnu võimalust metaandmete kohustuslikuks säilitamiseks, kuid lubab side konfidentsiaalsust piirata üldiste huvide kaitseks, kui austatakse põhiõiguste ja -vabaduste olemust. Algses määruse ettepanekus viidati isikuandmete kaitse üldmäärusele, mis näeb ühe võimalusena ette õiguste ja kohustuste piiramise, et tagada süütegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine. E-privaatsuse määruse muudatusettepanekus soovitakse aga ühe side konfidentsiaalsuse piiramist õigustava eesmärgina sätestada raskete kuritegude tõkestamine, uurimine, avastamine või nende eest vastutusele võtmine. Seega soovitakse muudatusettepanekus muuta kitsamaks eesmärki, mille alusel saab piirata õigust side konfidentsiaalsusele. Kui nimetatud muudatusettepanekuga arvestatakse, siis on tulevikus liikmesriikidel kriminaalmenetluses võimalik side metaandmetele juurdepääs vaid piiratud tingimustel – raskete kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise puhul.

Teine hüpotees väitis, et elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses on elektroonilise side seaduse ja sellega seonduvalt teiste seaduste

muutmise eelnõu väljatöötamiskavatsuse kohaselt kooskõlas kavandatava e-privaatsuse määrusega.

Eestis praegu kehtivad ESS normid kohustavad elektroonilise side ettevõtjaid säilitama kõiki side metaandmeid, mistõttu ei ole ESS-i sätted, eelkõige tulenevalt lahendist *Tele2 Sverige*, Euroopa Liidu õigusega kooskõlas. Sellest tulenevalt tekkis vajadus ESS-i muuta. Käesolevaks ajaks on lõppenud elektroonilise side ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsuse kooskõlastamise etapp. Eelnõu väljatöötamiskavatsuse alusel on plaanis sideandmete säilitamisel eristada, kas andmeid säilitatakse kriminaalmenetluslikul, riigi julgeoleku või muul eesmärgil. Riigi julgeoleku eesmärgil on plaanis kõikide elektroonilise side metaandmete säilitamine. Seega planeeritakse sisuliselt kõikide elektroonilise side metaandmete säilitamist ning kavatsetakse piirata üksnes neile andmetele juurdepääsu pädevate ametiasutuste poolt vastavalt säilitamise eesmärgile ja säilitamistähtajale. Elektroonilise side andmete üldine säilitamine ja vaid kasutamise eesmärkide ja säilitamistähtaegade osas piirangute seadmine ei oleks käesoleva töö autori arvates kooskõlas kohtuotsuses *Tele2 Sverige* välja toodud põhimõttega, et üldine kõikide sideandmete säilitamine ei ole põhjendatud ning liikmesriigid peavad piirama säilitatavaid andmeid nende liigi, asjassepuutuvate sidevahendite, isikute ning säilitamise kestuse osas rangelt vajalikuga.

Elektroonilise side andmetele juurdepääsu ei käsitleta 2013. aastast alates enam jälitustoiminguna vaid menetlustoiminguna. Seejuures on omanikupäringu tegemiseks õigustatud menetleja ning lisaks omanikupäringu abil saadavatele andmetele on kohtueelses menetluses prokuratuuri loal ning kohtumenetluses kohtu loal võimalik teha päring teistele elektroonilise side andmetele juurdepääsu saamiseks. Ka eelnõu väljatöötamiskavatsuses ei ole peetud vajalikuks, et loaandjaks oleks prokuratuuri asemel kohtueelses menetluses kohus. Seda seisukohta võib lugeda põhjendatuks, kuna prokuratuur peab seadusest tulenevalt juhtima kriminaalmenetlust sõltumatult. Samuti on inimõiguste kohus tunnustanud ühena põhiõiguste kuritarvitamise vastastest tagatistest sideettevõtjale metaandmete kohta päringu tegemisel prokuratuuri poolt eelneva loa taotlemise kohtustust.

