TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Karistusõiguse osakond

Airiin Antson

ELEKTROONILISE SIDE ANDMETE SÄILITAMISE JA PÕHIÕIGUSTE TAGAMISE VAHEKORD KRIMINAALMENETLUSES

Magistritöö

Juhendaja: M.A. Rauno Kiris

Kaasjuhendaja: professor Jaan Ginter

Tallinn
2021

SISUKORD

SISSEJUHATUS

Krüptovaluuta järjest laiem levik ning *darkweb* on vaid mõned märksõnad, mis pakuvad kurjategijatele rohkelt võimalusi kuritegude toime panemiseks. Ülemaailmne digitaliseerimine on kaasa toonud olukorra, kus lisaks kuritegevusele on küberruumi üle läinud üha rohkem teenuseid ja järjest rohkem on inimeste andmeid talletunud nii suhtlusportaalides kui ka erinevate teenusepakkujate juures. Tehnoloogia areng on kiire ja sageli ettearvamatu. Praegu peamiselt küberkuritegevust iseloomustav on varsti reaalsus ka paljudes teistes kuritegevuse valdkondades. Nimelt saab tulevikus tehnoloogiast horisontaalne mõõde enamikes kuritegudes, kus piirid füüsilise ja tehnoloogia vahel kipuvad segunema.[1] Seejuures on oluline märkida, et elektroonilised tõendid, muu hulgas elektroonilise side andmed, ei ole juba praegu omased mitte ainult küberkuritegudele, vaid need mängivad olulist rolli ka näiteks isiku- ning varavastaste kuritegude menetlemisel. Väga suurel osal kuritegudest on puutumus digitaalse dimensiooniga.[2]

Küberruumis ja elektroonilise side teenuseid kasutades jäävad maha andmed, mille pinnalt saab teha olulisi järeldusi. Andmete säilitamine Ameerika Ühendriikides sattus globaalses mastaabis eriti teravalt pildile nn Snowdeni skandaali valguses.[3] Kuigi Edward Snowdeni skandaal oli peamiselt seotud Ameerika Ühendriikide jälitustegevuse paljastamisega, kerkisid E. Snowdeni kui endise NSA töötaja avalduste pinnalt esile ka NSA töövõtted. Mitmed endised NSA töötajad on öelnud, et metaandmete pinnalt on võimalik inimeste kohta teha paikapanevaid järeldusi ning piisavalt paljude metaandmete olemasolu korral ei ole andmesubjekti profiili koostamiseks sisuandmeid vajagi. Üks NSA töötaja täpsustas, et inimesi tapetakse metaandmetest saadud informatsiooni põhjal, tehes sihtmärgid kindlaks andmete järgi.[4] E. Snowdeni avaldatud info tõttu on enda andmete säilitamise põhimõtteid muu hulgas asunud muutma *Apple*, *Google* ja *Facebook*, kes on asunud suhtlust krüpteerima.[5]

[1] Europol. *Exploring Tomorrow's Organised Crime* 2015, lk 38. Arvutivõrgus kättesaadav: https://www.europol.europa.eu/publications-documents/exploring-tomorrow's-organised-crime, 26.03.2021.
[2] *National Institute of Justice – Digital Evidence and Forensics*. Arvutivõrgus kättesaadav: https://nij.ojp.gov/digital-evidence-and-forensics, 07.02.2021.
[3] Mazzetti, M., Schmidt, M. S. *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance – The New York Times*. 09.06.2013. Arvutivõrgus kättesaadav: https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html, 15.03.2021.
[4] Cole, D. „*We Kill People Based on Metadata*" – *The New Yorker* 10.05.2014. Arvutivõrgus kättesaadav: https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/, 15.03.2021.
[5] Taylor, J. *Australian government blames Snowden for data retention – ZDNet* 22.01.2015. Arvutivõrgus kättesaadav: https://www.zdnet.com/article/australian-government-blames-snowden-for-data-retention/, 15.03.2021.

Tänasel päeval pole väärtuslikem vara mitte nafta vaid andmed.[6] Seda väidet illustreerib muu hulgas andmete kogumise maht Ameerika Ühendriikides. Nimelt sai 2019. aastal Ameerika Ühendriikide Riiklik Julgeolekuagentuur (*National Security Agency*, edaspidi NSA) sideettevõtjatelt nagu AT&T ja Verizon kätte 534 miljonit kannet telefonikõnede ja sõnumite kohta. See arv on kolm korda suurem NSA poolt 2016. aastal kogutud kannetest.[7] Küberruumis ja elektroonilise side seansi jooksul tekkinud andmeid on võimalik käsitleda elektroonilise tõendina. Elektroonilistel tõenditel on kriminaalmenetlustes järjest suurem osakaal ning vajadus selliste tõendite järele pole enam piiratud pelgalt küberkuritegude menetlemisega. Elektrooniliste tõendite osakaal on järjest rohkem kasvamas ning sellele viitab ka asjaolu, et 2020. aasta seisuga omasid elektroonilised tõendid tähtsust 85% kõikides Euroopa Liidu liikmesriikide menetlustes.[8] Kuivõrd sideandmete kasutamise võimalus võib olulist rolli mängida kuritegude lahendamisel ja menetleja saab ligi pääseda ainult sellistele andmetele, mis on olemas, on vaja tagada teatava osa elektroonilise side andmete säilitamine.

Digitaliseerimise üks tagajärgi on üha rohkemate andmete lisandumine ning selle tõttu on üha suurem kohustus ka riigil enda kodanikke kaitsta ning tagada, et andmete säilitamise regulatsioon ei oleks ebaproportsionaalselt põhiõiguseid riivav. Seadusandlus peab olema piisav, et ühest küljest ei väljuks õiguskaitseorganite töö lubatud raamidest, ent samas tuleb kodanikke kaitsta ka erinevate keskkondade eest, kehtestades regulatsiooni selle kohta, milliseid klientide andmeid, mis tingimustel ja kui kaua saab talletada ning tagada keskkondade turvanõuded, et inimeste andmed oleks kaitstud. Kuna elektroonilised tõendid omavad puutumust pea kõikide kuriteoliikidega, on teravalt päevakorras küsimus, kui laiad piirid on menetlejal kriminaalmenetluse läbiviimiseks, pidades silmas, et kellegi õigusi ei oleks ebaproportsionaalselt riivatud.

Kuigi ühiskonnas on debatt selle üle, et riik tahab järjest suuremat ligipääsu telekommunikatsioonivõrgus olevatele andmetele ning krüpteeritud sõnumirakendustele, on Euroopa Kohtu lahendite valguses tõstatunud tasakaaluks teravad küsimused ka põhiõiguste kaitsmise kohta. Asjaolule, et Eesti kehtiv õiguslik regulatsioon ei pruugi olla elektroonilise side andmete säilitamise osas piisav, viitas 2016. aastal Euroopa Liidu Nõukogu, mis soovitas

[6] Bhagespur, K. *Data Is The New Oil – And That's A Good Thing – Forbes* 15.11.2019. Arvutivõrgus kättesaadav: https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=2e1fdec17304, 21.02.2021.
[7] Savage, C. *N.S.A Triples Collection of Data From U.S. Phone Companies – The New York Times* 04.05.2018. Arvutivõrgus kättesaadav: https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html, 03.02.2021.
[8] *SIRIUS EU Digital Evidence Situation Report, 2nd Annual Report* 2020, lk 5. Arvutivõrgus kättesaadav: https://www.europol.europa.eu/sites/default/files/documents/sirius_desr_2020.pdf, 15.12.2020.

Eestil andmete säilitamise regulatsioon üle vaadata, võttes arvesse Euroopa kohtu lahendeid.[9] Ka õiguskantsler Ülle Madise on enda 2016. aasta elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise seaduspärasuse analüüsis leidnud, et kehtiv sideandmete töötlemise regulatsioon on ebaühtlane ja lünklik ning nõuab terviklikult üle vaatamist.[10]

Eelneva valguses on magistritöö eesmärgiks välja selgitada, kas kehtiv elektroonilise side seadus on põhiseaduspärane ja kas ning kuidas võimaldab Euroopa Kohtu sidevaldkonna praktikast tulenev raamistik tulemuslikult läbi viia menetlusi, samas tagades puudutatud isikute põhiõigused. Juhul kui Euroopa Kohtu praktika sätestatud piirid seda ei võimalda, siis milline on proportsionaalne lahendus, et oleks tagatud ühelt poolt tõhus menetluste läbiviimine ja teisalt oleks siiski piisavalt tagatud puudutatud isikute põhiõiguste kaitse. Uurimise eesmärgiks on Euroopa Liidu sidevaldkonna kohtulahendites sätestatud põhimõtete põhjal teha järeldus, kas ja kuidas on võimalik valdkonda reguleerida selliselt, et oleks tagatud nii tõhus menetlus kui ka põhiõiguste proportsionaalne kaitse. Kui kehtiv regulatsioon ei taga piisavat tasakaalu õiguskaitseasutuste ja privaatsuse vahel, pakutakse töös välja võimalikud lähtekohad, mis võimaldaksid tagada tasakaalu nii efektiivse menetluse kui põhiõiguste kaitse vahel.

Uurimiseesmärke aitavad saavutada püstitatud uurimisküsimused, milleks on:

1) Millised on elektroonilise side andmete liigid?
2) Milliseid nendest liikidest tuleb Eesti sideettevõtjatel säilitada?
3) Milliseid põhiõiguseid riivatakse elektroonilise side andmete säilitamise ja kasutamisega?
4) Milliseid põhiõiguseid riivatakse elektroonilise side andmete säilitamata ja kasutamata jätmisega?
5) Millised on Euroopa Kohtu seisukohad andmete säilitamise ja nendele juurdepääsu andmise osas?
6) Kas kehtiv riigisisene regulatsioon andmete säilitamise osas on põhiseaduspärane ja kooskõlas Euroopa Kohtu lahendites väljendatud seisukohtadega?

[9] Euroopa Liidu Nõukogu, 12.01.2016. Aruanne Eesti kohta - vastastikuste hindamiste seitsmenda vooru hindamisaruanne „Küberkuritegevuse ennetamise ja sellega võitlemise Euroopa poliitika praktiline rakendamine ja toimimine". Arvutivõrgus kättesaadav: https://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/et/pdf, 06.01.2020

[10] Madise, Ü. Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus 22.04.2016, lk 1. Arvutivõrgus kättesaadav: https://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf, 13.01.2021.

Töös käsitletavad teemad on aktuaalsed mitme nüansi poolest. Euroopa Nõukogu tegi kaks kuud pärast 2005. aastal Londonis aset leidnud pommitamisi ettepaneku direktiivi 2006/24/EÜ loomiseks.[11] Eesti on riigisisesesse õigusesse selle Euroopa Liidu direktiivi sideandmete säilitamise kohta[12] (edaspidi direktiiv 2006/24/EÜ) üle võtnud 17.12.2007 jõustunud elektroonilise side seadusega[13] (edaspidi ESS). Euroopa Kohus on 08.04.2014 ühendatud kohtuasjades C-293/12 ja C-594/12[14] (edaspidi *Digital Rights Ireland*) tunnistanud andmete säilitamise direktiivi 2006/24/EÜ tagasiulatuvalt kehtetuks. Seitse aastat tagasi Euroopa Kohtu otsusega kehtetuks tunnistatud direktiivi üle võtvad sätted kehtivad Eestis tänaseni. Kehtiva elektroonilise side seaduse kohaselt peavad sideettevõtjad säilitama kõiki elektroonilise side seansiga seonduvaid andmeid (välja arvatud sisuandmeid) kõikide elektroonilise side teenuste kasutajate kohta. Selliseid andmeid tuleb säilitada ühe aasta jooksul alates nende tekkimise ajast. Sideettevõtjalt säilitatud andmete välja nõudmiseks annab kohtueelses kriminaalmenetluses loa prokuratuur ja väärteomenetluses ning kriminaalmenetluse kohtulikus osas kohus. Teatud juhtudel ei ole menetlejal sideandmete väljanõudmisel isegi prokuratuuri või kohtu luba vaja.[15] Euroopa Kohtu lahenditest tulenevate põhimõtete kohaselt ei ole selline laussäilitamine lubatud, samuti ei ole prokuratuur selline sõltumatu haldusasutus, kelle kontrollile säilitatud sideandmete töötlemine alluma peaks.[16]

Varasemalt on elektroonilise side andmete säilitamise ja privaatsusõiguse teemadel kirjutanud 2016. aastal Piret Schasmin[17] ja 2017. aastal Kätlin Helena Sehver[18]. 2019. aastal kaitses magistritöö Christina Jõesaar, kes analüüsis elektroonilise side andmete säilitamist ja kasutamist kriminaalmenetluses e-privaatsuse määruse ettepaneku, kohtupraktika ja elektroonilise side seaduse väljatöötamiskavatsuse valguses.[19] Pärast C. Jõesaare magistritööd on Euroopa Kohus teinud kolm uut lahendit, milles kohus on korranud nii varasemaid seisukohti kui ka toonud uusi järeldusi. Käesolev magistritöö panustab valdkonda sellega, et

[11] Zubik, M., Podkowik, J., Rybski, R. *European Constitutional Courts Towards Data Retention Laws*. – *Springer International Publishing*: 2021, lk 232.
[12] Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ.
[13] Elektroonilise side seadus – RT I 2004, 87, 593...RT I, 20.05.2020, 34.
[14] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12. *Digital Rights Ireland*.
[15] KrMS § 90^1 lõige 1 alusel tehtav päring.
[16] EKo 02.03.2021, C-746/18. *H. K. vs Prokuratuur*, p 59.
[17] Schasmin, P. Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel. Magistritöö. – Tallinn: Tartu Ülikool, 2016.
[18] Sehver, K. H. Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel. Magistritöö. – Tallinn: Tartu Ülikool, 2017.
[19] Jõesaar, C. Elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses. Magistritöö. – Tartu: Tartu Ülikool, 2019.

analüüsib muu hulgas kohtupraktika värskeid lahendeid ja viib läbi elektroonilise side andmete säilitamist puudutava regulatsiooni põhiseaduspärasuse kontrolli.

Uurimisküsimustele vastuste leidmiseks on magistritöö jaotatud kolme peatükki. Nendest esimene avab elektroonilise teabe liigid kriminaalmenetluse kontekstis, samuti annab ülevaate elektroonilise side andmete liikidest ja nende talletamisest. Ka keskendub esimene peatükk Eesti seadusandlusele, andes ülevaate sätetest, millest riigisiseses õiguses lähtutakse.

Teise peatüki eesmärk on anda ülevaade välisriikide praktikast. Selle eesmärgi saavutamiseks analüüsitakse esmalt Austraalia õigussüsteemi ja seejärel olukorda Euroopa Liidus. Kuivõrd selles peatükis antakse laiahaardelisem ülevaade inimõigusi väärtustavate arenenud riikide lähenemistest, siis selleks, et omandada laiem kontekst, alustatakse analüüsi kaugemast riigist nagu Austraalia ja seejärel liigutakse nende riikide poole, kellel Eestiga on eelduslikult sarnasem kultuuri- ja õigusruum.

Euroopa Liidu liikmesriikide praktika andmete säilitamise seisukohalt on killustunud. Seda seisukohta illustreerib teise peatüki esimene pool, rõhutades, et ka maailma mastaabis on riigid andmesäilitamisega seonduvates küsimustes kehtestanud väga erinevaid regulatsioone. Väljaspool Euroopa Liidu riike on võrdlusaluseks riigiks valitud Austraalia. Austraalia on valimis seetõttu, et selles riigis ollakse andmete säilitamise küsimustes võrreldes Euroopaga polariseerunud seisukohtadel. Kui Euroopa Kohus on leidnud, et liidu õigusega ei ole kooskõlas õigusnormid, mis lubavad andmete üldist ja vahet tegemata säilitamist, siis Austraalia on asunud vastupidisele seisukohale. Nimelt kehtib Austraalias 2015. aastast õigusakt, mille kohaselt peavad sideettevõtjad andmeid säilitama kaheaastase perioodi pikkuse aja vältel. Euroopas kehtinud direktiivi 2006/24/EÜ kohaselt oli Euroopa riikidel maksimaalse säilitamisperioodina võimalik kehtestada andmete säilitamine kaheks aastaks. Austraalia on lähtunud nimetatud maksimaalsest säilitamise perioodist. Kontrastina – Saksamaal, Sloveenias ja Austrias puudub kohustus õiguskaitseorganite jaoks andmeid säilitada.

Peatüki teine pool annab ülevaate andmete säilitamisega seonduvast olukorrast Euroopa tasemel pärast seda, kui Euroopa Kohus tegi lahendi *Digital Rights Ireland* ning võrdluseks on toodud Belgia regulatsioon tänasel päeval. Belgia ja Eesti on riigisisese regulatsiooni muutmise osas võtnud erinevad lähenemised. Kui Belgia asus riigisisest regulatsiooni muutma kohe pärast *Digital Rights Ireland* lahendit, siis Eesti ei ole senini riigisisest regulatsiooni muutnud selliselt, mis võtaks arvesse ka Euroopa Liidu õiguse seisukohti.

Kolmas peatükk annab esmalt ülevaate põhiõigustest ja -vabadustest, mida elektroonilise side andmete säilitamisega riivatakse. Seejuures tuleb silmas pidada, et elektroonilise side andmete säilitamisega riivatakse andmesubjekti õigusi, ent teisest küljest riivatakse andmete säilitamata jätmisega kasu saavate osapoolte ja ka riigi ning erinevate institutsioonide huvisid, sest neil lasub põhiseaduslik kohustus tagada oma rahva elu, tervise ja vara kaitse. Kui riigil puuduvad meetmed, kuidas enda põhiseaduses määratud ülesandeid täita, siis formaalselt on inimestel põhiseaduse[20] (edaspidi PS) § 13 ja § 16 sätestatud õigused, ent sisuliselt neid õigusi tagatud ei ole. Samuti keskendub see peatükk soovitustele riigisisese regulatsiooni muutmiseks.

Kehtetuks tunnistatud direktiivi 2006/24/EÜ asemel reguleerib sideandmete säilitamisega seonduvat e-privaatsuse direktiiv ehk Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ[21] (edaspidi direktiiv 2002/58/EÜ). Direktiivi 2006/24/EÜ peamine eesmärk oli tagada säilitatud sideandmete kättesaadavus raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks. Direktiivi 2002/58/EÜ artikli 5 lõike 1 kohaselt on andmete säilitamisega kaasnev riive õigustatud vaid juhul, kui see teenib eesmärki, milleks võib olla kuritegude uurimine ja avastamine, riigi julgeoleku, territooriumi ja avaliku julgeoleku kaitse tagamine, kuritegevusvastane võitlus ning elektrooniliste sidesüsteemide keelatud kasutuse vältimine. Eesti seadusandja on läinud nendest miinimumnõuetest kaugemale, sest ESS § 111^1 lõike 11 alusel on võimalik andmeid edastada ka tsiviil- ja halduskohtutele ning neid kasutada väärteomenetluses. Magistritöös leitakse vastus küsimusele, kas selline olukord on Euroopa Kohtu lahenditega kooskõlas.

Töö autor käsitleb töös läbivalt muu hulgas Euroopa Kohtu praktikat. Euroopa Kohus on teinud olulise tähtsusega lahendeid andmete säilitamise teemal kaheaastase intervalliga alates 2014. aastast. Kaheaastast intervalli lõhkus 2021. aasta lahend *H. K. vs Prokuratuur*, milles kohus lahendas Eesti Riigikohtu poolt küsitud eelotsuse[22] küsimusi.