Väljatöötamiskavatsuse kohaselt plaanitakse tulevikus lisaks riigi julgeoleku tagamise ja kuritegude menetlemise eesmärgil metaandmetele juurdepääsu lubamisele, lubada sideandmete kasutamist ka väärteomenetluse ning haldus- ja tsiviilmenetluse puhul. Viimastel eesmärkidel andmete kasutamist soovitakse küll rangelt piiritleda, ei oleks selline side metaandmete

kasutamine kooskõlas Euroopa Liidu õigusega. Seda ei praeguse kohtupraktika alusel ega ka kavandatava e-privaatsuse määruse valguses.

Kokkuvõttes leidis esimene püstitatud hüpoteesidest kinnitust. E-privaatsuse määruse ettepanekus kavatsetakse rangelt piiritleda eesmärgid, mille puhul on õigustatud elektroonilise side andmete säilitamine ja kasutamine ning sellega kaasnevad põhiõiguste riived.

Teine hüpotees leidis osaliselt kinnitust. Elektroonilise side seaduse väljatöötamiskavatsuses soovitakse endiselt säilitada kõiki elektroonilise side metaandmeid ning piirata andmekategooriate abil vaid neile andmetele juurdepääsu erinevate menetluste raames. Erinevate menetluste ring on lai hõlmates nii haldus-, tsiviil- kui ka väärteomenetlust. Kriminaalmenetluses kavatsetakse siiski eristada raskemaid ja kergemaid kuritegusid, millest esimese puhul lubatakse laiemat andmete kasutamist. Seetõttu ei oleks andmete säilitamise osas elektroonilise side seaduse muutmise väljatöötamiskavatsus kooskõlas kavandatava e-privaatsuse määrusega, mille järgi tuleb liikmesriikidel arvestada ka Euroopa Kohtu otsuseid e-privaatsuse direktiivi tõlgendamise kohta. Metaandmete kasutamine kriminaalmenetluses oleks väljatöötamiskavatsuse kohaselt kooskõlas e-privaatsuse määruse algse ettepanekuga. Juhul, kui arvesse võetakse muudatusettepanekut, mille kohaselt võib andmeid kasutada vaid raskete kuritegude tõkestamise, uurimise, avastamise ja nende eest vastutusele võtmise puhul, siis ei ole ka elektroonilise side andmete kasutamise puhul kriminaalmenetluses väljatöötamiskavatsus kooskõlas kavandatava e-privaatsuse määrusega.

Retention of electronic communication metadata and usage of metadata in criminal procedure

Summary

In recent years, there has been an increasing debate in the society that the state is monitoring people more than it is believed. Many people are afraid that they are constantly being monitored and interfered in their right to privacy. One form of tracking is the retention of traffic and location data of electronic communications and making it available to the authorities. The retained metadata generally includes traffic data i.e. data about how a communication was transmitted including source, destination, time and location of transmission, subscriber data i.e. data identifying subscribers and data specific to the use of the communications service in question i.e. time of use, amount of data downloaded.

Following the European Court of Justice's decisions in the cases *Digital Rights Ireland* and *Tele2 Sverige* on retention of electronic communications data, Member States have not rushed to amend their national laws. According to the report published in September 2017, none of the examined 21 European Union Member States' legislation were in accordance with European Court of Justice's case law and human rights standards.

In recent years new requests for a preliminary ruling have been made to the European Court of Justice to clarify under what conditions and to what extent the retention and use of electronic communications data could comply with European Union law. European Court of Justice and European Court of Human Rights have made new decisions to clarify the situation. Since 2017 in European Union a new e-Privacy draft Regulation is discussed and at the end of the 2018 in Estonia legislative intent to draft an amendment to the Electronic Communications Act and other related acts was published. Thus, the topic of retention and use of electronic communications metadata is relevant in Estonia.

The aim of this thesis was to find out the conditions and extent to which the retention and use of electronic communications data in criminal proceedings is justified in the light of the proposal for a new e-Privacy Regulation and the legislative intent to amend Electronic Communications Act. The author proposed two hypotheses. First, if the e-Privacy Regulation will be in force, the retention and use of electronic communications metadata in criminal

proceedings would be justified only in limited circumstances due to the violation of fundamental rights arising from the storage and use of communication metadata. The second hypothesis stated that the legislative intent to amend Electronic Communications Act is in accordance with the proposal for a new e-Privacy Regulation concerning the retention and use of electronic communications metadata in criminal procedure.

The first chapter discussed how the retention of electronic communications data is regulated in European Union law and how it has been changed by the case law of the European Court of Justice and what kind of changes will be made by the new e-Privacy draft Regulation. In 2006 the European Union enforced Data Retention Directive which imposed the types of data for which Member States were required to ensure the retention of. In 2014 the European Court of Justice in its decision in case *Digital Rights Ireland* declared the Data Retention Directive invalid because the European Union legislature had exceeded the limits imposed by compliance with the principle of proportionality in the light of Articles 7, 8 and 52(1) of the Charter of Fundamental Rights of the European Union.

In European countries, however, questions were raised about the impact of the *Digital Rights Ireland* judgment and the repeal of the Data Retention Directive on national law. In its 2016 decision in case *Tele2 Sverige* the European Court of Justice stated that even fight against serious crime cannot justify national legislation providing for the general and indiscriminate retention of all traffic and location data. However, the Court pointed out that Member States may adopt legislation permitting, as a preventive measure, the targeted retention of traffic and location data, for the purpose of fighting serious crime.

The new e-Privacy draft Regulation does not contain very specific provisions on data retention. However, Member States can maintain or establish national data retention frameworks. According to the explanatory memorandum, such frameworks allow Member States to establish, among other things, measures for the retention of communications data in compliance with European Union law, taking into account the rulings of the European Court of Justice on the interpretation of the e-Privacy Directive and the Charter of Fundamental Rights.

In the first chapter the retention of electronic communications metadata in valid Electronic Communications Act and in legislative intent were analysed. First chapter also gave an overview of interference of fundamental rights which is caused by retention of electronic communication metadata. Electronic Communications Act’s provisions which impose on

providers of electronic communications services an obligation to retain metadata with no exceptions is not in accordance with the ruling in case *Tele2 Sverige*. Even in the legislative intent the retention of all electronic communications metadata is planned and only access to the data by the competent authorities is restricted according to the purpose of retention.

In the second chapter the access to the retained metadata was discussed. The European Court of Justice has explained in the case *Ministerio Fiscal* that "in accordance with the principle of proportionality, serious interference can be justified, in areas of prevention, investigation, detection and prosecution of criminal offences, only by the objective of fighting crime which must also be defined as 'serious'". When the interference by access to metadata is not serious, that access can be justified by the objective of preventing, investigating, detecting and prosecuting 'criminal offences' generally.

The original proposal for the e-Privacy Regulation referred to the General Data Protection Regulation, which provides for the restriction of rights and obligations to prevent, investigate, detect or prosecute criminal offenses. However, the amendment to the e-Privacy Regulation seeks to provide for the prevention, investigation, detection or prosecution of serious criminal offenses as a legitimate reason for limiting the confidentiality of a communication. If this amendment is taken into account, Member States will only be able to access metadata in criminal proceedings under limited conditions – preventing, investigating, detecting and prosecuting serious crimes.

The second chapter also discussed recent practice of the European Court of Human Rights and requests for the preliminary rulings from Member States to the European Court of Justice. The requests made by the Member States for preliminary rulings indicate that the States still wish to retain indiscriminately all the traffic and location data of electronic communications. Member States wish to find a way to retain all electronic communication metadata and therefore search for different arguments and interpretations in the European Court of Justice's case law. Based on the submitted questions the retained metadata is to be used for both national security and crime prevention, investigation and detection purposes.

Lastly the access to retained metadata in Estonian law was analysed. As of 2013, access to electronic communications metadata will no longer be regarded as a surveillance activity but as a procedural act. Also, the current law does not restrict access to retained communications data to the fight against serious crime.

According to the legislative intent in addition to allowing access to metadata for the purpose of ensuring national security and criminal procedure, the use of communication metadata in misdemeanour, administrative and civil proceedings is also allowed. For the latter purposes, the use of data is to be limited strictly. Nonetheless, such access to communication metadata would not be in accordance with European Union law. Also, it would not be in accordance with the case law nor the proposed e-Privacy Regulation.