Uurimisprobleemile lahenduse leidmisel kasutatakse võrdlev-analüütilist meetodit, mis väljendub kehtiva õiguse analüüsis ning teiste riikide õiguse võrdluses. Töö hüpoteesiks püstitab autor, et käesoleval hetkel kehtiv elektroonilise side seadus riivab

[20] Põhiseadus. – RT 1992, 26, 349...RT I, 15.05.2015, 2.
[21] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12.07.2002., milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv).
[22] RKKKm 1-16-6179.

ebaproportsionaalselt isikute põhiõigusi ja ei ole sellest tulenevalt põhiseaduspärane ega kooskõlas Euroopa Liidu õigusega.

Käesolevat tööd kõige enam iseloomustavad märksõnad on: elektroonilise side andmed, metaandmed, elektroonilise side andmete säilitamine, põhiõiguste riive.

1. ELEKTROONILISE TEABE LIIGID KRIMINAALMENETLUSE KONTEKSTIS JA ELEKTROONILISE SIDE ANDMETE LIIGID

1.1. Elektroonilise teabe liigid kriminaalmenetluse kontekstis

Maailmas, kus üha rohkematel inimestel on lisaks isiklikule mobiiltelefonile ka muid digitaalseid seadmeid, jäetakse endast maha üha rohkem digitaalseid jälgi, millest on väärteo- ja kriminaalmenetluses tihtipeale väga palju kasu.[23] Euroopa Kohus on lahendi *Digital Rights Ireland* punktis 43 sedastanud põhimõtet, mille kohaselt elektrooniliste sideteenuste kasutamisega seotud andmed on oluliseks ja väärtuslikuks vahendiks kuritegevuse ja eriti sellise raske kuriteo nagu organiseeritud kuritegevuse ennetamisel, uurimisel, avastamisel ja kohtus menetlemisel.

Mida enam inimesed kasutavad elektroonilise side vahendeid, seda rohkem tekib elektroonilise side andmeid, mida on võimalik süütegude menetlemisel kasutada. Tuginedes statistikale, siis aastal 2019 oli Eestis 1,28 miljonit internetikasutajat (see on 98% elanikkonnast) ning 71% Eesti elanikkonnast jättis endast internetti maha jälje mobiiltelefoni kaudu.[24]

Kuna üha enam inimesi omab ligipääsu tehnoloogilistele vahenditele, on sellest tulenevalt muutumas õigusrikkumiste toimepanemise vahendid ja ka õiguskaitseorganid kasutavad süütegude uurimisel uusi meetmeid ja strateegiaid andmete kogumisel ja nende edasisel töötlemisel. Asjaolule, et koos inimeste tegevusega on internetti kolinud ka kuritegevus, viitab statistika, mille kohaselt muu kuritegevus küll ajas väheneb, ent kuriteoliikidest on enim tõusutrendis küber- ehk arvutikuriteod nagu arvutikelmused ja arvutiandmete ning arvutisüsteemi kuriteod.[25]

Telekommunikeerimine telefoni ja interneti vahendusel on inimeste eludes üha kesksemal kohal. Telefoni ja internetti kasutades loovad inimesed suures mahus andmeid. Loodavate andmete seas ei ole ainult kommunikatsiooni sisu vaid ka andmed selle kohta, millal, kellega

[23] *Commission of the European Communities. Extended Impact Assessment: Annex to theproposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. SEC*(2005) 1131 21.09.2015. Arvutivõrgus kättesaadav: https://ec.europa.eu/transparency/regdoc/rep/2/2005/EN/2-2005-1131-EN-1-0.Pdf, 09.03.2021.

[24] Milos reklaam. Eestlaste internetikasutus 2019. Arvutivõrgus kättesaadav: https://milos.ee/eestlaste-internetikasutus-aastal-2019/, 12.02.2021.

[25] Kuritegevus Eestis 2020. Küberkuriteod. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevus2020/, 20.02.2021.

ja kui tihti inimesed omavahel kontaktis on ning millisest asukohast nad seda teevad. Informatsiooni talletamine sellisel kujul on lisaks õiguskaitseorganite huvile vajalik ka sideettevõtjatele enda teenuse pakkumiseks, selle eest arvete esitamiseks ning vajadusel hilisemates vaidlustes arvega seonduvate asjaolude tõendamiseks.

Arvestades, et üha rohkemate inimeste tegevus on kolinud digitaalsfääri, on kriminaalmenetluste kontekstis lisandunud sellised olulised terminid: digitaalsed tõendid, sideandmed, sisuandmed, metaandmed ning nende andmete säilitamine. Kuivõrd ükski Eesti seadus neid ei defineeri, on nendes mõistetes orienteerumiseks vaja teada nende sisu.

Asjaolule, et n.-ö. tavainimene kasutab neid mõisteid läbisegi, viitavad ühiskondliku debati käigus tõusetunud arutelud. Aruteludest ja arvamusartiklitest nähtub, et tihtipeale ei eristata, milliste sideandmete osas sideettevõtjatel säilitamiskohustus lasub. Sellest tulenevalt on kerge tekkima arusaam, et riigil on tegelikkusest laiemad õiguslikud hoovad andmetele ligi pääsemiseks[26]. Euroopa Kohtu otsus[27], mis puudutas Eesti eelotsusetaotlust[28], sai meedias laia järelkaja. Ka seda otsust puudutanud artiklid annavad aluse järeldada, et laiemal avalikkusel on mitmed olulised mõisted vahetusse läinud. Postimehes avaldatud artikkel pealkirjaga: „Eesti jälitamisseadused said Euroopa kohtult löögi“[29] on otsene faktiline ebatäpsus, sest Euroopa Kohtu lahend ei puuduta ühtegi nn jälitamisseadust. Nimelt ei ole alates 2013. aastast sideettevõtjale päringu tegemine enam käsitletav jälitustoiminguna.[30] Sideettevõtjale tehtava päringu alusel saadakse andmeid tagantjärgi juba aset leidnud sündmuste kohta ning seetõttu ei ole sideandmete säilitamine samastatav jälitustegevuse raames tehtavate toimingutega.

Elektroonilise side teenuse osutaja ehk sideettevõtja on ESS § 2 lõike 5 kohaselt isik, kes osutab lõppkasutajale või teisele üldkasutatava elektroonilise side teenuse osutajale üldkasutatavat elektroonilise side teenust. Eestis on suurimateks sideettevõtjateks Telia, Elisa ja Tele2. Sideettevõtjate säilitamiskohustus sideandmete osas ei hõlma valimatult kõike sideseansi jooksul tekkinud teavet. Nimelt saavad sideseansi jooksul tekkida sisuandmed[31] ja

[26] Lõugas, H. Kommentaar: Teie andmed salvestatakse! – Eesti Päevaleht 22.03.2011. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/51294003/kommentaar-teie-andmed-salvestatakse, 05.01.2021.
[27] EKo 02.03.2021, C-746/18. *H. K. vs Prokuratuur*.
[28] RKKKm 1-16-6179.
[29] Laks, L. Eesti jälitamisseadused said Euroopa kohtult löögi – Postimees 04.03.2021. Arvutivõrgus kättesaadav: https://leht.postimees.ee/7193284/euroopa-kohtu-otsus-voib-mojutada-eestis-tuhandeid-kriminaalmenetlusi, 04.03.2021.
[30] Täpsemalt on seda teemat käsitletud samas alapeatükis.
[31] Sisuandmed on digitaalses vormingus talletatud elektroonilise teabevahetuse sisu, näiteks e-kirjade ja tekstisõnumite sisu, fotod, videod, hääl, kujutised ja heli.

metaandmed[32] ning nendest kahest lasub sideettevõtjal üksnes viimases kategoorias olevate andmete säilitamise kohustus[33].

Esmalt avab töö autor digitaalse tõendi mõiste. Kriminaalmenetluse seadustiku[34] (edaspidi KrMS) § 63 lg 1 järgi on tõend kahtlustatava, süüdistatava, kannatanu, tunnistaja või asjatundja ütlus, ekspertiisiakt, eksperdi antud ütlus ekspertiisiakti selgitamisel, asitõend, uurimistoimingu, kohtuistungi ja jälitustoimingu protokoll või muu dokument ning foto või film või muu teabetalletus.

Kuigi KrMS § 63 lg 1 sätestab loetelu sellest, mis kvalifitseerub tõendina, puudub selles nimistus digitaalne tõend. Sellest hoolimata ei ole praktikas ette tulnud olukorda, kus kriminaalmenetluses tunnistatakse mõni digitaalne tõend lubamatuks sel põhjusel, et sel puuduvad KrMS § 63 lõikes 1 sätestatud tõendi tunnused.[35] Digitaalsete tõenditena saab käsitleda registrites sisalduvat teavet, pilte, interneti kasutamise ajalugu, sisuandmeid, e-kirju, IP-aadresse, elektroonilisi dokumente, digitaalseid video- ja audiofaile ning fotosid, arvutustabelite andmeid, andmebaase, küpsiseid, elektroonilist raamatupidamist, väljatrükke, GPSi abil saadud geograafilisi asukohaandmeid, pangatoimingute logisid jne.[36] Mainitud digitaalseid tõendeid saab KrMS § 63 lg 1 mõttes kvalifitseerida asitõendi, muu dokumendi või muu teabetalletusena. Seevastu KrMS § 90^1 alusel sideettevõtjale esitatud päringu ning protokollina vormistatud saadud andmete näol on tegemist KrMS § 63^1 lõikes 1 loetletud uurimistoimingu protokolliga.

Nii Eesti riigisiseses õiguses kui ka rahvusvahelisel tasandil puudub selge konsensus elektrooniliste tõendite definitsiooni osas. Sellegipoolest on erinevad asutused üritanud rahvusvahelisel tasandil definitsioonis kokku leppida. Näiteks on Euroopa Nõukogu defineerinud elektroonilisi tõendeid kui tõendeid, mis on saadud ükskõik millisest seadmest, mille funktsioneerimine sõltub tarkvarast. Tõendite alla kuuluvad ka selliste seadmete poolt loodud andmed. Nimetatud seadmed peavad töötama tarkvara kasutades. Elektroonilisteks tõenditeks võivad ka olla sellised andmed, mida on hoiustatud või edastatud arvutisüsteemi või

[32] Metaandmetega saab tuvastada konkreetse sideseansiga seotud asjaolusid.
[33] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine), lk 2. Arvutivõrgus kättesaadav: http://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83?activity=1#fVKzRoTp, 09.12.2020.
[34] Kriminaalmenetluse seadustik. – RT I 2003, 27, 166...RT I, 29.12.2020, 10.
[35] Tehver, J. Digitaalsete tõendite kasutamise võimaldamine, 2016. Lk 2. Arvutivõrgus kättesaadav: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf, 24.01.2021.
[36] Euroopa Liidu Nõukogu. Vastastikuste hindamiste seitsmes voor – küberkuritegevuse ennetamise ja sellega võitlemise Euroopa poliitika praktiline rakendamine ja toimimine 09.06.2017. Arvutivõrgus kättesaadav: https://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/et/pdf, 25.01.2021.

-võrgu kaudu.[37] Teise definitsiooni kohaselt hõlmavad digitaalsed tõendid ükskõik millist teavet, mis on loodud, säilitatud või edastatud elektrooniliste seadmete kasutamise teel. Selline teave võimaldab tuvastada õigusrikkumise olemasolu või selle puudumist, samuti tuvastada rikkumise toime pannud isiku ning muid kriminaalmenetluse lahendamise seisukohast vajalikke asjaolusid.[38]

Andmeid on võimalik talletada elektroonilistel seadmetel (arvutid, nutitelefonid, tahvelarvutid, telefonid, printerid, *smart*-TV-d ning muud seadmed, millel on digitaalne mälumaht) ja välistel salvestusseadmetel (välised kõvakettad ja mälupulgad), võrgukomponentidel ja seadmetel (ruuterid), serverites ja pilves.[39] Nimetatud seadmetel võivad olla jäädvustunud nii sisuandmed kui metaandmed. Kriminaalmenetluses on menetlejal mõlemasse kategooriasse kuuluvatele andmetele võimalik teatavatel tingimustel ligi pääseda.

Sisuandmeteks on otseselt suhtluse või sõnumite sisu puudutav: videod, pildid, e-mailide ning (hääl)sõnumite sisu ja failid.[40] Samuti ka sotsiaalmeedia kasutajakontode sisu puudutavad andmed.[41] Menetlejal on võimalik sisuandmeid koguda nii läbiotsimise, jälitustegevuse kui ka vaatluse kaudu.

KrMS § 91 kohaselt on läbiotsimise eesmärk leida hoonest, ruumist, sõidukist või piirdega alalt asitõendina kasutatav või konfiskeeritav objekt, kriminaalasja lahendamiseks vajalik dokument, asi või isik või kuriteoga tekitatud kahju hüvitamiseks või konfiskeerimiseks arestitav vara või laip või tabada tagaotsitav. Kui läbiotsimise käigus leitakse arvuti, on selles olevatest süsteemidest lubatud kopeerida andmeid, milleks võivad olla näiteks e-mailide sisu, kartmata sõnumisaladuse riivet.[42]

KrMS §-s 126^3 defineeritud jälitustoimingu tegemine on relevantne olukorras, kus tõusetub vajadus varjatult jälgida isikut, asja või paikkonda, koguda varjatult võrdlusmaterjali ja teha esmauuringuid, teostada varjatult asja läbivaatust ning asendada selle varjatult, vaadata varjatult läbi postisaadetist, vaadata või kuulata salaja pealt teavet, kasutada politseiagenti, matkida kuritegu või varjatult siseneda hoonesse ruumi, sõidukisse, piirdega alale või

[37] *Council of Europe. Electronic Evidence in Civil and Administrative Proceedings* 2019, lk 6. Arvutivõrgus kättesaadav: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5, 08.01.2021.
[38] Euroopa Liidu Nõukogu. Vastastikuste hindamiste seitsmes voor.
[39] *UNODC E4J University Module Series: Cybercrime, Digital Evidence*. Arvutivõrgus kättesaadav: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html, 07.01.2021.
[40] *SIRIUS EU Digital Evidence Situation Report,* lk 13.
[41] *UNODC E4J University Module Series: Cybercrime, Digital Evidence*.
[42] RKKKo 3-1-1-93-15, p 100.

arvutisüsteemi. Jälitustegevust viiakse läbi näiteks juhul, kui on vajalik jälgida reaalajas toimuvat sõnumivahetust. Seda on võimalik teha, sisenedes varjatult arvutisüsteemi. ESS sisaldab endas sätet, mis kohustab sideettevõtjat võimaldama juurdepääsu jälitustoimingute teostamiseks. Nimelt sätestab ESS § 113 lõige 1, et sideettevõtjal lasub kohustus võimaldada jälitus- või julgeolekuasutusele juurdepääs sidevõrgule vastavalt jälitustoimingu teostamiseks või sõnumi saladuse õiguse piiramiseks.

KrMS § 83 lg 1 järgi on vaatluse eesmärgiks koguda kriminaalasja lahendamiseks vajalikke andmeid, avastada kuriteojäljed ja võtta asitõenditena kasutatavad objektid ära. Vajadus vaatluse järele võib tõusetuda näiteks olukorras, kus on vaja arvuti vaatluse raames kindlaks teha, kas ja millised vajalikud tõendid (nt e-kirjad) on olemas.

Metaandmeid seevastu kogutakse päringu esitamisega sideettevõtjale KrMS § 90^1 lg 1 alusel. KrMS § 90^1 alusel tehtavate päringute tegemisel on oluline eristada, et lõigete 1 ja 2 alusel tehtavad päringud reguleerivad erinevaid andmete liike.

KrMS § 90^1 lõike 1 kohaselt võib menetleja teha päringu elektroonilise side ettevõtjale üldkasutatava elektroonilise side võrgus kasutatavate identifitseerimistunnustega seotud lõppkasutaja tuvastamiseks vajalike andmete kohta, välja arvatud sõnumi edastamise faktiga seotud andmed. KrMS § 90^1 lg 1 alusel tehtav päring on nn omanikupäring. See tähendab, et sideettevõtjatelt on võimalik päringuga saada lõppkasutaja tuvastamiseks vajalikke andmeid. Andmed identifitseerimistunnuste kohta võivad olla näiteks IMEI, IMSI, SIM, IP-aadress ja kasutajatunnus (nt kasutajanimi, meilikonto). Selle lõike järgi tehtava päringuga saadavad andmed on mõningatel juhtudel kättesaadavad ka ilma menetlustoiminguta. Näiteks salvestavad mõned veebilehed nende külastamisel kasutatava IP-aadressi.[43] Samas tuleb tähele panna, et ainuüksi IP-aadressist ei ole kasu. KrMS § 90^1 lõike 1 alusel tehtava päringuga on võimalik saada andmeid lõppkasutaja kohta ning sümbioosis tuvastada IP-aadressi kasutanud isik.

Ajal, mil olid kasutusel telefoniraamatud, oli võimalik nendest saada informatsiooni telefoninumbri omaniku kohta. Lisaks telefoninumbritele avaldati telefoniraamatus ka isikute aadresse. Seejuures on tähtis märkida, et telefoniraamatus avaldatud numbrite ja aadresside puhul on tegemist oluliselt väiksema õiguste riivega, kui seda on sideettevõtjalt andmete kogumine. Selleks, et isiku kohta telefoniraamatus tema telefoninumber ja aadress avaldati, pidi

[43] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 175 SE, lk 4. Arvutivõrgus kättesaadav: https://www.riigikogu.ee/download/2c393ed9-49bc-4438-9496-df52ecdf3560, 15.12.2020.

isik sellega nõus olema ning isikud said igal hetkel valida, et järgmises telefoniraamatus enam nende andmeid ei avaldata. Seevastu KrMS § 90^1 lõike 1 alusel tehtava päringuga saadakse andmeid, mida isikud ei ole ise avalikkusele teatavaks teinud.

KrMS § 90^1 lõike 1 alusel saadavate andmete puhul on tähtis silmas pidada, et need andmed üksinda ei pruugi anda olulist infot. Saades teada telefonumbri omaniku, ei tähenda, et see sama inimene pani kuriteo toime; samuti võivad ühelt IP-aadressilt külastada veebilehti erinevad inimesed. Seetõttu on see päring tihtipeale algpunktiks edasiste tõendite kogumisel.[44]

KrMS § 90^1 lõike 2 kohaselt võib prokuratuuri loal kohtueelses menetluses või kohtu loal kohtumenetluses teha sideettevõtjale päringu ESS § 111^1 lõigetes 2 ja 3 loetletud andmete kohta, mida ei ole nimetatud KrMS § 90^1 lõikes 1. Päringu tegemise loas tuleb kuupäevalise täpsusega märkida ajavahemik, mille kohta andmete nõudmine lubatud on. Enamik KrMS § 90^1 lg 2 alusel tehtavatest päringutest on nn kõneeristuse päringud, mis muu hulgas võimaldavad saada informatsiooni isiku suhtlusringi kohta. Selle päringuga saadakse andmeid mobiiltelefonilt tehtud või vastuvõetud kõnede kohta, kõne alguse ja lõpu kuupäeva ning kellaaja; kärjetunnuse kõne alustamise ajal; andmeid tugijaama geograafilise asukoha kohta; anonüümse ettemakstud kõnekaardi korral teenuse esmase aktiveerimise kuupäeva, kellaaja ning kärjetunnuse; internetiseansi alguse ja lõpu kuupäeva ja kellaaja; elektronposti või internetitelefoni teenuse kasutamise alguse ja lõpu kuupäeva ning kellaaja kohta. Need andmed ei ava sõnumi sisu, ent seonduvad sõnumi edastamise faktiga.[45] Selle lõike alusel ei tehta ainult kõneeristuse päringuid, vaid on võimalik saada andmeid näiteks ka selle kohta, kus sidevahend elektroonilise side toimumise ajal asus. Kõneeristuse tähtsust on rõhutatud Veronika Dari kaasuses[46], kus aset leidnud mõrv lahendati just kõneeristuse andmete tõttu. Ka Juri Ustimenko pommiplahvatuse kaasus lahendati tänu kõneeristusele ja digianalüütikale.[47]

Puutuvalt KrMS § 90^1 lõigete 1 ja 2 erinevustesse, siis lõike 1 alusel tehtav omanikupäring toimub menetleja päringuga, ent lõike 2 alusel tehtava kõneeristuse jaoks on kohtueelses menetluses vajalik prokuratuuri luba. Praktikas kasutatakse lõigete 1 ja 2 alusel saadavat teavet näiteks jälitusloa saamiseks, et tõendada kellega inimene suhtleb, kus kahtlustatav viibis kuriteo toimepanemise hetkel, kes on hakanud varastatud telefoni kasutama jne.

---

[44] *Ibid.*, lk 3.
[45] *Ibid*., lk 4.
[46] TlnRnKo 1-06-2292.
[47] Lamp, D., Anvelt, A. Eesti roimad. Koolitüdruk Veronika Dari tapmise tõe paljastas üks pisiasi. – Elu24 15.04.2021. Arvutivõrgus kättesaadav: https://www.elu24.ee/7224532/koolitudruk-veronika-dari-morva-poleks-ehk-avastatud-kui-poleks-olnud-uht-pisiasja, 16.04.2021.

Nii KrMS § 90^1 lg 3 kui ka väärteomenetluse seadustiku[48] (edaspidi VTMS) § 31^2 lg 3 sätestavad *ultima ratio* põhimõtte. Selle kohaselt võib päringu sideettevõtjale teha üksnes juhul, kui see on kriminaalmenetluses vältimatult vajalik kriminaalmenetluse eesmärgi ja väärteomenetluses väärteomenetluse eesmärgi saavutamiseks. Kuigi päring sideettevõtjale ei ole alates 01.01.2013 enam käsitlev jälitustoiminguna, tähendab KrMS § 90^1 lõikes 3 sätestatud *ultima ratio* põhimõte, et päringut sideettevõtjale ei saa teha n.-ö. igaks juhuks või et seda võimalust peaks tingimata iga kuriteo menetlemisel kasutama.[49]

ESS § 111^1 lg 11 sätestab asutused, kellele sama paragrahvi lõigetes 2 ja 3 nimetatud andmeid edastatakse. ESS § 111^1 lg 11 kohaselt edastatakse andmeid järgnevatele asutustele: kriminaalmenetluse seadustiku kohaselt uurimisasutusele, jälitusasutusele, prokuratuurile ja kohtule; julgeolekuasutusele; väärteomenetluse seadustiku kohaselt Andmekaitse Inspektsioonile, Finantsinspektsioonile, Tarbijakaitse ja Tehnilise Järelevalve Ametile, Keskkonnaametile, Politsei- ja Piirivalveametile, Kaitsepolitseiametile ning Maksu- ja Tolliametile; väärtpaberituru seaduse kohaselt Finantsinspektsioonile; tsiviilkohtumenetluse seadustiku kohaselt kohtule; jälitusasutusele kaitseväe korralduse seaduses, maksukorralduse seaduses, politsei ja piirivalve seaduses, relvaseaduses, strateegilise kauba seaduses, tolliseaduses, tunnistajakaitse seaduses, turvaseaduses, vangistusseaduses ja välismaalaste seaduses sätestatud juhtudel.

Küsimuse võib tõstatada asjaolu, et ESS § 111^1 lõige 11 punkti 5 alusel edastatakse sama paragrahvi lõigetes 2 ja 3 nimetatud andmeid ka tsiviilkohtumenetluse seadustiku kohaselt kohtule. Vastuolu seisneb selles, et sideettevõtjad peaks elektroonilise side andmeid säilitama raskete kuritegude ennetamise, uurimise, avastamise ja kohtus menetlemise eesmärgil ning neid sellest tulenevalt edastama ka üksnes õiguskaitseorganitele. Sellest hoolimata on loetellu lisatud andmete edastamine tsiviilkohtule, samuti toimub andmete edastamine menetlejale väärteomenetluste raames.

Direktiivi 2006/24/EÜ preambulas on viidatud Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni[50] (edaspidi EIÕK) artiklile 8, mille kohaselt on igaühel õigus oma eraelu austamisele. Avalik võim võib selle õiguse teostamisse sekkuda üksnes õigusliku aluse esinemisel ja juhul, kui see on vajalik muu hulgas riikliku julgeoleku või üldise turvalisuse,

[48] Väärteomenetluse seadustik. – RT I 2002, 50, 313...RT I, 10.12.2020, 37.
[49] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 175 SE, lk 3.
[50] Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Euroopa Nõukogu, 4 november 1950. – RT II 2010, 14, 54.

korrarikkumise või kuriteo takistamise huvides või teiste isikute õiguste ja vabaduste kaitseks.[51] Selle loeteluga klapib olukord, kus tsiviilkohtumenetluses nõutakse kohtult päringu tegemist tuvastamaks IP-aadressi taga peituv inimene, kes on internetti jätnud laimavaid kommentaare.[52] Kuigi kommentaariumite IP-aadressidest on kriminaalmenetlustes tavaliselt vähe kasu, on praktikast teada, et IP-aadresside väljanõudmine kommentaariumites sõna võtnud inimeste tuvastamiseks võib esineda ka kriminaalmenetluse raames.[53]

Kuivõrd Euroopa Kohus tunnistas enda lahendiga *Digital Rights Ireland* direktiivi 2006/24/EÜ tagasiulatuvalt kehtetuks selle jõustumise hetkest saadik, tähendab see seda, et nimetatud direktiiv ei ole praeguse õiguse kohaselt mitte kunagi kehtinud. Eesti seadusesse võeti nimetatud direktiiv üle elektroonilise side seadusega, ent pärast direktiivi kehtetuks tunnistamist ei ole riigisiseseid sätteid Euroopa Liidu õigusega kooskõlla viidud. ESS vastuvõtmise ajal kehtisid direktiivis sätestatud põhjendused, ent praegune pilt andmete säilitamise õigusmaastikul on kardinaalselt teine võrreldes direktiivi ülevõtmise ajaga. Eeltoodust tulenevalt ei ole Euroopa Kohtu praktikaga kooskõlas olukord, kus säilitatud andmeid on võimalik edastada nii tsiviilkohtule kui väärtegude menetlemiseks menetlejale.

Illustreerimaks, kui palju laiem on Eestis sideandmete kasutamine võrreldes Euroopa Kohtu seisukohtadega, toob töö autor välja, milliseid andmeid on võimalik päringuga saada sideettevõtjalt VTMS alusel. VTMS § 31^2 lõige 1 on sisuliselt identne KrMS § 90^1 lg 1 alusel tehtava päringuga ehk nn omanikupäringuga. VTMS § 31^2 lõike 2 alusel tehtavat päringut on võimalik teha üksnes üksikpäringuna konkreetse kõne, lühisõnumi, e-kirja või muu sõnumi kohta.[54] Seejuures on lõikes 2 loetletud päringu tegemise jaoks vaja kohtu luba. See on erinevus KrMS § 90^1 lõike 2 alusel tehtava päringuga, mille tarbeks on kohtueelses menetluses nõutav prokuratuurilt loa saamine – kohtult loa saamine on tugevam privaatsuse kaitse meede kui prokuratuuri luba. Õiguskantsleri kantselei õiguskorra kaitse osakonna juhataja Külli Taro on kitsaskohana välja toonud asjaolu, et kohtunikud tõlgendavad üksikpäringu tegemist erinevalt – mõni kohtunik on loa kõneeristuseks väljastanud mõne tunni kohta, kui teine kohtunik on

[51] Direktiiv 2006/24/EÜ, põhjenduspunkt 9.
[52] Mihkels, D. Näitlejanna ristiretk. Anonüümne mõnitamine läks Perekooli „kägudele“ kalliks maksma. – Eesti Päevaleht 01.10.2018. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/83856517/naitlejanna-ristiretk-anonuumne-monitamine-laks-perekooli-kagudele-kalliks-maksma, 02.03.2021.
[53] Berendson, R. Pavlihhini uurimine ja IP-aadresside teabenõue olid eri asjad – Postimees 24.01.2014. Arvutivõrgus kättesaadav: https://www.postimees.ee/2673656/pavlihhini-uurimine-ja-ip-aadresside-teabenoue-olid-eri-asjad, 07.02.2021.
[54] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 175 SE, lk 24.

analoogsete asjaolude pinnalt väljastanud loa kõneeristuse saamiseks mitme kuu pikkuse perioodi ulatuses.[55]

Kuivõrd kõikidel kohtuvälistel menetlejatel ei peaks olema võimalust kõneeristuse jaoks päringut teha, loetleb VTMS § 31^2 lg 1 need asutused, kellel selline pädevus on. Nendeks on Andmekaitse Inspektsioon, Finantsinspektsioon, Kaitsepolitseiamet, Keskkonnaamet, Maksu- ja Tolliamet, Rahapesu Andmebüroo ning Politsei- ja Piirivalveamet.

KrMS § 126^1 lg 1 kohaselt on jälitustoiming isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise sisu ja fakti andmesubjekti eest. Oma olemuselt mahuks selle definitsiooni alla ka sideettevõtjalt andmete nõudmine, sest andmete küsimise fakti soovitakse andmesubjekti eest varjata. Inimene saab tema osas tehtud päringust teada vaid siis, kui päringust saadav info vormistatakse tõendina ning see lisatakse kriminaalasja materjalide juurde. Selleks, et sideettevõtjalt saadud andmed oleks kriminaalmenetluses tõendina kasutatavad, tuleb saadud andmete kohta koostada sideettevõtjalt saadud andmete protokoll.

KrMS § 126^3 loetleb toimingud, mida käsitletakse jälitustoiminguna, ent selles nimistus puudub andmete nõudmine sideettevõtjalt. Seda sel põhjusel, et alates 01.01.2013 ei ole sideettevõtjale tehtav päring enam käsitletav jälitustoiminguna, vaid menetlustoiminguna.[56] Üks põhjendusi, miks sideettevõtjale päringu tegemine ei ole enam käsitletav jälitustoiminguna, on asjaolu, et menetlejal on õigus kriminaalmenetluse käigus teha andmesubjekti kohta ka mitmeid muid päringuid, mis annavad aimu isiku igapäevastest tegevustest ning sellised päringud ei ole samuti käsitletavad jälitustoiminguna.[57] Sellisteks päringuteks võivad näiteks olla päring kinnistusraamatusse, Maksu- ja Tolliametile, päring pangale saamaks konto väljavõtteid jne.

Sideettevõtjale päringu saatmine jälitustoimingust menetlustoiminguks muutmise kasuks räägib ka asjaolu, et andmete saamist näiteks tugijaama geograafilise asukoha kohta või sõnumi edastamise kellaaja ja kuupäeva infot ei ole võimalik samastada sellise jälitustoiminguga nagu isiku varjatud jälgimine. Seda seetõttu, et sideettevõtjale tehtava päringu vastusega saab vaid tagantjärele teada, millises mobiilimasti piirkonnas konkreetne mobiiltelefon on viibinud ning see ei ole võrreldav isiku reaalajas jälgimisega. Sellist infot on võimalik isiku asukoha kohta saada ka näiteks tänaval, kauplustes, bensiinijaamade või sularahaautomaatide paigutatud

[55] Taro, K. Külli Taro: jälitamisest ja jälgimisest – ERR 04.10.2018. Arvutivõrgus kättesaadav: https://www.err.ee/866452/kulli-taro-jalitamisest-ja-jalgimisest, 15.03.2021.
[56] *Ibid.*, lk 3.
[57] *Ibid.*, lk 3.

kaamerate kaudu. Kaamerapildist saadavad andmed on oluliselt nüansirohkemad kui pelk ESS-s nimetatud tugijaama asukoht.[58]

1.2. Elektroonilise side andmete liigid

1.2.1. Abonendi- ehk kliendiandmed (ingl *subscriber information*)

Elektroonilise side andmed jagunevad sisuandmeteks (*content data*) ja muudeks kui sisuandmeteks (*non-content data*) ehk metaandmeteks. Analoogia korras saab neid andmeid võrrelda ümbrikus saadetud kirjaga: kui kirja ümbrik on metaandmed, siis ümbriku sees olev kiri on sisuandmed. Nn ümbrikul olevate andmete tähtsust illustreerib ka asjaolu, et Ameerika Ühendriikides pildistatakse kõikide posti teel saadetud ümbrikel olevaid andmeid. Aastal 2013 jäädvustati selliselt fotona 160 miljardi kirjasaadetise välised küljed.[59] Ameerika Ühendriikides alluvad postisaadetised seega samasugusele kontrollile nagu emailid ja kõned, mille puhul samuti metaandmeid säilitatakse. Kuigi postisaadetised ei genereeri elektroonilise side andmeid, ilmestab antud näide asjaolu, et metaandmed mängivad tähtsat rolli. Elektroonilise side metaandmete säilitamise tähtsust on tunnistanud ka Riigikohus, sedastades, et elektroonilise side andmete kogumine sideettevõtjalt on efektiivne meede saamaks objektiivseid tõendeid isikute suhtlemise fakti ja viibimiskoha kohta.[60]

Puutuvalt elektrooniliste sideandmete säilitamise reeglitesse, siis ESS reguleerib üksnes sideseansiga seotud metaandmeid ning mitte sõnumi sisu.[61] See tähendab, et ESS alusel peavad sideettevõtjad säilitama abonendi- ehk kliendiandmeid (*subscriber information*), liiklusandmeid (*traffic data*), juurdepääsuandmeid (*access data*) ja asukohaandmeid (*location data*). Mainitud neli andmetüüpi paigutavad muude kui sisuandmete kategooriasse.

Sideandmete säilitamise kohustus tähendab näiteks seda, et sideettevõtjad peavad telefonikõnede puhul säilitama omavahel helistavate inimeste telefoninumbreid ning kõne kestust, mitte aga seda, mida telefonikõne jooksul räägiti. Emailide puhul säilitatakse emailiaadresse ning andmeid selle kohta, millal emaile on saadetud. Ei säilitata emailide sisu ega emailide pealkirjasid. Menetlejatele on olulise tähtsusega ka IP-aadressid, sest need võimaldavad kokku viia seadet seda kasutanud inimese nimega. Näiteks kui politsei avastab

[58] *Ibid.,* lk 5.
[59] Nixon, R. *U.S. Postal Service Logging All Mail for Law Enforcement*. – *The New York Times* 03.07.2013. Arvutivõrgus kättesaadav: https://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html, 18.02.2021.
[60] RKKKo 3-1-1-51-14, p 22.
[61] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine), lk 2.

serveri, milles on lapspornot sisaldavad failid, on võimalik näha, millistelt IP-aadressidelt nimetatud serverit on külastatud. Sellisel juhul saab sideettevõtjalt nõuda andmeid serverit kasutanud IP-aadresside kohta, et tuvastada isik, kes kasutas seda konkreetset IP-aadressi sel hetkel, kui lapspornot sisaldanud serverile ligi pääseti.

Kuivõrd ESS ei jaota säilitatavaid andmeid mitte eespool nimetatud liikide põhiselt, vaid andmed on kategoriseeritud lähtuvalt telefoni- ja mobiiltelefoniteenuse ning Interneti-teenuse põhiste andmeliikide järgi, võib n.-ö. tavakasutajale olla keeruline hoomata, milliste andmete säilitamise kohustus sideettevõtjal lasub.

Kui võrrelda elektroonilise side andmete liikide väljanõudmise sagedust, siis kriminaalmenetlustes Euroopa mastaabis tõusetub enim vajadus abonendiandmete järele.[62] Abonent on üldkasutatavat elektroonilise side teenust kasutav isik, kellel on üldkasutatava elektroonilise side teenuse kasutamiseks leping sideettevõtjaga. Elektroonilise side seaduses kasutatakse abonendi asemel mõistet klient.[63] Abonendiandmetena on käsitletavad andmed, mille alusel on võimalik tuvastada kasutajat. Sellisteks andmeteks on näiteks nimi, sünniaeg, elukoha aadress, telefoninumber või e-mailiaadress ja arveldusandmed (nt arveldusarve number ja arve edastamise aadress).[64]

Kuigi elektroonilise side seadus reguleerib Eesti sideettevõtjate elektroonilise side andmete säilitamise kohustust, on rahvusvahelise koostöö kaudu võimalik andmeid küsida ka välismaistelt teenusepakkujatelt. Valdavale osale Euroopa Liidu riikidest on võimalik esitada Euroopa uurimismäärus ning muudele riikidele õigusabitaotlus. Õigusabi palve saamise järgselt saab õigusabi palve saanud riik esitada päringu enda riigis olevale sideettevõtjale. Selliselt on võimalik näiteks andmeid küsida internetipõhiseid teenuseid pakkuvalt *over-the-top* kiirsõnumiteenusepakkujalt *Viber*. Kuna *Viberi* peakontor on registreeritud Luksemburgis[65], on võimalik Eestis oleval menetlejal saata Iirimaale KrMS §-s 489[37] sätestatud Euroopa uurimismäärus.

[62] *SIRIUS EU Digital Evidence Situation Report,* lk 13.
[63] Elektroonilise side seadus, § 2 p 15.
[64] *European Commission. Frequently Asked Questions: New EU rules to obtain electronic evidence* 17.04.2018. Arvutivõrgus kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345, 06.01.2021.
[65] *Viber DMCA Policy*. Arvutivõrgus kättesaadav: https://www.viber.com/en/terms/dmca/, 21.04.2021.

2019. aastal oli Euroopa Liidu liikmesriikide kriminaalmenetlustes nõutud elektroonilise side andmete liikide osakaal järgnev: 52,9% moodustasid abonendiandmed, 32,4% moodustasid liiklusandmed (sh ka asukoha-, tehingu- ja juurdepääsuandmed) ning 14,7% sisuandmed.[66]

1.2.2. Liiklusandmed (ingl *traffic data*)

Arvutikuritegevusvastase konventsiooni[67] artikli 1 p d) kohaselt on liiklusandmed arvutisidesüsteemi ühe osana toimiva süsteemi andmed, mis käsitlevad edastatud teabe päritolu; teabe edastamise eesmärki, marsruuti ja kuupäeva; samuti teabe mahtu ja teabe edastamise kestust ning asjaomase teenuse liiki.

Direktiivi 2002/58/EÜ kohaselt on liiklusandmed üldmõiste, mis hõlmab ka asukoha-, juurdepääsu- ja tehinguandmeid.[68] Nimelt sätestab direktiivi seletuspunkt 15 järgmist: „Liiklusandmed võivad sisaldada side edastamiseks tehtud kõnealuse teabe transleeringuid võrgus, mille kaudu side edastatakse. Liiklusandmed võivad muu hulgas koosneda andmetest, mis viitavad side marsruutimisele, kestusele, ajale või mahule, kasutatud protokollile, saatja või vastuvõtja lõppseadme asukohale, võrgule, milles side algab või kus ta lõpeb, ühenduse algusele, lõpule ja kestusele. Lisaks sellele võivad need andmed sisaldada ka vormingut, milles side võrgus edasi antakse."