In conclusion, the first hypothesis was supported. The proposal for an e-Privacy Regulation intends to strictly define the objectives justifying the retention and use of electronic communications metadata. The second hypothesis was partially supported. The legislative intent of the Electronic Communications Act is to retain all the metadata of electronic communications and to limit only the access to data in different procedures by means of different categories of data. The range of procedures is wide, covering both administrative, civil and misdemeanour procedures. However, in criminal procedure it is planned to distinguish between more serious and lighter offenses, the first of which allows wider use of data. Therefore, concerning data retention, the legislative intent to amend Electronic Communications Act would not be in line with the proposed e-Privacy Regulation, which requires Member States to take into account the European Court of Justice's decisions on the interpretation of the e-Privacy Directive. The use of metadata in criminal procedure would be in line with the original proposal of the e-Privacy Regulation. If the amendment that allows data to be used only for the prevention, investigation, detection and prosecution of serious criminal offenses will be in force, the legislative intent of the Electronic Communications Act is not in line with the proposed e-Privacy Regulation considering the use of metadata in criminal procedure.

30.04.2019

Kasutatud materjalid

Kohtupraktika

1. EIKo 03.04.2007, 62617/00, *Copland vs. Ühendkuningriik*.
2. EIKo 04.12.2008, 30562/04, 30566/04, *S. ja Marper vs. Ühendkuningriik*.
3. EIKo 13.09.2018, 58170/13, 62322/14, 24960/15, *Big Brother Watch jt vs. Ühendkuningriik.*
4. EIKo 19.06.2018, 35252/08, *Centrum för Rättvisa vs. Rootsi*.
5. EIKo 29.06.2006, 54934/00, *Weber ja Saravia vs. Saksamaa*.
6. EIKo 4.12.2015, 47143/06, *Roman Zakharov vs. Venemaa*.
7. EIKo 8.02.2018, 31446/12, *Ben Faiza vs. Prantsusmaa*.
8. EIKo 8.11.2016, 72384/14, *Figueiredo Teixeira vs. Andorra*.
9. EKo 06.09.2011, C-163/10, *Patriciello*.
10. EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland*.
11. EKo 17.12.2015, C-419/14, *WebMindLicenses.*
12. EKo 2.10.2018, C-207/16, *Ministerio Fiscal*.
13. EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige*.
14. RKKKm 12.11.2018, 1-16-6179.
15. RKKKo 20.11.2015, 3-1-1-93-15.
16. RKKKo 21.03.2003, 3-1-1-25-03.
17. RKKKo 23.02.2015, 3-1-1-51-14.
18. RKKKo 30.06.2014, 3-1-1-14-14.

Õigusaktid

Eesti õigusaktid:

19. Eesti Vabariigi põhiseadus. – RT I, 15.05.2015, 2.
20. Elektroonilise side seadus. – RT I, 12.12.2018, 33.
21. Elektroonilise side seaduse ja rahvatervise seaduse muutmise seadus. – RT I 2007, 63, 397.
22. Julgeolekuasutuste seadus. – RT I, 05.05.2017, 2.
23. Kaitseväe korralduse seadus. – RT I, 29.05.2018, 2.
24. Kriminaalmenetluse seadustik. – RT I, 13.03.2019, 7.
25. Maksukorralduse seadus. – RT I, 07.12.2018, 5.

26. Politsei ja piirivalve seadus. – RT I, 05.02.2019, 3.
27. Relvaseadus. – RT I, 12.12.2018, 4.
28. Strateegilise kauba seadus. – RT I, 29.06.2018, 59.
29. Tolliseadus. – RT I, 11.01.2018, 14.
30. Tunnistajakaitse seadus. – RT I, 29.06.2012, 46.
31. Turvaseadus. – RT I, 03.03.2017, 27.
32. Vangistusseadus. – RT I, 09.03.2018, 19.
33. Välismaalaste seadus. – RT I, 29.06.2018, 76.