Liiklusandmetena käsitletakse üldjuhul andmeid, mida töödeldakse side edastamiseks elektroonilises sidevõrgus või sellise edastamisega seotud arveldamiseks.[69] Liiklusandmete alla kuuluvad näiteks ühenduste logid ja sõnumite arv. Tehes telefonikõne, säilitab sideettevõtja selliseid liiklusandmeid nagu kõne tegemise aeg, kuupäev ja kõne kestus – need andmed on sideettevõtjale olulised ka arve esitamise eesmärgil.

1.2.3. Asukohaandmed (ingl *location data*)

Sideandmete liikide puhul on tähtis meeles pidada, et Euroopa Kohus käsitleb kohtulahendites sideandmetena üksnes liiklus- ja asukohaandmeid.[70] Liiklus- ja asukohaandmed üldmõistena võimaldavad tuvastada, millal toimus sideseanss, kui pikk see oli ja kus helistaja või vastuvõtja liikus.[71] Asukohaandmetena käsitletakse elektroonilises sidevõrgus või elektrooniliste

[66] *SIRIUS EU Digital Evidence Situation Report,* lk 13.
[67] *Council of Europe. Convention on Cybercrime – European Treaty Series no.* 185.
[68] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, seletuspunkt 15.
[69] EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-203/15. *Tele2 Sverige*.
[70] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12. *Digital Rights Ireland* , p 16. EKo *Tele2 Sverige*, p 75. EKo 06.10.2020, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18. *La Quadrature du Ne*t, p 96.
[71] Lõhmus, U. Uno Lõhmus: kaua tuleb oodata õiguse kooskõlla viimist põhiõiguste nõuetega? – ERR 04.03.2021. Arvutivõrgus kättesaadav: https://www.err.ee/1608129820/uno-lohmus-kaua-tuleb-oodata-oiguse-kooskolla-viimist-pohioiguste-nouetega, 04.03.2021.

sideteenuste poolt töödeldavaid andmeid, mis näitavad üldkasutatavate elektrooniliste sideteenuste kasutaja lõppseadme geograafilist asukohta.[72]

Eelnevalt on magistritöös selgitatud, et elektroonilise side seansi jooksul saavad tekkida nii sisu- kui ka metaandmed. Privaatsust ja elektroonilist sidet käsitleva määruse ettepanek[73] (edaspidi e-privaatsuse määruse ettepanek) rõhutab lahendis liidetud kohtuasjades C-203/15 ja C-698/15 (edaspidi *Tele2 Sverige*) väljendatud seisukohta metaandmete konfidentsiaalsusastme kohta. Esmalt markeeritakse, et elektroonilise side seansist tekkinud sisuandmed võivad füüsiliste isikute kohta anda väga tundlikku teavet, muu hulgas isiklikke kogemusi, emotsioone, tervislikku seisundit, seksuaalset sättumust ja poliitilisi vaateid, mille avaldamine võib andmesubjektile põhjustada isiklikku, sotsiaalset ja majanduslikku kahju või häbitunnet. Seejärel korratakse üle lahendist *Tele2 Sverige* tuttav seisukoht, mille kohaselt võivad andmesubjekti kohta väga isiklikku ja tundlikku teavet anda ka elektroonilise side metaandmed. Sellised metaandmed hõlmavad numbreid, millele on helistatud, külastatud veebisaite, geograafilist asukohta, helistamise kellaaega, kuupäeva ja kõne kestust. Need andmed võivaldavad teha täpseid järeldusi andmesubjektide eraelu, sotsiaalsete suhete, igapäevaste harjumuste ja tegevuste, huvide ning eelistuste kohta.[74]

1.2.4. Juurdepääsuandmed (ingl *access data)*

Juurdepääsuandmeid kasutatakse samal eesmärgil nagu abonendiandmeid elik nendega seotud kasutaja isiku tuvastamiseks.[75] Sellegipoolest on juurdepääsuandmete näol tegu andmetega, mille alusel ei ole otseselt võimalik kasutajat tuvastada, ent mis on kasutaja tuvastamisel siiski oluliseks juhtlõngaks.[76] Juurdepääsuandmed on seotud kasutaja teenusele juurdepääsu seansi alguse ja lõpuga seotud andmed.[77] Nendeks andmeteks võivad näiteks olla informatsioon selle kohta, millal kasutaja elektronposti või Interneti-telefoni teenust kasutas – kuupäev ja kellaaeg, millal sisse- ja väljalogimine toimus ning samuti teenusepakkuja poolt kasutajale eraldatud IP-aadress.[78]

---

[72] EKo *Tele2 Sverige*, p 5.
[73] Euroopa Parlamendi ja nõukogu määruse, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus) ettepaneku seletuskiri. Arvutivõrgus kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010, 13.12.2021
[74] E-privaatsuse määruse ettepaneku põhjenduspunkt 2.
[75] *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters 2018/0108(COD)*. Art 2 lg 8. Arvutivõrgus kättesaadav: https://eur-lex.europa.eu/legal-content/EN-ET/TXT/?from=EN&uri=CELEX%3A52018PC0225, 22.01.2021.
[76] *European Commission. Frequently Asked Questions: New EU rules to obtain electronic evidence* 17.04.2018.
[77] *Proposal 2018/0108(COD)*, art 2 lg 8.
[78] *European Commission. Frequently Asked Questions: New EU rules to obtain electronic evidence*.

1.2.5. Tehinguandmed (ingl *transactional data*)

Kavandatav Euroopa andmesäilitamismäärus[79] (edaspidi andmesäilitamismääruse ettepanek) on asunud metaandmeid liigitama teistel alustel, kui näiteks direktiiv 2006/24/EÜ ja direktiiv 2002/58/EÜ seda senini teinud on. Andmesäilitamismääruse ettepanek kategoriseerib andmed neljaks: sisu-, juurdepääsu-, tehingu- ja abonendiandmed. Andmesäilitamismääruse ettepanek ei too eraldi kategooriatena välja liiklus- ega asukohaandmeid, ent need on kaetud eespool mainitud nelja kategooriaga.

Tehinguandmed on teenuse osutaja poolt pakutava teenuse osutamisega seotud andmed, mille eesmärgiks on anda teavet sellise teenuse taustaandmete kohta või lisateavet ning mis luuakse või mida töödeldakse teenuse osutaja infosüsteemis. Nendeks andmeteks võivad olla näiteks sõnumi või muud liiki suhtluse allikas ja sihtkoht, seadme asukoha andmed, kuupäev, kellaaeg, kestus, suurus, marsruut, formaat, kasutatav protokoll ja tihenduse liik, välja arvatud juhul, kui selliste andmete näol on tegu juurdepääsuandmetega.[80]

Komisjoni ettepanekus on nii juurdepääsu- kui ka tehinguandmete kirjelduses toodud välja, et säilitatakse kuupäev ja kellaaeg, mis on kasutusel erinevate funktsioonide täitmisel. Juurdepääsuandmete puhul näitab kuupäev ja kellaaeg seda, millal sideseanss toimus. Tehinguandmete puhul seob kuupäev ja kellaaeg seansil olnu teatud kohta sellel kuupäeval ja kellaajal. Kui sideseansil muid tehinguandmeid juures ei ole siis kuupäeva ja kellaaja andmed jäävad juurdepääsuandmeteks ning muutuvad tehinguandmeteks üksnes siis, kui on juures ka mingid muud tehinguandmed (kindlasti asukohaandmed, aga võib olla ka midagi muud).

Kavandatava andmesäilitamismääruse ettepanekus on kõik need andmed kaetud Euroopa Liidu andmekaitseõigustikust tulenevate kaitsemeetmetega. Seejuures tuleb tähele panna, et andmekategooriate puhul varieerub põhiõigustele avalduva mõju suurus ning andmekategooriatele on ette nähtud erinevad režiimid. Tehingu- ja sisuandmed kuuluvad rangema režiimi alla ning juurdepääsu- ja abonendiandmete jaoks on ette nähtud kergem režiim. Abonendi- ja juurdepääsuandmed on uurimises kasulikud kahtlustatava isiku tuvastamiseks esimeste juhtlõngade leidmisel. Seevastu tehingu- ja sisuandmed on kõige asjakohasemad tõendusmaterjalina. Kuivõrd sekkumine põhiõigustesse on nende kategooriatega erinev,

[79] *Proposal 2018/0108(COD).*
[80] *Ibid.*

kehtestatakse erinevad tingimused ühelt poolt abonendi- ja juurdepääsuandmete ning teiselt poolt tehingu- ja sisuandmete hankimisele.[81]

Andmesäilitamismääruse ettepaneku kohaselt võib abonendi- ning juurdepääsuandmeid küsida mistahes kuriteo puhul. Seevastu tehingu- ja sisuandmetele tuleks kohaldada rangemaid nõudeid, sest need kaks andmeliiki on tundlikumad ning nende andmete küsimisega on sekkumise määr kõrgem võrreldes abonendi- ning juurdepääsuandmetega. Andmesäilitamismäärust võib ettepaneku kohaselt esitada üksnes nende kuritegude puhul, mis näevad karistusena ette vähemalt kolmeaastase vabadusekaotuse. Andmesäilitamismääruse ettepanek tagab vabadusekaotusel põhineva künnisega proportsionaalse lähenemisviisi.[82]

1.3. Elektroonilise side andmete talletamine

KrMS § 90^1 lg 1 alusel tehtava päringuga on võimalik saada abonendi- ja juurdepääsuandmeid ning lõike 2 alusel liiklus- ja asukohaandmeid.

Eraldi andmete tüüp, mida ESS ei reguleeri, on sisu puudutavad andmed. Sisuandmete mitte säilitamine ei ole mitte sideettevõtja õigus, vaid vastupidiselt kohustab ESS § 111^1 lg 9 p 4 sideettevõtjat andmete säilitamise korral side sisu kajastavad andmed säilitamata jätma. Andmete säilitamise eesmärk sideettevõtja poolt on kogutud andmete kättesaadavaks tegemine ESS § 111^1 lõikes 11 loetletud asutustele, et neil oleks võimalik enda ülesandeid täita.

Eesti on riigisisesesse õigusesse üle võtnud direktiivi 2006/24/EÜ elektroonilise side seadusega. Direktiivist 2006/24/EÜ on otseselt ESSi üle võetud ka selliste andmete liigid, mida sideettevõtjad on kohustatud säilitama. Nimelt sätestab direktiivi 2006/24/EÜ art 2 lg 2 p a), et sideandmed tähendavad eelkõige liiklus- või asukohaandmeid ja nendega seotud teavet, mis on vajalik abonendi või kasutaja kindlakstegemiseks.

Direktiivi 2006/24/EÜ artikkel 6 reguleerib säilitamistähtaegasid. Liikmesriikidel lasub kohustus sideandmeid säilitada minimaalselt kuue kuu ning kõige rohkem kahe aasta vältel alates side toimumise kuupäevast. Tulenevalt ESS § 111^1 lõikest 4 lasub sideettevõtjatel kohustus sama paragrahvi lõigetes 2 ja 3 nimetatud andmeid säilitada ühe aasta vältel alates side toimumise ajast.

[81] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, seletuspunkt 23.
[82] *Ibid.,* art 5.

Direktiivi 2006/24/EÜ artikkel 5 täpsustab säilitavate andmete liigid, mille alusel saab tuvastada järgnevaid asjaolusid: andmed, mis on vajalikud sideallika seiramiseks ja tuvastamiseks; andmed, mis on vajalikud side sihtpunkti tuvastamiseks; sideandmed, aeg ja koht; side liik; kasutaja sidevahend ja andmed, mis on vajalikud mobiilsidevahendi asukoha kindlaksmääramiseks.

ESS § 111^1 lõiked 2 ja 3 sätestavad andmed, mille säilitamise kohustus vastavalt telefoni- ja mobiiltelefoniteenuse, telefonivõrgu ja mobiiltelefonivõrgu teenuse osutajal ning Interneti-ühenduse, elektronposti ja Interneti-telefoni teenuse osutajal lasub. Täpne loetelu andmetest, mida telefoni- ja mobiiltelefoniteenuse ning telefoni- ja mobiiltelefonivõrgu teenuse osutaja on kohustatud säilitama, on sätestatud ESS § 111^1 lõikes 2 ning andmed, mille säilitamise kohustus lasub Interneti-ühenduse, elektronposti ja Interneti-telefoni teenuse osutajal, on välja toodud ESS 111^1 lõikes 3.

Euroopa Kohus tegi lahendi *Digital Rights Ireland* punktis 67 etteheite kehtetuks tunnistatud direktiivile 2006/24/EÜ ka säilitatud andmete hävitamise regulatsiooni osas. Etteheite kohaselt puudus direktiivis säte, mis kohustaks andmeid pöördumatult hävitama pärast säilitamistähtaja lõppu. Elektroonilise side seaduse § 106 lõike 3 kohaselt tuleb ESS § 111^1 lõigetes 2 ja 3 toodud andmed ning § 112 kohaselt esitatud järelepärimised ja teave kustutada viivitamatult pärast § 111^1 lõikes 4 nimetatud tähtaja möödumist. ESS § 111^1 lg 4 kohaselt peab sideettevõtja säilitama andmeid ühe aasta vältel alates side toimumise ajast. Sama sätte kohaselt säilitab päringu esitaja sideettevõtjalt saadud andmeid kaks aastat. See lõige reguleerib olukorda, kus andmete kustutamise kohustus on sideettevõtjale tehtud päringu esitajal, ent täpsemalt ei ole reguleeritud kuidas nende andmete kustutamine käib. Lisaks vajaks reguleerimist ka andmete kustutamine olukorras, kus kriminaalmenetluse raames kogutakse andmeid isiku kohta, kelle suhtes hiljem kahtlustus ära langeb.

Isikuandmete kaitse seaduse[83] § 14 lõige 1 sätestab isikuandmete töötlemise põhimõttena seaduslikkuse ja õigluse. See põhimõte kätkeb endas printsiipi, mille kohaselt isikuandmeid töödeldakse seaduslikult ja õiglaselt. Selle põhimõtte kohaselt saab isikuandmeid säilitada ja töödelda üksnes siis, kui selleks eksisteerib seaduslik alus. Sideettevõtjal kaob selline seaduslik alus ühe aasta möödumisel. Isikuandmete kaitse seadusest tulenevate põhimõtete kohaselt ei või sideettevõtja andmeid kauem säilitada. Ka selle seaduse kaudu saab tõlgendada andmete säilitamise ja töötlemise tähtaega.

[83] Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.

2. VÄLISRIIKIDE PRAKTIKA

2.1. Austraalia

2.1.1. Andmete säilitamise kohustus

Austraalia on võrreldes mitmete Euroopa riikidega elektroonilise side andmete säilitamise osas polariseerunud seisukohtadel. Euroopas on mitu riiki, kus õiguskaitseorganite jaoks andmete säilitamise kohustus puudub – Austria, Saksamaa ja Sloveenia. Nendes kolmes riigis saavad õiguskaitseorganid välja nõuda üksnes neid andmeid, mida sideettevõtjad on säilitanud ärilistel eesmärkidel.[84] Kontrastina – Austraalias on andmete säilitamise tähtajaks ette nähtud periood pikkusega kaks aastat.

Austraalias reguleerib elektroonilise side andmete säilitamisega seonduvat õigusakt *Telecommunications (Interception and Access) Act* 1979[85]. Nimetatud õigusaktiga on väga konkreetselt reguleeritud, kes, kui kaua ja milliseid elektroonilise side andmeid säilitama on kohustatud. Austraalias on laiapõhist andmete säilitamise kohustust põhjendatud eelkõige terrorismi vastu võitlemise vajadusega.[86] Elektroonilise side andmete säilitamise kohustus laieneb kõigile teenusepakkujatele, kes kasutavad enda teenuste pakkumiseks Austraalia infrastruktuure. Kohustus andmete säilitamise perioodi pikkuse osas tuleb sideettevõtjatele õigusaktist *Telecommunications (Interception and Access) Act* 1979, mille 2015. aastal uuendatud redaktsioon pani sideettevõtjatele kohustuse säilitada sideandmeid kaks aastat alates andmete tekkimise ajast.[87]

Austraalia õiguskaitseorganid on leidnud, et kaks aastat on kõige optimaalsem aeg andmete säilitamiseks. Kuigi enamik menetlusi saab läbi viidud andmete najal, mis on kuue kuu pikkuse perioodi vältel talletatud, on keerulisemate ja mitmetahulisemate raskete kuritegude lahendamiseks vajalik kuni kaheaastase perioodi vältel talletatud sideandmeid. Sellisteks keeruliseks ja mitmetahulisteks menetlusteks on terrorismi-, spionaaži-, majandus-, korruptsioonikuriteod ja organiseeritud kuritegevus.[88]

---

[84] *European Commission. Study on the retention of electronic communications non-content data for law enforcement purposes. Final report*. 2020. Lk 39-40. Arvutivõrgus kättesaadav: https://www.statewatch.org/media/1453/eu-com-study-data-retention-10-20.pdf, 20.03.2021.
[85] *Telecommunications (Interception and Access) Act* 1979.
[86] Reilly, C. *The metadata debate: What you need to know about data retention. – Cnet* 13.08.2014. Arvutivõrgus kättesaadav: https://www.cnet.com/news/what-you-need-to-know-about-data-retention/, 04.02.2021.
[87] *Telecommunications (Interception and Access) Act* 1979 § 187C 1 (b) (ii).
[88] *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Why data is retained for 2 years*. Arvutivõrgus kättesaadav: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations, 02.03.2021.

Kuigi üldine andmete säilitamise aeg on kaks aastat, tuleb abonendiandmeid täiendavalt säilitada terve kasutaja avatud olemise vältel ning lisaks veel kaks aastat pärast konto sulgemist. Säilitatud andmetele laienevad lisaks mitmed kohustused nagu andmete krüpteerimine ning andmeid tuleb kaitsta kolmandate osapoolte lubamatu ligipääsu eest.[89] Üldine andmete säilitamise kohustus on küll kaks aastat, ent sideettevõtjal on lubatud andmeid säilitada kauem, juhul kui see on sideettevõtjale vajalik. Kui sideettevõtja otsustab andmeid maksimaalselt lubatud kaheaastasest perioodist kauem säilitada, on õiguskaitseorganitel õigus nõuda ligipääsu ka kauem säilitatud andmetele.[90]

Austraalia kahe aasta pikkune andmete säilitamise periood on mitmel korral langenud kriitika alla. Näiteks ei peeta andmete säilitamise perioodi mõistlikuks, sest 2016-2017. aastal oli enamik välja nõutud metaandmeid alla kuuekuuse perioodi kohta ning sellest omakorda 80% andmetest lühema kui kolmekuuse perioodi kohta. Üksnes 4% välja nõutud andmetest hõlmasid pikemat kui kaheteistkuust perioodi ning ainult 1% andmetest oli 21-24-kuuse perioodi kohta.[91] Austraalia kaheaastane andmete säilitamise periood on kriitika osaliseks saanud ka seetõttu, et Austraalia tugines perioodi pikkuse valikul Euroopa eeskujule ning valis maksimaalse võimaliku pikkusega perioodi[92], ent Euroopa Kohus on avaldanud kriitikat selle kohta, et andmete säilitamine peaks piirduma üksnes sellega, mis on vältimatult vajalik.[93]

Eespool nimetatud kohustused on pandud sideettevõtjatele eesmärgiga anda Austraalia õiguskaitse- ja julgeolekuorganitele vajaduse korral andmetele ligipääs. Austraalia valitsus on rõhutanud, et andmed mängivad suurt rolli enamikes kriminaal- ning rahvusliku julgeolekuga seotud menetlustes. Eraldi on välja toodud, et elektroonilise side andmed on eriti tähtsad laste ärakasutamisega seotud kuritegude tõendamisel, sest seda liiki kuritegudes jagavad kurjategijad palju informatsiooni internetis.[94]

---

[89] *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Service Provider Obligations.*

[90] *Australian Government Attorney-General's Department. Data Retention*, 2015. Arvutivõrgus kättesaadav: https://www.homeaffairs.gov.au/nat-security/files/data-retention-industry-faqs.pdf, 06.03.2021.

[91] Vaile, D., Wijeyaratne. S., Churches. G., Zalneriutne, M. *Submission Telecommunications Data Review. University of New South Wales Law Research Series – Researchgate* VII/2019, lk 6.

[92] *Australian Government Department of Home Affairs. Parliamentary Joint Committee on Intelligence and Security. Review of the mandatory data retention regime. Home Affairs Portfolio submission*. Arvutivõrgus kättesaadav: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024394/toc_pdf/Reviewofthemandatorydataretentionregime.pdf;fileType=application%2Fpdf, 06.03.2021

[93] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12. *Digital Rights Ireland*, p 62 ja 65.

[94] *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Why lawful access to data is important*.

Austraalias saavad õiguskaitseorganid sideettevõtjatelt nende poolt talletatud elektroonilise side andmeid kätte ilma kohtumääruseta. Seevastu sisuandmete saamiseks kasutatakse telefoni pealtkuulamist ning selle toimingu jaoks on vaja kohtumäärust.[95] Sideettevõtjad ei ole kohustatud säilitama sisu-, vaid üksnes metaandmeid. Internetiteenuste pakkujatele ei laiene kohustus säilitada isiku internetis külastatud lehtede ajalugu[96] ega sotsiaalmeedias toimuvat.[97]

2.1.2. Säilitatavate andmete liigid

Telecommunications (Interception and Access) Act 1979 jagab säilitatavad andmed kuueks kategooriaks, milleks on:

1) kliendiandmed. Nende andmete kogumine on vajalik, et tuvastada abonendi nimi, aadress, samuti kontaktandmed nagu telefoninumber ja emaili aadress. Nende andmete pinnalt on võimalik kindlaks teha abonendi identiteet või seostada teda konkreetse kasutajaga või teenuse kasutamisega. Siia kategooriasse kuuluvad ka kasutajale eraldatud IP aadress ning arveldusandmed. Teenuse kasutamisega seoses on võimalik koguda andmeid selle kohta, millal kasutaja loodi ja mis on kasutaja staatus. Teenusepakkujatel ei ole kohustust koguda ja säilitada salasõnasid ja salaküsimusi.[98]

2) elektroonilise side andmete allikas. Nimetatud kategooriasse kuuluvad andmed on vajalikud tuvastamaks elektroonilise side seansiga seotud teenust, kasutajat või seadet. Selleks, et tuvastada elektroonilise side seansi allikas, kogutakse andmeid nagu telefoninumber, IMSI või IMEI kood, mis oli kasutusel telefonikõne tegemiseks või sõnumi saatmiseks. Samuti on võimalik sideettevõtjatelt saada andmeid nagu kasutajatunnus ja aadress, et tuvastada kasutaja, teenus või seade, mida kasutati tekst-, häälsõnumi või emaili saatmiseks. Sideettevõtjatelt on võimalik siin kategoorias nõuda ka kasutajale eraldatud IP-aadressi ning muid olemasolevaid andmeid, mille alusel tuvastada elektroonilise side seansiks kasutatud seade.[99] Täpsed säilitatavad andmed sõltuvad pakutavast teenusest. Selliselt on traditsiooniliste häälkõnede puhul elektroonilise side andmete allikaks ja säilitatavateks andmeteks telefoninumber, millelt

[95] Sarre, R. *Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia. University of South* Australia. – *ResearchGate* 2017, lk 2.
[96] *Ibid.*
[97] *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Web-browsing histories*.
[98] *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Data set*.
[99] *Ibid.*

kõne tehti. Seevastu internetiteenuse puhul on siin kategoorias säilitatavateks andmeteks IP-aadress.[100]

3) elektroonilise side lõpp-punktiga seotud andmed. Nende andmete põhjal on võimalik tuvastada millisele kasutajale, millise seadme või teenuse abil elektrooniline side on saadetud, edastatud või proovitud edastada või saata. Siia kategooriasse kuulub näiteks telefoninumber, millele helistati või saadeti tekstsõnum. Samuti ka kasutajatunnus ja aadress, et tuvastada kasutaja, teenus või seade, mida kasutati tekst-, häälsõnumi või vastuvõtmiseks. Sideettevõtjatelt on võimalik nõuda ka muid andmeid, mille alusel tuvastada elektroonilise side seansi vastu võtnud seadme andmeid.[101]

4) elektroonilise side toimumise kestus, kuupäev ja aeg. Neljanda kategooria alla kuuluvad andmed nagu elektroonilise side seansi või konkreetse teenuse kasutamise algus- ja lõpuaeg. Selle kategooria andmed on olulised telefonikõnede ja interneti kasutamise seansside puhul. Telefonikõnedega seoses on võimalik sideettevõtjalt saada informatsiooni seoses sellega, mis kellaajal telefonikõne algas ning millal see lõpetati. Internetiseansside puhul on võimalik saada andmeid selle kohta, millal konkreetne seade või kasutaja ennast võrku lülitas ning millal uuesti välja lülitas. Need seansid võivad kesta päevi, nädalaid või ka pikemaid perioode.

5) elektroonilise side liik ja side toimumisega seotud teenus. Siin kategoorias on võimalik eristada erinevaid elektroonilise side liike, milleks võivad olla hääl-, tekstsõnumid, emailid, foorumid ja sotsiaalmeedia. Teenusetüüpidest on võimalik eristada selliseid liike nagu ADSL[102], wifi, VoIP[103], kaabel, GPRS[104], VoLTE[105] ja LTE[106]. Siia kategooriasse kuuluvate andmete pinnalt on võimalik eristada, millist viisi side pidamiseks kasutati: häälsõnumid, internet, kas sõnumi saatmiseks kasutati SMS või MMS teenust. Samuti kuulub siia

[100] *Australian Government Attorney-General's Department. Data Retention* 2015.
[101] *Ibid.*
[102] Tegemist on interneti püsiühenduse liigiga. Ansi, T. *Network and Customer Installation Interfaces - Asymmetric Digital Subscriber Line (ADSL) Metallic Interface – Network Scholar*. 1998. Arvutivõrgus kättesaadav: https://www.semanticscholar.org/paper/Network-and-Customer-Installation-Interfaces-Line-Ansi/f1338fe5d9e583cde4901e49f35ca21bfbd0acbc, 01.02.2021.
[103] Tegemist on internetitelefoniga, kus heli transporditakse interneti või kohtvõrgu kaudu. Näiteks Skype. *Federal Communications Commission. Voice Over Internet Protocol*. Arvutivõrgus kättesaadav: https://www.fcc.gov/general/voice-over-internet-protocol-voip, 02.03.2020.
[104] Tegemist on pakettandmesideteenusega 2G ja 3G võrkudes.
[105] Tegemist on tehnoloogiaga, mis võimaldab häälkõnesid edastada 4G ehk LTE võrgu kaudu. Telia. Kõned 4G võrgus. Arvutivõrgus kättesaadav: https://www.telia.ee/era/mobiil/muud-lisateenused/volte/, 02.03.2021.
[106] Mobiilsidestandard.

kategooriasse ka interneti kasutamise maht, mis puudutab abonendi poolt üles või alla laetud andmete mahtu. [107]

6) elektroonilise side toimumise asukohaga seotud andmed. Siia kategooriasse kuuluvate andmete järgi on võimalik kindlaks teha nii sideseansi jaoks kasutatud seadme alg- kui ka lõppasukohta mobiilimasti või wifi võrgu asukoha järgi. Selliseid andmeid on võimalik saada kõnede, SMSide ja ADSL võrgus olevate seadmete kohta.[108]

Sõltuvalt pakutavast teenusest, ei pruugi sideettevõtjal lasuda kohustust säilitada andmeid kõigis kuues kategoorias. Näiteks ei pea internetiteenuste pakkujad säilitama kolmandas kategoorias olevaid andmeid, sest sellisel juhul oleks säilitatavaks andmeteks abonendi internetis külastatud lehtede ajalugu. Seadusandja on välistanud internetis külastatud lehtedega seotud andmete säilitamise kohustuse.[109]

Ühest küljest on Austraalias elektroonilise side andmete säilitamise kord rangem kui Eestis, sest Eestis kehtib sideettevõtjatel kohustus andmeid säilitada üks aasta *versus* Austraalias kehtiv andmete säilitamise periood kaks aastat. Teisest küljest on Eestis seadused paindlikumad selle poolest, et andmeid saab nõuda ka näiteks tsiviil- ja halduskohtumenetluses.[110] Austraalias saavad säilitatud sideandmetele ligipääsu nõuda üksnes õiguskaitseorganid.[111]

Inimõiguste tagamise seisukohalt, on oluline märkida, et Austraalias puudub selline analoogne keskne õigusakt nagu Euroopas on Euroopa Liidu põhiõiguste harta[112] (edaspidi harta). Austraalia seadused sideandmete säilitamise osas on leebemad ka nüansis, mis puudutab kohtu loa saamist. Austraalias ei ole kohtumäärust tarvis mitte ühegi elektroonilise side metaandmete liigi väljanõudmiseks, ent Eestis on prokuratuuri luba kohtueelses menetluses ning kohtumenetluses kohtu luba vaja KrMS § 90^1 lõike 2 alusel tehtava päringu jaoks. Austraalia andmete säilitamise põhimõtetele on ette heidetud madalat künnist nende kasutamiseks.[113] Kriitikas on võrdluseks toodud Ameerika Ülemkohus seisukoht, kus leiti, et kuivõrd asukohaandmed on samasuguse konfidentsiaalsusastmega nagu sisuandmed, vajavad need

[107] *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Data set.*
[108] *Ibid.*
[109] *Australian Government Attorney-General's Department. Data Retention* 2015.
[110] ESS § 111^1 lg 11 p 5.
[111] *Telecommunications (Interception and Access) Act* 1979 § 110A.
[112] Euroopa Liidu põhiõiguste harta. 2010/C 83/02
[113] Churches, G., Zalnieriute, M. – *A Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA – Australian Public Law* 26.02.2020. Arvutivõrgus kättesaadav: https://auspublaw.org/2020/02/a-window-for-change-why-the-australian-metadata-retention-scheme-lags-behind-the-eu-and-usa/, 02.04.2021.

sellest tulenevalt samasugust kaitset ning nende väljanõudmiseks on vaja kohtumäärust.[114] Austraalias sellist nõuet ei ole.

Lahendis *Carpenter v. United States* rõhutatakse riivet põhiõigustele, mis tekib seoses asukohaandmete säilitamisega.[115] Nimelt leidis kohus, et asukohaandmete säilitamise näol oli riive niivõrd ebaproportsionaalne, et asukohaandmetele ligipääsu saamine oli läbiotsimine Ameerika Ühendriikide põhiseaduse neljanda paranduse mõttes ning oleks seetõttu nõudnud kohtumäärust, mis tugineb küllaldasele alusele (*probable cause*). Kohus täpsustas, et asukohaandmed on samasuguse konfidentsiaalsusastmega nagu sisuandmed ning asukohaandmete põhjal tehtavad järeldused on sarnased nendele, mida tehakse inimese kohta GPS-seadme jälgimise teel.[116]

Ka Euroopa Kohus ja Euroopa Inimõiguste Kohus on mitmel korral rõhutanud, et elektroonilise side andmed võimaldavad isiku kohta teha sama täpseid järeldusi, kui neid saab teha sisuandmete pinnalt. Selliselt rõhutas Euroopa Kohus, et kuivõrd liiklus- ja asukohaandmete põhjal saab teha isiku kohta selliseid järeldusi nagu igapäevased või muud liikumised, tegevused, sotsiaalsed suhted ja ühiskonnagrupid, kellega läbi käiakse, siis on sellised andmed sama tundlik teave kui sideseansi sisu ise.[117] Euroopa Inimõiguste Kohus sedastas, et metaandmete kogumine ei ole tingimata vähem inimõigusi riivav kui sisuandmete kogumine. Sisuandmed võivad olla tihtipeale krüpteeritud, ent isegi kui nad seda pole, ei pruugi alati sisuandmete põhjal saada isiku kohta järeldusi teha. See-eest metaandmed paljastavad isiku identiteedi ja geograafilise asukoha ning võimaldavad saada aimdust isiku suhtlusringi ja suhtlemise mustrite (sh kellega ja kui tihti isik suhtleb) kohta.[118]

2.2. Euroopa riigid

2000. aastate alguses tõusetus järjest sagenevate terrorismirünnakute[119] valguses kõrgenenud vajadus kriminaalmenetluses andmete säilitamise ja sellise praktika ühtlustamise järele. Euroopa riigid rakendasid väga erinevaid praktikaid elektroonilise side andmete säilitamise osas. Osades riikides oli paigas seadusandlus, mis kohustas elektroonilise side andmete säilitamist teatud eesmärkidel, muu hulgas kuritegevuse vastu võitlemiseks. Enamikes riikides

[114] *Carpenter v United States,* 585 US 1 (6th Cir. 2018).
[115] *Ibid.*
[116] *Ibid*., p-d 426-428.
[117] EKo *Digital Rights Ireland,* p 27. EKo *Tele2 Sverige,* p 99.
[118] EIKo 13.09.2019, 58179/13, 62322/14 ja 24960/15. *Big Brother Watch vs the United Kingdom*, p 356.
[119] 2004. a Madridis ja 2005. a Londonis.

selline regulatsioon puudus. Kuivõrd riigid suhtusid andmete säilitamisse erinevalt, puudusid ühtsed arusaamad ja praktikad.[120]

Esimene euroopaülene õigusakt, mis üritas harmoniseerida liikmesriikide erinevat praktikat elektroonilise side andmete osas, oli direktiiv 2006/24/EÜ. Nimelt leiti, et seadusandlikud ja tehnilised erinevused siseriiklike sätete osas, mis puudutavad andmete säilitamist kuritegude ennetamise, avastamise, uurimise ja kohtus menetlemise eesmärgil, on takistuseks elektrooniliste sideteenuste siseturul. Sideettevõtjatele seatakse erinevates riikides erinevaid nõudmisi sõltuvalt andmete liigist, säilitamistingimustest ja säilitamistähtaegadest.[121]

Täpsemalt sätestas direktiivi 2006/24/EÜ eesmärgi artikkel 1, mille kohaselt oli direktiivi eesmärk ühtlustada liikmesriikide sätteid, mis käsitlevad üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate kohustusi säilitada teatavaid andmeid, mida nad loovad või töötlevad, et need oleksid kättesaadavad iga liikmesriigi riiklikus õiguses määratletud raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks. Direktiiv nägi ette, et seatud eesmärki saavutatakse artikli 3 punkti 1 kaudu. Nimelt sätestas artikli 3 punkt 1, et liikmesriigid peavad kohaldama meetmeid, mis tagavad nende jurisdiktsiooni alla kuuluvate üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate andmete, milleks on telefoni- ja internetiteenuste liiklus-, asukoha- ja kliendiandmed, säilitamise. Nimetatud direktiivi kohaldamisalast on *expressis verbis* välja jäetud sisuandmete talletamise kohustus[122]. Direktiiv 2006/24/EÜ väljendas põhimõtet, mille kohaselt andmete säilitamine peab ühest küljest olema vahend terrorismiga võitlemiseks, ent teisest küljest tuleb leida tasakaal inimeste põhiõiguste tagamise vahel.

Kuivõrd ei Euroopa Kohus, ega direktiivid 2006/24/EÜ ja 2002/58/EÜ ei anna juhiseid defineerimaks, mis kvalifitseerub raske kuriteona ja mis mitte, jääb see liikmesriikide enda otsustada. Liikmesriigid on sellele lähenenud väga erinevalt: mõned liikmesriigid on sätestanud nimekirja raske kuriteona kvalifitseeruvatest kuritegudest, teised riigid on lähtunud künnise põhimõttest. See tähendab, et raske kuriteona kvalifitseeruvad need kuriteod, mille eest on ette nähtud teatud aastate pikkune vabadusekaotus.[123] Kolmanda variandina on mõned riigid,

[120] Fenelly, D. *Data retention: the life, death and afterlife of a directive – Springer* VII/2018, lk 675.
[121] Direktiiv 2006/24/EÜ preambula.
[122] Direktiiv 2006/24/EÜ, art 5 lg 1.
[123] Vedaschi, V., Lubello, V. *Data Retention and its Implications for the Fundamental Right to Privacy*. *Tilburg Law Review*: 2015, lk 20.

näiteks Eesti, läinud seda teed, et on säilitatud sideandmetele seaduses ettenähtud ametkondadele taganud ligipääsu kõikide kuritegude (mh ka väärtegude) lahendamiseks.