Rahvusvahelised õigusaktid:

34. Euroopa Liidu lepingu ja Euroopa Liidu toimimise lepingu konsolideeritud versioonid. – ELT 2016/C 202/01, 7.06.2016.
35. Euroopa Liidu põhiõiguste harta. – ELT C 326, 26.10.2012.
36. Euroopa Parlamendi ja nõukogu direktiiv 2000/31/EÜ, 8. juuni 2000, infoühiskonna teenuste teatavate õiguslike aspektide, eriti elektroonilise kaubanduse kohta siseturul (direktiiv elektroonilise kaubanduse kohta). – ELT L 178, 17.07.2000.
37. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). – ELT L 201, 31.07.2002.
38. 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. – ELT L 105, 13.04.2006.
39. Euroopa Parlamendi ja nõukogu direktiiv 2011/92/EL, 13. detsember 2011 , mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust ja mis asendab nõukogu raamotsuse 2004/68/JSK. – ELT L 335, 17.12.2011.
40. Euroopa Parlamendi ja nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. – ELT L 281, 23.11.1995.
41. Euroopa Parlamendi ja nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). – ELT L 119, 4.05.2016.

42. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2000, 11, 57.
43. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.

Muud allikad

44. Advokaadid: Eesti riik rikub elektroonilise side andmeid kogudes ja kasutades teadlikult ja räigelt inimõigusi. – Objektiiv, 20.11.2017.
45. Banisar, D, Davies, S. Global Trends in Privacy Protection: An International Survey of Privacy, Data Protection, and Surveillance Laws and Developments. – The John Marshall Journal of Information Technology & Privacy Law. 1999/1.
46. Eelotsusetaotluse kokkuvõte vastavalt Euroopa Kohtu kodukorra artikli 98 lõikele 1. Kohtuasi C-520/18. Arvutivõrgus: https://eelnoud.valitsus.ee/main/mount/docList/0226101f-9cd8-46e9-b80c-7dcd6ae7ccf8 (22.03.2019).
47. Eesti seisukohad Euroopa Kohtule liidetud eelotsusetaotluste C-511/18 ja C-512/18 (French Data Network) ja eelotsusetaotluse C-520/18 (Ordre des barreaux francophones et germanophone) kohta. Eelnõu toimik nr 18-1233. Arvutivõrgus: https://eelnoud.valitsus.ee/main/mount/docList/0226101f-9cd8-46e9-b80c-7dcd6ae7ccf8 (22.03.2019).
48. EK C-207/16, *Ministerio Fiscal*, kohtujurist H. Saugmandsgaard Øe ettepanek.
49. EK C-520/18, *Ordre des barreaux francophones et germanophone jt versus Conseil des ministres*, eelotsusetaotlus.
50. EK C-623/17, *Privacy International versus Secretary of State for Foreign and Commonwealth Affairs jt*, eelotsusetaotlus.
51. EK liidetud kohtuasjad C-511/18 ja C-512/18, *French Data Network*, eelotsusetaotlus.
52. Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine). Arvutivõrgus: http://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83?activity=1#fVKzRoTp (20.02.2019).
53. Ettepanek: Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). 10.01.2017. Arvutivõrgus: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010&qid=1550151482281 (14.02.2019).

54. Euroopa Inimõiguste Kohus. Inimõiguste ja põhivabaduste kaitse konventsiooni inglis- ja prantsuskeelne versioon. Arvutivõrgus: https://www.echr.coe.int/Pages/home.aspx?p=basictexts/convention (12.04.2019).
55. European Court of Human Rights. Hearings, Cases pending before the Grand Chamber. Arvutivõrgus: https://www.echr.coe.int/Pages/home.aspx?p=hearings/gcpending&c (3.04.2019).
56. ICT Regulation Toolkit. Regulating 'Over-the-Top' Services. Arvutivõrgus: http://www.ictregulationtoolkit.org/toolkit/2.5 (20.04.2019).
57. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 175 SE. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. Arvutivõrgus: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0 (02.04.2019).
58. Külli Taro: jälitamisest ja jälgimisest. 4.10.2018. Arvutivõrgus: https://www.err.ee/866452/kulli-taro-jalitamisest-ja-jalgimisest (19.04.2019).
59. La Rue, F. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. 17.04.2013. A/HRC/23/40. Arvutivõrgus: www.un.org/Docs/journal/asp/ws.asp?m=A/HRC/23/40 (21.04.2019).
60. Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Tartu, 2015.
61. Lõhmus, U. Kolm suurt probleemi kodanike jälgimisega. – ERR 21.09.2018. Arvutivõrgus: https://www.err.ee/862981/uno-lohmus-kolm-suurt-probleemi-kodanike-jalgimisega (16.04.2019).
62. Lõhmus, U. Põhiõigused kriminaalmenetluses. Tallinn: Juura 2014.
63. Lõhmus, U. Veel kord õigusest sõnumite saladusele ehk kuidas 20. sajandi tehnoloogia mõjutab põhiseaduse tõlgendusi. – Juridica III/2016.
64. Madise, Ü jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 4. vlj. Tallinn: Juura 2017.
65. Madise, Ü. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus. 22.04.2016. Arvutivõrgus: https://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (15.02.2019).
66. Madise, Ü. Õiguskantsleri seisukoht elektroonilise side seaduse § 111^1 põhiseaduspärasuse kohta. 20.07.2015. Arvutivõrgus: https://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotte_poolt.pdf (15.02.2019).