Ajal, mil sideettevõtjale elektroonilise side andmete päringu tegemist kvalifitseeriti jälitustegevusena, leidis kohus, et teise astme kuriteo (kindlustuskelmus) menetluse raames sideettevõtjale andmete saamiseks päringu tegemine on kooskõlas põhiseadusega ning isiku õigusi liigselt mitte riivav. Kohus põhistas nimetatud järeldust muu hulgas sellega, et jälitustoimingu õiguspärasuse üle oli ette nähtud kohtulik järelkontroll.[124]

Kuigi liikmesriikide riigisisesed kohtud seadsid direktiivi 2006/24/EÜ kehtivust kahtluse alla sisuliselt direktiivi loomise ajast, jõudis direktiiv enne Euroopa Kohtu poolt kehtetuks tunnistamist jõus olla kaheksa aastat. Mitmete liikmesriikide kõrgeimad kohtud leidsid, et riigisisesed õigusaktid, millega nimetatud direktiiv üle võeti, olid kõik vastuolus põhiõiguste tagamisega. Nendeks riikideks olid Rumeenia, Saksamaa, Tšehhi, Bulgaaria ja Küpros.[125]

2011. aastal rõhutas Euroopa Komisjon enda direktiivi 2006/24/EÜ hindamisaruandes, et isikuandmed vajavad täiendavat kaitset ning seda on võimalik saavutada muu hulgas kuriteoliikide piiramise, mille puhul võimaldatakse andmete säilitamist ja nende kasutamist; andmete säilitusaja lühendamise ja säilitatavate andmeliikide vähendamise kaudu.[126] Kohus viitas Euroopa Inimõiguste Kohtu lahendis *S. and Marper vs the United Kingdom* kehtestatud standardile, millega seati piir eraisiku kohta andmete kogumise ja avaliku turvalisuse ja julgeoleku vahel. Nimetatud lahendis käsitleti DNA-profiilide ja sõrmejälgede säilitamist nii kuriteo toimepannud isikute kui ka isikute puhul, kelle osas kohtumenetlus on lõpetatud. Kohus leidis, et sellist eraelu puutumatuse piirangut saab põhjendatuks pidada üksnes sellisel juhul, kui tegemist on tungiva ühiskondliku vajadusega, kui piirang on taotletava eesmärgi suhtes proportsionaalne ja kui ametiasutuste esitatud põhjendused on asjakohased ja piisavad.[127]

Paralleele on võimalik tõmmata DNA-profiilide ja sõrmejälgede säilitamise ning elektroonilise side andmete säilitamise vahel. Ka Ameerika Ühendriikide lahend *United States v. Gratkowski* ilmestab olukorda, et kuigi elektroonilise side andmed ei hõlma andmeid bitcoinitehingute sisu

[124] RKKKo 3-1-1-51-14, p 20.2-22.4.
[125] *European Commission. Report from the commission to the council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC). COM(2011) 225 final*, 18.04.2011. Lk 5 ja 6. Arvutivõrgus kättesaadav: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF, 10.03.2021.
[126] *Ibid*., lk 30.
[127] EIKo 04.12.2008, 30562/04 ja 30566/04. *S. and Marper vs the United Kingdom*, p 101.

kohta, on seisukohad elektroonilise andmete säilitamise kohta analoogia korras üle kantavad ka muudele andmete liikidele. Nimelt leidis Ameerika Ühendriikide Apellatsioonikohus, et andmed bitcoini tehingute kohta on analoogsed arveldusandmete ning telefonikõnede logiga, sest bitcoiniga tehingute tegemine nõuab teadlikku tegevust, mis on analoogne telefoninumbri valimisega.[128] Samuti sedastas kohus, et on väga ebatõenäoline, et bitcoiniga tehinguid tegevad inimesed eeldaksid nende tehingute privaatsust olukorras, kus andmed kõikide tehingute kohta on plokiahelas avalikult nähtavad.[129]

Alates hetkest, mil lahendiga *Digital Rights Ireland* tunnistati direktiiv 2006/24/EÜ kehtetuks, on Euroopa tasemel andmete säilitamine riikide kaupa väga erinevalt reguleeritud. Seda hoolimata mitmetest Euroopa Kohtu lahendites[130] väljendatud seisukohtadest. Kohtu seisukohad lahendis *Digital Rights Ireland* ei jätnud kahetise arusaamise võimalust direktiivi 2006/24/EÜ kehtivuse osas, ent lahend ei puudutanud seda osa, mida liikmesriigid peavad tegema seadusandlusega, millega nimetatud direktiiv üle võeti. Sellest hoolimata tunnistasid mitmed liikmesriigid enda andmete säilitamisega seonduvad seadused kehtetuks ning mitmed riigid asusid seaduseid ümber tegema, et olla kooskõlas Euroopa Kohtu seisukohtadega.[131]

Direktiivi 2006/24/EÜ kehtetuks tunnistamine ei toonud endaga automaatselt kaasa riigisisese regulatsiooni, millega nimetatud direktiiv üle võeti, kehtetust. Seda sel põhjusel, et direktiivi ülevõtmisel on seadusandjal riigisisese regulatsiooni loomisel kaalutlusõigus.

21. detsembril 2016. aastal tegi Euroopa Kohus otsuse *Tele2 Sverige,* mis puudutas Euroopa Liidu liikmesriikide riigisisese sideandmete säilitamist puudutava regulatsiooni kooskõla Euroopa Liidu õigusega. Kuivõrd kaks aastat varem ilmunud lahendiga *Digital Rights Ireland* oli direktiiv 2006/24/EÜ tagasiulatuvalt kehtetuks tunnistatud, analüüsis kohus selle asemele kehtima jäänud direktiivi 2002/58/EÜ sätteid. Täpsemalt analüüsis kohus küsimust, kas direktiivi 2002/58 artikli 15 lõikega 1 koos harta artiklite 7, 8 ja 11 ning artikli 52 lõikega 1 on vastuolus sellised liikmesriigi õigusnormid, mis näevad kuritegevuse vastu võitlemise eesmärgil ette kohustuse säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud

[128] *United States v. Gratkowski, 9*64 F.3d 307, 311-312 (5th Cir. 2020).
[129] *United States v. Gratkowski*, 964 F.3d 312 (5th Cir. 2020).
[130] EKo *Digital Rights Ireland,* EKo*Tele2 Sverige,* EKo *La Quadrature du Net,* EKo *Privacy International,* EKo *Ministerio Fiscal* jne.
[131] Reichert, C. *Germany moves closer to data retention – ZDNet* 19.10.2015. Arvutivõrgus kättesaadav: https://www.zdnet.com/article/germany-moves-closer-to-data-retention/, 04.02.2021.

kasutajate kõik liiklusandmed ja asukohaandmed, olenemata kasutatud elektroonilise sidevahendi liigist.[132]

Kohus jõudis järeldusele, et Euroopa Liidu õigus ei luba liikmesriikidel panna sideettevõtjatele kohustust säilitada liiklus- ja asukohaandmeid üldiselt ja vahet tegemata.[133] Seda seetõttu, et andmesubjektide kohta liiklus- ja asukohaandmete säilitamine kujutab endast rasket ja ulatuslikku põhiõiguste riivet, sest säilitatud andmed võimaldavad andmesubjekti kohta teha väga täpseid järeldusi ning andmete säilitamine tekitab isikutes tunde, et nende eraelu on konstantse jälgimise all.[134] Sellist rasket riivet saab põhjendada üksnes võitlusega raskete kuritegude vastu.[135] Olulise põhimõttena sedastas kohus, et Euroopa Liidu õigusega ei ole vastuolus selline olukord, kus liikmesriigi õigusnormid sätestavad liiklus- ja asukohaandmete eesmärgipärase ennetava säilitamise (*targeted retention*) raske kuritegevuse võitlemise eesmärgil väga kindlal tingimusel. Nimelt peab liikmesriik tagama, et andmete säilitamine oleks säilitatavate andmete liigi, asjassepuutuvate sidevahendite ja isikute ning säilitamise kestuse osas piiratud rangelt vajalikuga.[136]

Kohus rõhutas, et direktiiv 2002/58/EÜ ei välista liikmesriikide riigisisesest õigusest norme, mis võimaldavad liiklus- ja asukohaandmete eesmärgipärast ennetavat säilitamist. Riigisisesed normid, mis sellist säilitamist võimaldavad, peavad vastama vältimatult vajaliku kriteeriumitele. Nendeks kriteeriumiteks on:

1) selged, täpsed ja siduvad sätted, mis määravad kindlaks, mis tingimustel annavad sideettevõtjad pädevatele riigiasutustele loa andmetele ligi pääsemiseks;
2) üldise printsiibi kohaselt saab ligipääsu andmetele tagada ainult siis, kui selle eesmärk on kuritegevusega võitlemine. Andmeid saab väljastada siis, kui isiku suhtes on tekkinud kahtlus, et ta planeerib, paneb kuritegu toime või on kuriteo toime pannud. Erandina on andmete väljastamine vastuvõetav näiteks sellises olukorras, kus terroristi rünnak ohustab rahvusliku julgeoleku huve;
3) säilitatud andmetele ligipääsu lubamine peaks olema kohtu või muu sõltumatu asutuse kontrolli all;

[132] EKo *Tele2 Sverige*, p 62.
[133] *Ibid.*, p 112.
[134] *Ibid.*, p 99-101.
[135] *Ibid.*, p 102.
[136] *Ibid.*, p 108.

4) võttes arvesse andmete sensitiivsust, peab riigisisene regulatsioon tagama meetmed, millega sätestatakse, et andmeid säilitatakse üksnes Euroopa Liidu riikide territooriumil ning et andmed hävitatakse pöördumatult säilitamisperioodi tähtaja möödumisel;
5) säilitatud andmete kasutamist peavad reguleerima materiaal- ja menetlusõiguslikud tingimused.[137]

Kolmas sideandmete säilitamist puudutav lahend oli *Ministerio Fiscal*.[138] Kui varasemate lahenditega kohus pigem piiras õiguskaitseorganite võimalusi, siis nimetatud lahendis olid kohtu seisukohad võrreldes eelmiste lahenditega leebed. Kohus selgitas, et kui andmete juurdepääsuga kaasnev riive ei ole raske, siis võib juurdepääsu põhjendada üldise kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga.[139] Kohus leidis, et õiguskaitseorganite juurdepääs sellistele andmetele nagu andmesubjekti ees- ja perekonnanimi ning aadress, millega saab identifitseerida seadme omanikku, kujutab endast riivet, mis ei ole nii raske, et seda saaks piirata üksnes võitlusega raske kuritegevuse vastu.[140]

6. oktoobril 2020. aastal tegi Euroopa Kohus andmete säilitamise teemal kaks põhimõttelise tähtsusega lahendit, milleks olid C-623/17 (edaspidi *Privacy International*)[141] ja liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18 (edaspidi *La Quadrature du Net*)[142].

Lahendites *La Quadrature du Net* ja *Privacy International* vaagiti muu hulgas sideandmete julgeolekuasutustele edastamise küsimust. Kohus sedastas esmalt lahendis *Privacy International*, et direktiivi 2002/58/EÜ kohaldamisalasse kuuluvad need õigusnormid, mis näevad ette sideettevõtjale kohustuse riigi julgeoleku kaitsmise eesmärgil edastada julgeoleku- ja luureteenistusele liiklus- ja asukohaandmeid.[143] Kohus pidi selles osas seisukoha võtma, sest Suurbritannia eelotsuse esimese küsimusega seati direktiivi kohaldamisala kahtluse alla põhjendusega, et riigi julgeoleku tagamine kuulub liikmesriikide ainupädevusse ja jääb seetõttu kohaldamisalast välja.[144] Kohus märkis, et direktiiv 2002/58/EÜ lubab riikidel artikli 15 lõikes 1 sätestatud meetmeid võtta üksnes selles ette nähtud tingimustel, milleks on muu hulgas

[137] *Eucrim The European Criminal Law Associates Forum – 2016/4. Focus: Anti-Money Laundering. Data Protection. CJEU Opposes General Data Retention Regimes (Case Tele2 Sverige),* lk 164. Arvutivõrgus kättesaadav: https://eucrim.eu/media/issue/pdf/eucrim_issue_2016-04.pdf#page=14, 16.03.2021.
[138] EKo 02.10.2018, C-207/16. *Ministerio Fiscal*.
[139] *Ibid*., p 57.
[140] *Ibid*., p 58.
[141] EKo 06.10.2020, C-623/17. *Privacy International*.
[142] EKo 06.10.2020, liidetud kohtuasjad C-511/18 (*La Quadrature du Net*), C-512/18 (*French Data Network*) ja C-520/18 (*Ordre des barreaux francophones et germanophone*), *La Quadrature du Net.*
[143] EKo *Privacy International*, p 49.
[144] *Ibid*., p 32.

elektrooniliste side teenuste osutajate tegevus.[145] Sideettevõtjad on aga teenuse osutajad, kelle näol ei ole tegemist riigiasutustega ning sellest tulenevalt on tegemist andmete töötlemisega teenuseosutaja poolt, mida ei saa võrdsustada riigile omaste tegevustega.[146]

Kuivõrd varasemates lahendites ei olnud Euroopa Kohus analüüsinud andmete säilitamist riigi julgeoleku kaitse seisukohast, siis lahendis *La Quadrature du Net* pidas Euroopa Kohus vajalikuks seda aspekti käsitleda. Kohus kinnitas lahendis *La Quadrature du* Net varasemast *Tele2 Sverige* lahendist tuttavat seisukohta, mille kohaselt Euroopa Liidu õigusega ei ole kooskõlas need liikmesriikide riigisisesed õigusnormid, mis lubavad kuritegevusevastase võitluse eesmärgil üldist ja vahet tegemata andmete säilitamist.[147] Sellegipoolest on liikmesriikidel lubatud rakendada sellist seadusandlikku meedet, mis lubab pädevatel asutustel kohustada sideettevõtjaid säilitama kõikide elektroonilise side vahendite kasutajate liiklus- ja asukohaandmeid piiratud aja vältel, kui riik seisab silmitsi riigi julgeolekut ähvardava suure ohuga, mis osutub tõeliseks, vahetuks ja ettearvatavaks.[148]

Lahendis *Privacy International* lahendati Suurbritannia poolt esitatud eelotsusetaotlust. Nimelt kehtib Suurbritannias kord, mille kohaselt sideettevõtjad edastavad andmed automaatselt julgeoleku- ja luureteenistustele, kes need andmed säilitavad.[149] Kohus keelas ära sellise regulatsiooni, mis paneb sideettevõtjatele kohustuse andmeid säilitada üldiselt ja vahet tegemata julgeoleku- ja luureteenistusele edastamise eesmärgil.[150] Kohus põhistas oma seisukohta sellega, et liiklus- ja asukohaandmete edastamine julgeoleku- ja luureteenistustele kujutab endast harta artikliga 7 kaitstud õiguse eriti rasket riivet.[151] Samuti säilitatakse andmeid julgeoleku- ja luureteenistustele andmete edastamise eesmärgil üldiselt ja vahet tegemata kõigi isikute kohta, isegi kui pole alust nende käitumist seostada riigi julgeoleku ohtu seadmisega.[152] Teisisõnu, andmete üldine ja vahet tegemata säilitamine tähendaks sellisel juhul, et kõikide sideteenuste tarbijate osas on kahtlus, et nad on terroristid.

Selleks, et kaardistada elektroonilise side andmete säilitamisega seonduvat olukorda Euroopas, toob töö autor esmalt ülevaate olukorrast pärast lahendit *Digital Rights Ireland* ja seejärel selgitab Belgia regulatsiooni tänasel päeval.

[145] *Ibid.*, p 32.
[146] *Ibid.*, p 38.
[147] EKo *Tele2 Sverige*, p 112.
[148] EKo *La Quadrature du net*, p 37.
[149] *Ibid*., p 52.
[150] *Ibid*., p 81.
[151] *Ibid*., p 71.
[152] *Ibid*., p 80.

Direktiiv 2006/24/EÜ tunnistati kehtetuks 8. aprillil 2014. aastal. 26. oktoobri 2015. aasta seisuga oli lahend *Digital Rights Ireland* liikmesriikidele väga erinevat mõju avaldanud. Järgmised riigid olid 2015. aastaks direktiivi 2006/24/EÜ üle võtvad õigusaktid tühistanud: Austria, Belgia, Bulgaaria, Holland, Poola, Rumeenia, Saksamaa, Slovakkia ja Sloveenia. Soomes ja Taanis olid tuginedes lahendile *Digital Rights Ireland* 2015. aastaks õigusakte muutnud. Endiselt eksisteeris mitmeid riike, mille õigusaktides kehtis andmete säilitamist puudutav osa 2015. aastal muutmata kujul edasi, nendeks riikideks on Eesti, Hispaania, Horvaatia, Iirimaa, Läti, Luksemburg, Malta, Portugal, Prantsusmaa, Rootsi, Tšehhi ja Ungari.[153]

Belgia oli üks neid riike, mis tühistas pärast lahendit *Digital Rights Ireland* enda riigisisese õigusakti, millega võeti üle direktiiv 2006/24/EÜ. Belgia kassatsioonikohtusse jõudis menetlus, mille üks küsimusi taandus sellele, kas tühistatud riigisisese õigusakti alusel kogutud tõendid on lubatavad. Kohus tugines selle küsimuse lahendamisel nn antigoon doktriinile (*antigoon doctrine*).[154] Antigoon doktriini kohaselt on kohtunikul lubatud tugineda lubamatule tõendile sellisel juhul, kui lubamatu tõendi kogumise viis on võrreldes kuriteo enda raskusega väikese tähtsusega. Seni, kuni lubamatul viisil kogutud tõend ei ole ebausaldusväärne või ei riku õigust ausale kohtumenetlusele, on lubatud sellist tõendit kasutada. Doktriini järgi ei ole tõend, mis on kogutud, inimõiguste konventsiooni artiklit 8 (õigus era- ja perekonnaelu austamisele) rikkudes, automaatselt lubamatu, vaid tõendi lubamatuks kuulutamiseks peaks lisaks veel aset leidma näiteks artikli 6 (õigus õiglasele kohtumenetlusele) rikkumine.[155]

Belgia kassatsioonikohus jõudis sideandmete kui tõendi lubatavuse osas järeldusele, et kuigi selle kogumisega rikuti inimõiguste konventsiooni artiklit 8, ei ole tegemist lubamatu tõendiga, sest puudub artiklis 6 sätestatud rikkumine ega pole põhjust kahelda tõendi usaldusväärsuses.[156] Selline seisukoht on kooskõlas Euroopa Inimõiguste Kohtu praktikaga, kus kohus on järjekindlalt juurutanud põhimõtet, mille kohaselt tõendi kogumisel konventsiooni artikli 8 rikkumine ei too automaatselt kaasa artikli 6 rikkumist.[157]

---

[153] *Eurojust's analysis of EU Member States' legal framework and current challenges on data retention* 26.10.2015, lk 4-5. Arvutivõrgus kättesaadav: https://www.statewatch.org/media/documents/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf, 07.03.2021.
[154] Zubik, *et al.*, lk 64.
[155] De Hert, P. *Courts, Privacy and Data Protection. An Inventory of Belgian Case Law from the pre-GDPR regime* (1995-2015) – *Brussels Privacy Hub*: 2019, lk 9-10.
[156] Zubik, *et al.*, lk 65.
[157] EIKo 12.05.2000, 35394/97. *Khan vs the United Kingdom*, p 40. EIKo 05.11.2002. 48539/99. *Allan vs the United Kingdom*, p 52.

Belgias pärast *Digital Rights Ireland* lahendit jõustatud seaduse kohaselt oli sideettevõtjatel endiselt kohustus abonendi-, liiklus- ja asukohaandmeid säilitada kuni 12 kuuks. Erinevus võrreldes vana seadusega seisnes selles, et uue redaktsiooni kohaselt ei saanud enam taotleda andmete säilitamise pikendamise tähtaega. Kuigi andmeid säilitati 12 kuu pikkuse perioodi jooksul, ei tähenda see tingimata, et säilitatud andmetele saadakse kriminaalmenetluses kasutamise otstarbeks kergekäeliselt luba. Sideandmete kasutamiseks luba andev prokurör või eeluurimiskohtunik peab põhjendama sellise meetme proportsionaalsust ja vajalikkust. Sideandmeid on võimalik välja nõuda *ultima ratio* põhimõttel, kui puuduvad muud vahendid, millega sellistele andmetele ligi pääseda.[158]

Belgia on valinud lähenemise, mille kohaselt loa sideandmete kasutamiseks annab sõltuvalt andmete liigist kas prokurör või eeluurimiskohtunik. Periood, mille jooksul säilitatud andmeid tuleb välja nõuda, on vastavuses kuriteo raskusega. Prokuröri pädevus on anda lubasid abonendiandmete välja nõudmiseks. Andmeid tuleb küsida 6 kuu jooksul kuritegude kohta, mille karistusena on ette nähtud alla ühe aasta vangistust ja 12 kuu jooksul nende kuritegude kohta, mille karistusena on ette nähtud vähemalt ühe aasta pikkune vangistus. Eeluurimiskohtunik saab anda loa liiklus- ja asukohaandmetele nõudmiseks. Andmeid tuleb küsida 12 kuu jooksul spetsiifiliste terrorismikuritegude kohta, 9 kuu jooksul nende kuritegude kohta, mis on toime pandud kuritegeliku ühenduse raames ning mille karistusena on ette nähtud vähemalt 5 aasta pikkune vangistus ja 6 kuu jooksul muude kuritegude kohta.[159]

Belgia riigisiseses regulatsioonis on eraldi säte, mis tagab advokaatide ja arstide kutsesaladuse hoidmise. Nimelt on advokaatide ja arstide kohta võimalik elektroonilise side andmeid saada vaid juhul, kui neid kahtlustatakse kuriteo toimepanemises.[160] Nimetatud eeltoodud muudatuste tõttu hindas Belgia andmekaitsevolinik, et uue seadusega on peamised kitsaskohad elimineeritud.[161] Belgia andmekaitsevolinik kritiseeris enda aruandes Euroopa Kohtu lahendeid, leides, et on raske luua toimivat süsteemi, kus on kohustus andmete säilitamist piirata ainult konkreetsete isikute, perioodide või geograafiliste piirkondadega. Samuti toodi välja, et riivet õigusele eraelule kompenseerib piiratud säilitamisperioodi kestus, andmete hävitamine, erapooletu institutsiooni kontroll andmete säilitamise üle ning kutsesaladuse kaitsmine.[162]

---

[158] Zubik, *et al.*, lk 65.
[159] *Ibid*., lk 66.
[160] *Ibid.*, lk 65.
[161] Jacques, L., Cavez, B. *National Intelligence authorities and surveillance in the EU: FUndamental rights safeguards and remedies* 13.06.2016. Arvutivõrgus kättesaadav: https://staging-new.fra.europa.eu/sites/default/files/fra_uploads/belgium-study-data-surveillance-ii-be.pdf, 15.03.2021.
[162] Zubik, *et al.*, lk 66.