67. National Data Retention Laws since the CJEU's Tele-2/Watson Judgment. A Concerning State of Play for the Right to Privacy in Europe. Privacy International. September 2017. Arvutivõrgus: https://privacyinternational.org/sites/default/files/2017-10/Data%20Retention_2017_0.pdf (20.04.2019).
68. Press Release: New Privacy International Report Shows That 21 European Countries Are Unlawfully Retaining Personal Data. Privacy International. 6.09.2017. Arvutivõrgus: https://privacyinternational.org/press-release/634/press-release-new-privacy-international-report-shows-21-european-countries-are (19.04.2019).
69. Pruul, K. Riik lausjälgimisest loobuma ei rutta. – Äripäev 28.11.2018.
70. Raport ettepaneku kohta võtta vastu Euroopa Parlamendi ja nõukogu määrus, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus). Menetlus 2017/0003(COD).
71. Raport Euroopa Parlamendi ja nõukogu 13. detsembri 2011. aasta direktiivi 2011/93/EL (mis käsitleb laste seksuaalse kuritarvitamise ja ärakasutamise ning lasteporno vastast võitlust) rakendamise kohta. Menetlus (2015/2129(INI)). Euroopa Parlamendi resolutsiooni ettepanek.
72. Reconsidering the blanket-data-retention-taboo, for human rights' sake? – European Law Blog. 1. 10.2018. Arvutivõrgus: http://europeanlawblog.eu/2018/10/01/reconsidering-the-blanket-data-retention-taboo-for-human-rights-sake/ (20.03.2019).
73. Schasmin, P. Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel. Magistritöö. Tallinn: Tartu Ülikool, 2016.
74. Sehver, K. H. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. Tallinn: Tartu Ülikool, 2017.
75. Selgitused põhiõiguste harta kohta. – ELT C 303, 14.12.2007.
76. Strasbourg Observers. "Bulk interception of communications in Sweden meets Convention standards": the latest addition to mass surveillance case law by the European Court of Human Rights. 9.07.2018. Arvutivõrgus: https://strasbourgobservers.com/2018/07/09/bulk-interception-of-communications-in-sweden-meets-convention-standards-the-latest-addition-to-mass-surveillance-case-law-by-the-european-court-of-human-rights/ (20.03.2019).
77. The Conceil d'État. Arvutivõrgus: http://english.conseil-etat.fr/ (18.04.2019).
78. The Tech Terms Computer Dictionary. SIM Card. Arvutivõrgus: https://techterms.com/definition/sim_card (19.04.2019).

79. Vabariigi Valitsuse tegevusprogramm 2015-2019. Arvutivõrgus: https://www.riigiteataja.ee/aktilisa/3030/6201/5006/231klisa.pdf (19.02.2019).
80. Ülevaade Eesti osalemisest Euroopa Liidu Kohtu ja EFTA kohtu menetlustes, Eesti vastu algatatud rikkumismenetlustest ja projekti „EU Pilot“ päringutest aastal 2018. Välisministeerium, juriidiline osakond, Euroopa Liidu õiguse büroo, 2019.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Christina Jõesaar,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses“, mille juhendaja on Jaan Ginter,

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

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

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

Tartus, 30.04.2019