2016. aastal kui kohus tegi uue lahendi *Tele2 Sverige*, sattus Belgia senine andmete säilitamist reguleeriv regulatsioon kriitikatule alla ning konstitutsioonikohtul paluti hinnata regulatsiooni uue Euroopa Kohtu lahendi valguses. Belgia andmekaitsevoliniku esindajad leidsid, et uus seadus on lahendis *Tele2 Sverige* toodud seisukohtadega kooskõlas, sest seadusandja oli seaduse parandamisel silmas pidanud harta artiklit 7, tagades mitmeid kaitsemeetmeid. Seevastu õigusteadlaste hinnangul ei ole seadus siiski kooskõlas, sest *Tele2 Sverige* lahendis leiti sõnaselgelt, et EL õigusega ei ole kooskõlas need riigisisesed õigusnormid, mis lubavad andmete laussäilitamist, sõltumata eksisteerivatest maandamismeetmetest.[163]

Belgia konstitutsioonikohus esitas Euroopa Kohtule oma eelotsusetaotluses kolm küsimust. Nendest esimesega soovis konstitutsioonikohus välja selgitada, kas direktiiviga 2002/58/EÜ ja hartaga on vastuolus need riigisisesed normid, mille eesmärk ei ole ainult raskete kuritegude uurimine, avastamine ja kohtus menetlemine, vaid ka riigi julgeoleku, territooriumi ja avaliku julgeoleku kaitse tagamine, muude kui raskete kuritegude uurimine, avastamine ja kohtus menetlemine või elektrooniliste sidesüsteemide keelatud kasutuse vältimine, kui andmete säilitamise ja neile juurdepääsuga on ette nähtud piisavad tagatised.[164]

Euroopa Kohus sedastas lahendis *La Quadrature du Net*, et Euroopa Liidu õigusega on üldprintsiibina vastuolus selline riigisisene õigusnorm, mis näeb ette üldist ja vahet tegemata andmete säilitamist. Siiski on lubatud sellised riigisisesed seadusandlikud meetmed, mis lubavad riigi julgeoleku kaitsel teha sideettevõtjale ettekirjutuse säilitada liiklus- ja asukohaandmeid üldiselt ja vahet tegemata nendes olukordades, kus liikmesriik seisab silmitsi riigi julgeolekut ähvardava suure ohuga, mis osutub tõeliseks, vahetuks või ettearvatavaks.[165]

Teise küsimusega soovis konstitutsioonikohus teada, kas direktiiviga 2002/58/EÜ ja hartaga on vastuolus need riigisisesed õigusnormid, mille eesmärk on eelkõige nende positiivsete kohustuste täitmine, mis tulenevad harta artiklitest 4 ja 8, milleks on kehtestada õiguslik raamistik, mis võimaldab tõhusat kriminaaluurimist ja alaealiste seksuaalse kuritarvitamise tõhusat karistamist ning mis võimaldab kuriteo toimepanijat tegelikult tuvastada, kui on kasutatud elektroonilisi sidevahendeid.[166]

Kohus leidis sellele küsimusele vastamisel, et internetis toime pandud süüteo korral võib tihtipeale IP-aadress olla ainuke uurimisvahend, mis võimaldab tuvastada isiku, kellele see

[163] *Ibid*., lk 67.
[164] EKo *La Quadrature du Net*, p 79.
[165] *Ibid*., p 137.
[166] *Ibid*., p 79.

aadress süüteo toimepanemise ajal kuulus.[167] Kohus sedastas, et IP-aadressid on vähem tundlik teave kui muud liiklusandmed, sest e-kirjade ja internetitelefonide puhul säilitatakse ainult sideallika IP-aadressid, ent mitte vastuvõtja IP-aadressid ning seega ei koguta teavet kolmandate isikute kohta, kes suhtlesid side algatanud isikuga.[168] Kuivõrd IP-aadresside säilitamisega kaasnev riive on vähem raske kui muude andmete säilitamisega ning sellest tulenevalt võib olla põhjendatud IP-aadresside säilitamine üldise kuritegude ennetamise, uurimise, avastamise ja menetlemise eesmärgiga.[169] Samuti on põhjendatud sideühenduse lähtepunktile omistatud IP-aadresside üldine ja vahet tegemata säilitamine, kui see toimus riigi julgeoleku kaitsmise, raskete kuritegude vastu võitlemise ja avalikku julgeolekut ähvardava suure ohu ennetamise eesmärgil ajavahemikus, mis on piiratud tingimata vajalikuga.[170] Kohus leidis, et on põhjendatud elektroonilise side vahendite kasutajate identiteediga seotud andmete (nimi, eesnimi, nendega seotud postiaadressid, nende e-posti aadressid või nendega seotud konto aadressid, salasõnad ja juhul, kui lepingu sõlmimine või konto loomine on tasuline, siis kasutatud makseviis, makse viitenumber, summa ning tehingu kuupäev ja kellaaeg)[171] üldine ja vahet tegemata säilitamine riigi julgeoleku kaitsmise, kuritegevuse vastu võitlemise ja avaliku julgeoleku kaitsmise eesmärgil.[172]

Kolmanda küsimusega soovis kohus teada saada, et juhul kui konstitutsioonikohus „peaks oma esimesele või teisele eelotsuse küsimusele antud vastuste alusel jõudma järeldusele, et vaidlustatud seadus eirab ühte või mitut nendes küsimustes nimetatud õigusnormidest tulenevat kohustust, kas ta võib seaduse õiguslikud tagajärjed ajutiselt jõusse jätta, et vältida õiguslikku ebakindlust ja võimaldada, et eelnevalt kogutud ja säilitatud andmeid saaks veel seaduses osutatud eesmärkide jaoks kasutada?“[173]

Kolmandale küsimusele vastates jõudis kohus järeldusele, et liikmesriigi kohus ei või säilitada erakorraliselt ja ajutiselt tühistatud õigusakti mõjusid. Kui liikmesriikidele antaks õigus kas või ajutiselt enda riigisisestele sätetele anda ülimus liidu õiguse ees, siis kahjustaks see liidu õiguse ülimust.[174] Kohus markeeris, et ainult Euroopa Kohus võib erandlikel juhtudel ja õiguskindlusest tulenevatel ülekaalukatel põhjustel ajutiselt peatada välistava mõju, mis on liidu õigusnormil sellega vastuolus oleva riigisisese õigusakti suhtes.[175] Liikmesriigid ei saa

[167] *Ibid*., p 154.
[168] *Ibid*., p 152.
[169] *Ibid*., p 157-158.
[170] *Ibid*., p 168.
[171] *Ibid*., p 195.
[172] *Ibid*., p 168.
[173] *Ibid*., p 79.
[174] *Ibid*., p 217.
[175] *Ibid*., p 216.

säilitada selliste riigisiseste õigusnormide toimet, mis panevad liidu õigusega vastuolus olevaid kohustusi sideettevõtjatele ja millega kaasnevad andmesubjektide rasked riived.[176] Kuivõrd kolmas küsimus tõstatab kaudselt küsimuse, kas liidu õigusega on vastuolus liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamise teel saadud tõendite kasutamine, võttis kohus seisukoha ka selles. Kohus selgitas, et üksnes riigisiseses õiguses saab kindlaks määrata reeglid tõendite lubatavuse hindamiseks.[177] Sellegipoolest peab kohus välistama tõendi, kui ta leiab, et kriminaalmenetluse pool ei saa tõhusalt kommenteerida tõendit, mis kuulub valdkonda, millest kohtunikud teadlikud ei ole ja mis võib ülekaalukalt mõjutada faktiliste asjaolude hindamist.[178]

Eesti ja Belgia on lähenenud riigisisese õiguse muutmisele väga erinevalt. Kui Eesti on pigem võtnud passiivse seisukoha ja senini oodanud Euroopa Kohtu lõplikke seisukohti, enne kui riigisisest seadust Euroopa Kohtu praktikaga kooskõlla viia, siis Belgia asus riigisisest seadust muutma pärast esimest Euroopa Kohtu andmesäilitamismaastikku reguleerivat lahendit. Praegu kehtib Belgias 2016. aastal muudetud reaktsioon, mis ilmselt läbib peatselt uuenduskuuri.

Kui Belgias on kohtud rajanud enda otsused lähtuvalt antigooni doktriinist tulenevatele põhimõtetele, siis Ameerika Ühendriikides on tähtsal kohal kolmanda osapoole doktriin.

1970. aastatel tegi Ameerika Ühendriikide Ülemkohus kaks markantse tähtsusega lahendit[179], mis puudutavad Ameerika Ühendriikide põhiseaduse neljandat parandust[180] ja seda, kuidas selle raames tõlgendada õigust privaatsusele. Nende lahendite keskseks punktiks on Ameerika Ühendriikide põhiseaduse neljandas paranduses sätestatud põhimõte, mille kohaselt isikul on õigus olla kaitstud põhjendamatu vahistamise, enda kodu või iseenese läbiotsimise eest. Täpsemalt sätestab põhiseaduse neljas parandus, et keelatud on rikkuda inimeste õigust olla kaitstud iseenda, oma kodu, dokumentide ja vara alusetu läbiotsimise ja konfiskeerimise eest. Vastav määrus läbiotsimiste ja konfiskeerimiste läbiviimiseks väljastatakse üksnes küllaldase aluse korral ning määruse koostaja peab olema andnud vande või ametliku kinnituse. Määruses peab olema kirjeldatud läbiotsitavat kohta, vahistatavat isikut või konfiskeeritavat eset.

Lahenditest *United States v. Miller* ja *Smith v. Maryland* tulenevad olulised põhimõtted, mis on aluse pannud kolmanda osapoole doktriinile. Nimelt juurutas kohus neis kahes lahendis

[176] *Ibid*., p 219.
[177] *Ibid*., p 222.
[178] *Ibid*., p 226.
[179] *United States v. Miller*, 425 U.S. 435 (1976) ja *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).
[180] *U.S. Constution Amendment IV*. Arvutivõrgus kättesaadav: https://constitution.congress.gov/constitution/.

seisukohti, mille kohaselt isikutel, kes on vabatahtlikult enda andmed teinud kättesaadavaks kolmandatele osapooltele (mh telefonifirmad, Interneti-teenuse pakkujad, e-posti serverid), ei ole mõistlikku ootust privaatsusele. Kohus kiitis mõlemas lahendis heaks valitsuse juurdepääsu suurele hulgale andmetele nagu milliseid veebilehti isikud külastavad, kellele nad emaile saadavad, millistele telefoninumbritele nad helistavad, nende hariduse ja pangandusega seotud andmed jne.

Lahendites *United States v. Miller* ja *Smith v. Maryland* jõudis kohus järeldusele, et valitsuse ligipääs telefonikõnedele ja pangaandmetele ei ole läbiotsimine põhiseaduse neljanda paranduse mõttes ning sellest tulenevalt ei ole selleks ka kohtumäärust vaja. Sarnaselt ei ole tegemist läbiotsimisega ning isikute õigus privaatsusele ei ole kaitstud ka sellisel juhul, kui politsei vaatab läbi prügi, mille inimene on teepervele jätnud[181] või kui politsei jälgib isiku liikumist avalikel tänavatel[182]. Mõlemas lahendis leidis kohus, et kuivõrd isikud ise tegid enda andmed avalikkusele teatavaks, siis ei saanud nad mõistlikult eeldada kaitset privaatsusele.

Kuivõrd lahendid *United States v. Miller* ja *Smith v. Maryland* tehti 1970. aastatel, pärast mida on aastakümnete vältel toimunud suured tehnoloogilised ja sotsiaalsed muutused, on esile kerkinud küsimus, kas lahendites väljendatud seisukohad ja kolmanda poole doktriin peaks kehtima seniajani.[183] Teravat kriitikat on väljendatud lahendite osas seetõttu, et pärast 1970. aastaid on oluliselt muutunud ja arenenud viisid, kuidas andmeid kogutakse, automatiseeritakse ja töödeldakse.[184]

[181] *California v. Greenwood*, 486 U.S. 35, 43-44 (1988).
[182] *United States v. Knotts*, 460 U.S. 276, 285 (1983).
[183] Thompson II, R. M. *The Fourth Amendment Third-Party Doctrine – Congressional Research Service* VI/2014, lk 7.
[184] Tene, O., Polonetsky, J. *Big Data for All: Privacy and User Control in the Age of Analytics. – Northwestern Journal of Technology and Intellectual Property* V/2013, lk 240.

3. SIDEANDMETE SÄILITAMISE PÕHISEADUSPÄRASUS

3.1. Riivatavad põhiõigused ja riive lubatavus

21. sajandil on inimeste privaatsus seatud ohtu mitme allika poolt. Üheks selliseks ohuks on seadused, mis panevad sideettevõtjatele kohustuse kõikide inimeste kohta andmeid säilitada. Teisalt on selline andmete kogumise viis väga efektiivne terrorismi ja raskete kuritegude vastases võitluses, mis on hädavajalik inimeste õiguse elule ja tervisele kaitseks. Arvestades, milliste fataalsete tagajärgedega on terrorismikuriteod, on nende ärahoidmine vajalik tegevus.

Sideandmete säilitamise puhul tuleb mõista, et kaalukausil on ühest küljest need inimesed, kelle õigusi andmete säilitamisega riivatakse. Teisel kaalukausil on need inimesed, kes on huvitatud andmete säilitamisest ja seeläbi kasu saamisest – nende inimeste õigusi riivatakse andmete säilitamata jätmisega. Samuti riivatakse andmete säilitamata jätmisega riigi ja erinevate institutsioonide huvisid, sest neil lasub põhiseaduslik kohustus tagada oma rahva elu ja tervise ning vara kaitse. Peatüki alapeatükkides 3.1.1. kuni 3.1.3. tuuakse välja, millised on need õigused, mida riivatakse andmesubjektide sideandmete säilitamisega. Peatüki alapeatükkides 3.1.4. ja 3.1.5. tuuakse välja nende andmete töötlemisest kasu saavate osapoolte põhiõigused, mida riivatakse andmete säilitamata jätmisega.

Euroopa tasandil hakati andmete säilitamise ja inimõiguste tagamisega seonduvat õigusmaastikku kujundama 2014. aastal lahendiga *Digital Rights Ireland*. 21. detsembril 2016. tegi Euroopa Kohus lahendi *Tele2 Sverige*, milles arendati edasi lahendi *Digital Rights Ireland* seisukohti. Euroopa Kohus sedastas, et liikmesriikide sellised õigusnormid, näevad ette kohustuse säilitada üldiselt ja vahet tegemata kõikide abonentide ja registreeritud kasutajate kõik liiklusandmed ja asukohaandmed, olenemata kasutatud elektroonilise sidevahendi liigist, ja kohustavad elektroonilise side teenuste osutajaid neid andmeid süstemaatiliselt ja pidevalt säilitama, nägemata ette mingeid erandeid, on vastuolus direktiivi 2002/58 artikli 15 lõikega 1, harta artiklitega 7, 8 ja 11 ning artikli 52 lõikega 1.[185]

Asjaolule, et Euroopa tasemel on Euroopa Kohtu lahendite mõistmisega palju segadust, viitab ka eelotsusetaotluse esitanud riikide arv. Mitmete riikide[186] ülemkohtud või põhiseaduslikkuse

[185] EKo *Tele2 Sverige*, p 112.
[186] Prantsusmaa (C-511/18 ja C-512/18 *French Data Network, La Quadrature du Net*), Belgia (C-520/18 *Ordre des barreaux francophones et germanophone*), Eesti (C-746/18 *H. K. vs Prokuratuur*), Saksamaa (C-793 ja C-794/19 *SpaceNet*), Iirimaa (C-140/20 *Commissioner of the Garda Síochána*), Ühendkuningriik (C-623/17 *Privacy International*) ja Hispaania (C-207/16 *Ministerio Fiscal).*

järelevalve kohtud on Euroopa Kohtule esitanud eelotsusetaotlused, et saada selgust Euroopa Kohtu tõlgenduste osas. Nende eelotsusetaotluse esitamisega sai Euroopa Kohus järjekordse võimaluse kujundada kohtupraktikat elektroonilise side andmete säilitamise osas.

Kehtetuks tunnistatud direktiivi asemel reguleerib sideandmete säilitamisega seonduvat Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ[187]. 10. jaanuaril 2017. aastal avaldati e-privaatsuse määruse ettepanek, millega tahetakse asendada direktiivi 2002/58/EÜ. E-privaatsuse määrus on vajalik eelkõige selleks, et elektroonilise side teenuse kasutajatele oleks tagatud privaatsuse kõrge tase ning luua võrdsed võimalused kõigile turuosalistele.[188]

Kuivõrd direktiiv 2002/58/EÜ anti välja 2002. aastal, on tekkinud vajadus uue õigusakti järele, mis võtaks arvesse tehnoloogia arengut ning turu tegelikku olukorda. Tarbijad kasutavad traditsiooniliste sideteenuste alternatiivina üha uusi teenuseid. Tavaliste kõnede tegemise ja SMSide saatmise kõrval on võimalik nii kirjalikuks suhtluseks kui ka kõnede tegemiseks kasutada internetipõhiste teenuste ehk *over-the-*top (edaspidi OTT) teenuste pakkujate rakendusi nagu *Facebook Messenger, Viber, Telegram, Whatsapp, Signal* jne. Käesoleval hetkel ei rakendu OTT-teenuste pakkujatele Euroopa Liidus kehtiv elektroonilise side raamistik ega ka elektroonilise side seadus, mis samuti saadab signaali sellest, et OTT-teenuste pakkujaid ning traditsioonilisi sideettevõtjaid ei kohelda seaduse silmis võrdselt. E-privaatsuse määruse ettepaneku kohaselt hõlmab e-privaatsuse määruse kohaldamisala ka OTT-teenuse osutajaid, sest tagamaks privaatsuse ja side austamise tõhusat õiguskaitset, ei saa põhiõiguste kaitset jätta sektori enda reguleerida.

Muu hulgas leiti lahendis *Digital Rights Ireland*, et direktiiv 2006/24/EÜ rikub ebaproportsionaalselt Euroopa Liidu põhiõiguste harta artikleid 7 ja 8, mis sätestavad vastavalt era- ja perekonnaelu austamise ning isikuandmete kaitse. Artikkel 7 kohaselt on igaühel õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust. Artikkel 8 sätestab igaüheõiguse isikuandmete kaitsele. Puutuvalt põhiõiguste riivesse on põhilist lahendamist vajav küsimus, kuidas leida tasakaal ära hoidmaks isikute õiguste põhjendamatut riivet, ent sellegipoolest tagada kriminaalasja seisukohalt vajalike elektrooniliste tõendite efektiivne kogumine.

[187] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12.07.2002., milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv).
[188] *Ibid.*, põhjenduspunkt 1.1.

Lahendis *La Quadrature du Net* täpsustas Euroopa Kohus direktiiviga 2002/58/EÜ õigusi, mis on kaitstud harta artiklitega 7 ja 8. Kohus rõhutas direktiivi 2002/58/EÜ artiklis 6 ja põhjenduspunktides 22 ja 26 sätestatut, mille kohaselt liiklusandmete töötlemine on lubatud üksnes teenuste turustamise, nende eest arvete esitamise ja lisaväärtusteenuste osutamise jaoks vajalikul määral ja vajaliku aja jooksul. Pärast sellise aja möödumist on kohustus töödeldud ja salvestatud andmed kas kustutada või anonüümseks muuta. Puutuvalt muudesse asukohaandmetesse kui liiklusandmed, on neid lubatud töödelda vaid teatavatel tingimustel ja pärast nende anonüümseks muutmist või kasutajate või abonentide nõusolekul.[189] Eespool toodust tulenevalt on elektroonilise side vahendite kasutajatel põhimõtteliselt õigus eeldada, et nende side ja sellega seotud andmed jäävad anonüümseks ja neid ei salvestata ilma nendepoolse nõusoleku andmiseta.[190] Sellegipoolest ei tohi muutuda reegliks erand põhimõttelisest kohustusest tagada elektroonilise side ja sellega seotud andmete konfidentsiaalsus.[191]

Väljendatud seisukohast hoolimata ei tohi ära unustada, et direktiivi 2002/58/EÜ artikli 15 lg 1 võimaldab liikmesriikidel teha erandeid põhimõttelisest kohustusest tagada isikuandmete konfidentsiaalsus, kui selline piiramine on demokraatlikus ühiskonnas vajalik, otstarbekas ja proportsionaalne meede selleks, et tagada riigi julgeolek, riigikaitse ja avalik julgeolek või kuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamine, uurimine, avastamine ja kohtus menetlemine. Liikmesriikidel on lubatud võtta seadusandlikke meetmeid, millega sätestatakse andmete säilitamine piiratud aja jooksul, kui selleks esineb mõni mainitud põhjus.[192]

Euroopa Kohus on märkinud, et Euroopa Liidu põhiõiguste harta artiklites 7, 8 ja 11 väljendatud õigused ei ole absoluutsed eelisõigused.[193] See tähendab, et neid tuleb arvesse võtta kooskõlas nende funktsiooniga ühiskonnas.[194] Euroopa Liidu põhiõiguste harta artikkel 52 lõige 1 sätestab, et nimetatud artiklites väljendatud õiguste teostamist võib piirata, kui piirangud on ette nähtud seaduses, võtavad arvesse nende õiguste olemust, on proportsionaalsuse põhimõtet silmas pidades vajalikud ja vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või vajadusele kaitsta teiste isikute õigusi ja vabadusi.

Kuigi kohus sedastas, et artiklite 7, 8 ja 11 õiguste näol ei ole tegemist absoluutsete eelisõigustega, on sellegipoolest neid õigusi põhjendamatult riivavad sellised liikmesriigi

[189] EKo *La Quadrature du Net,* p 108.
[190] *Ibid*., p 109.
[191] *Ibid*., p 110.
[192] *Ibid.,* p 110.
[193] EKo *Privacy International,* p 63.
[194] EKo 16.07.2020, C-311/18. *Facebook Ireland,* p 172.

õigusnormid, mis kohustavad sideettevõtjaid riigi julgeoleku kaitsmise eesmärgil edastama üldiselt ja vahet tegemata liiklus- ja asukohaandmeid julgeoleku- ja luureteenistusele.[195]

Sideandmete säilitamise näol on tegemist põhiõiguste riivega, ent selline riive ei ole alati lubamatu. Harta artikli 52 lõike 1 kohaselt tohib hartaga tunnustatud õiguste ja vabaduste teostamist piirata ainult seadusega ning arvestades õiguste ja vabaduste olemust. Lähtuvalt proportsionaalsuse põhimõttest võib piiranguid seada üksnes siis, kui need on vajalikud ja vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi. Riigisisese õiguse kohaselt on riive põhiseadusega kooskõlas siis, kui see on formaalselt ja materiaalselt põhiseadusega kooskõlas.[196]

Puutuvalt elektroonilise side andmete säilitamisse, võivad liikmesriigid seadusega piirata isikute õigusi, kui õiguste piiramine on vajalik, otstarbekas ja proportsionaalne abinõu tagamaks riiklik julgeolek, riigikaitse, avalik kord, kuritegude või elektroonilise sidesüsteemi volitamata kasutamise ennetamine, uurimine, avastamine ja kohtus menetlemine. Liikmesriikidel on nimetatud eesmärkide saavutamiseks lubatud ette näha meetmeid nagu andmete säilitamine piiratud aja jooksul.[197]

3.1.1. Õigus era- ja perekonnaelu puutumatusele

Mõiste „õigus privaatsusele“ on midagi, mida pole sõna-sõnalt kirjas mitte üheski Eesti õigusaktis. Sellegipoolest hõlmab õigus era- ja perekonnaelu puutumatusele endas ka õigust privaatsusele. Privaatsusõigust tagab mitu rahvusvahelist õigusakti, nende seas ka EIÕK, mille artikli 8 punkt 1 sätestab igaüheõiguse sellele, et austataks tema era- ja perekonnaelu ja kodu ning korrespondentsi saladust. EIÕK-ga sarnane definitsioon on ka Euroopa Liidu põhiõiguste hartas, mille artikkel 7 sätestab, et igaühel on õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust.

Euroopa Liidu põhiõiguste harta artikkel 7 ekvivalent riigisiseses õiguses on põhiseaduse § 26, mis tagab igaühe õiguse perekonna- ja eraelu puutumatusele. Riigiasutustel, kohalikel omavalitsustel ja nende ametiisikutel ei ole lubatud kellegi perekonna- ega eraellu sekkuda muudel juhtudel, kui seaduses sätestatud korras kaitsmaks tervist, kõlblust, avalikku korda või

[195] EKo *Privacy International*, p 82.
[196] RKPJKo 3-4-1-5-05, p 7.
[197] Direktiiv 2002/58/EÜ, art 15 lg 1.

teiste inimeste õigusi ja vabadusi. Isikute perekonna- või eraellu võib sekkuda kuriteo tõkestamiseks või kurjategija tabamise eesmärkidel.[198]

Õiguskantsler on enda 2016. aasta elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise seaduspärasuse analüüsis leidnud, et sideettevõtja kohustus sideandmeid säilitada ESS § 111[1] alusel riivab eelkõige nimetatud paragrahvis sätestatud õigust perekonna- ja eraelu puutumatusele.[199]

3.1.2. Õigus isikuandmete kaitsele

Euroopa Liidu põhiõiguste harta artikkel 8 tagab eraldi õiguse isikuandmete kaitsele. Õigus isikuandmete kaitsele tõusetub elektroonilise side andmete säilitamise kontekstis seetõttu, et üksikisikud, kelle andmetele juurde pääsetakse, ei ole tihtipeale sellest isegi teadlikud.

Harta artikkel 8 lõike 2 kohaselt tuleb isikuandmeid töödelda asjakohaselt, kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Artikli 8 lõikega 2 on tagatud igaüheõigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist. Artikli 8 lõike 3 kohaselt kontrollib nimetatud sätete täitmist sõltumatu asutus.

Euroopa Kohus on korduvalt väljendanud seisukohta, mille kohaselt artiklite 7 ja 8 riived on omavahel tihedalt seotud.[200] Nimetatud seisukohad väljendavad põhimõtet, et riivates harta artikliga 7 tagatud õigust eraelu puutumatusele, riivatakse paratamatult ka artikliga 8 tagatud põhiõigust. Füüsilise isiku isikuandmetele nende säilitamise või kasutamise eesmärgil ligi pääsemine mõjutab selle isiku põhiõigust eraelu puutumatusele ning sellisel kujul andmetöötlus peab vastama artiklis 8 ette nähtud andmekaitsenõuetele, sest sel viisil andmete töötlemine kuulub artikkel 8 kohaldamisalasse.

Informatsioonilise enesemääramise õigust ei ole *expressis verbis* ühegi riigi põhiseaduses ega EIÕK-s sätestatud[201], ent õigus eraelu puutumatusele kätkeb endas ka informatsioonilist enesemääratlemise õigust. See tähendab, et inimesel on õigus otsustada, kas ja millisel määral tema isikuandmeid säilitatakse, kogutakse ja kasutatakse.[202] Teisisõnu, isikul peab säilima vaba

[198] PS § 26.
[199] Madise. Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus, lk 1.
[200] EKo *Facebook Ireland*, p 170-171, EKo *Digital Rights Ireland*, p 33-36.
[201] Kergandberg, E. *Per aspera ad fair trial*. – Juridica 2011/I, lk 75.
[202] Andmekaitse inspektsioon. Eraelu kaitse 31.10.2019. Arvutivõrgus kättesaadav: https://www.aki.ee/et/eraelu-kaitse/eraelu-kaitse, 12.01.2021

voli puutuvalt sellesse, mil määral tema eraelu kohta käivat informatsiooni saab avalikustada. Sarnaselt teistele põhiõigustele, ei ole ka nimetatud õigus absoluutne.[203]

Kuigi õigust isikuandmete kaitsele Eesti põhiseaduses eraldi õigusena sätestatud ei ole, hõlmab õigus eraelu puutumatusel ka õigust isikuandmete kaitsele. Konkreetsemalt aitab nimetatud õigust tagada isikuandmete kaitse seadus.

3.1.3. Õigus sõnavabadusele

Euroopa Liidu põhiõiguste harta artikli 11 kohaselt on igaühel õigus sõnavabadusele. See tähendab ka õigust arvamusvabadusele ning vabadust saada ja levitada teavet ja ideid avaliku võimu sekkumiseta ning sõltumata riigipiiridest. Samuti kätkeb nimetatud artikkel endas põhimõtet, mille kohaselt massiteabevahendite vabadust ja mitmekesisust austatakse. Ka EIÕK artikkel 10 sätestab õiguse sõnavabadusele.

Harta artikliga 11 tagatud õigusel sõnavabadusele on eriti suur tähtsus igas demokraatlikus ühiskonnas ja seda põhimõtet on Euroopa Kohus väga mitmetes lahendites juurutanud.[204] Õigus sõnavabadusele on üks demokraatliku ja pluralistliku ühiskonna alustaladest, mis peegeldab väärtusi, millel liit Euroopa Liidu lepingu[205] artikli 2 kohaselt rajaneb.[206]

Direktiivile 2006/24/EÜ ja andmete säilitamisele üleüldiselt heidetakse ette liigset väljendus- ja suhtlusvabaduse piiramist.[207] Kohtujurist P. C. Villalón tõi enda ettepanekus kohtuasjas *Digital Rights Ireland* välja, et direktiivi 2006/24/EÜ rakendamisega tekitatav üldlevinud tunne, et isikud on jälgimise all, võib avaldada mõju isikutele nende sõna- ja teabevabaduse teostamise perspektiivis.[208] Kuigi elektroonilise side andmete kogumine ja eelkõige säilitamine loob tingimused isikute tegevuse üksnes tagantjärele kontrollimiseks, on sellegipoolest tegu eraelu selge riivega.[209] Euroopa Kohus nõustus kohtujuristiga ja sedastas lahendis *Digital Rights Ireland*, et andmete säilitamine ja nende hilisem kasutamine ilma isikut, kelle kohta

---

[203] Andmekaitse inspektsioon, *Ibid.*
[204] EKo *Tele2 Sverige*, p 193. EKo 12.06.2003, C-112/00. *Eugen Schmidberger, Internationale Transporte und Planzüge vs Austria*, p 79. EKo 06.09.2011, C-163/10. *Aldo Patriciello*, p 31.
[205] Euroopa Liidu toimimise lepingu konsolideeritud versioon – ELT C 326, 26.10.2002.
[206] EKo 06.03.2001, C-274/99 P. *Bernard Conolly vs Commission of the European Communities.*
[207] Benedizione, L., Paris, E. – *Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive. – German Law Review* 2015/6, lk 1735.
[208] Kohtujuristi ettepanek, Pedro Cruz Villalón. Liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland* 12.12.2013, p 52. Arvutivõrgus kättesaadav: https://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=3594439, 10.03.2021.
[209] *Ibid*., p 72.

andmeid säilitati, teavitamata võib tekitada asjassepuutuvates isikutes tunde, et nende eraelu on pideva jälgimise all.[210] Selline konstantne jälgimine piirab asjassepuutuvate isikute väljendus- ja suhtlusvabadust.

Sõnavabaduse riive puhul ei ole oluline, kas säilitatud andmeid hiljem kasutatakse või mitte. Juurdepääs säilitatud andmetele kujutab nende potentsiaalsest hilisemast kasutamisest hoolimata sõnavabaduse eraldiseisvat riivet.[211] Riive hindamisel ei ole oluline, kas andmesubjektid on riive tõttu pidanud taluma ebamugavusi või mitte.[212]

Eestis on õigus sõnavabadusele tagatud põhiseaduse §-ga 45. Põhiseaduse § 45 kohaselt on igaühel õigus vabalt levitada ideid arvamusi, veendumusi ja muud informatsiooni sõnas, trükis, pildis või muul viisil.

3.1.4. Õigus riigi ja seaduse kaitsele

Eestis tagab õigust riigi ja seaduse kaitsele põhiseaduse § 13. Elektroonilise side andmete säilitamine võimaldab andmeid hiljem kriminaalmenetluses kasutada ning kuritegudes (kui ka Eestis väärtegudes) süüdi mõista. Kui kriminaalmenetluses kaob ära säilitatud sideandmete kasutamise võimalus, muutub raskemaks ka tõendite kogumine ning laiemas pildis süüdistuste esitamine. See toob kaasa kurjategijates karistamatuse tunde tekkimise. Samuti tunnevad sellisel juhul kannatanud end vähem kaitstuna. Euroopa nõukogu poolt läbi viidud uuringuga on leitud, et Euroopa Liidu kodanikud tunnevad tõusvat hirmu terrorismi, küberkuritegevuse ja organiseeritud kuritegevuse osas.[213]

3.1.5. Õigus elule

EIÕK artikkel 2 lõike 1 kohaselt kaitstakse igaühe õigust elule. Eestis on õigus elule tagatud PS §-ga 16. Õigus elule on kõige olulisem põhiõigus, sest see on eeldus kõigi teiste õiguste ja vabaduste kasutamisele.[214]

Andmete säilitamise vajadust on eelkõige põhjendatud terrorismi ja organiseeritud kuritegevuse vastase võitluse vajadusega.[215] Võttes arvesse, et terrorismi ja ka muude raskete

[210] EKo *Digital Rights Ireland*, p 37.
[211] EKo *La Quadrature du Net*, p 116.
[212] *Ibid*., p 115.
[213] *European Commission. Migration and Home Affairs. Europeans' attitudes towards cyber security*. 19.11.2017. Arvutivõrgus kättesaadav: https://ec.europa.eu/home-affairs/news/europeans'-attitudes-towards-cyber-security_en. 14.03.2021.
[214] Roosma, P. PSKomm § 16. – Madise, Ü. (peatoimetaja). Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas, täiendatud väljaanne. Tallinn: Juura 2012.
[215] Direktiiv 2006/24/EÜ, põhjenduspunkt 9.

kuritegude puhul võivad ohus olla paljude inimeste elud, siis seda enam lasub riigil vastutus selliste süütegude karistatavuse sätestamisele ja selliste kuritegude uurimise osas. Säilitatud andmete kasutamisega kriminaalmenetluses on võimalik efektiivselt menetleda (raskeid) kuritegusid ja ennetada terrorismikuritegusid. Võttes riigilt võimaluse säilitatud sideandmeid kasutada, vähendab see meetmeid, millega saab rahva kaitset ja elu tagada. See toob kaasa selle, et näiliselt on inimestele õigus elule tagatud, ent sisuliselt on riigil seda õigust raske tagada.

Eesti on lahendi *La Quadrature du Net* tarbeks edastatud seisukohtades rõhutanud sideandmete säilitamise tähtsust riigi julgeoleku tagamisel.[216] Nimelt on rõhutatud, et terrorismi vastu võitlemine on Eesti hinnangul lahutamatu osa riigi julgeoleku tagamisest. Julgeolekuasutuste poolt luure- ja vastuluurealase teabe kogumine ja töötlemine moodustab olulise osa riigi julgeoleku kaitse süsteemist, sest sellega tagatakse sõjaliste ja muude ohtude eelhoiatuse ja tundliku informatsiooni kaitstuse. Julgeoleku valdkonna toimimine sõltub informatsiooni kogumisest, töötlemisest, analüüsimisest ja selle põhjal järelduste tegemisest ning vajalike vastumeetmete võtmisest. Ka on rõhutatud, et riigi ühe tuumikfunktsiooni täitmisel on julgeolekuasutuste tegevuse eesmärk koguda riigi julgeolekupoliitiliste otsuste tegemiseks informatsiooni ning anda eelhoiatus võimalike riigivastaste, sh sõjaliste ja terroristlike rünnakute kohta. Eeltoodust tulenevalt on Eesti hinnangul tegemist vajaliku, otstarbeka ja proportsionaalse meetmega.[217]

Seisukohtades on välja toodud, et Euroopa Kohus ei ole seni andnud hinnangut, kas riigi julgeoleku kaitsmiseks võib andmeid säilitada ning kas massandmete säilitamine julgeoleku kaitsmise eesmärgil on vajalik, otstarbekas ja proportsionaalne meede.[218] Selle küsimuse lahendas Euroopa Kohus lahendis *La Quadrature du Net*, leides, et sideandmete säilitamine on lubatav, ent see võib toimuda ainult piiratud aja vältel, kui esinevad piisavalt konkreetsed asjaolud, mis võimaldavad asuda seisukohale, et asjaomane liikmesriik seisab silmitsi riigi julgeolekut ähvardava sellise suure ohuga.[219]

Euroopa Kohtu senistes lahendites on analüüsitud üksnes säilitatud sideandmete andmesubjekti riivatavaid õigusi. Käsitlemata on jäänud sideandmete säilitamise olulisus andmete töötlemisest huvitatud osapoolte vaatenurgast, kõrvutades julgeoleku ja turvalisuse aspektis. Riigi üks

[216] Eesti seisukohad Euroopa Kohtule liidetud eelotsusetaotluste C-511/18 (*La Quadrature du Net*) ja C-512/18 (*French Data Network*) ja eelotsusetaotluse C-520/18 (*Ordre des barreaux francophones et germanophone*) kohta. Eelnõu toimik nr 18-1233, lk 6. Arvutivõrgus kättesaadav: https://eelnoud.valitsus.ee/main/mount/docList/0226101f-9cd8-46e9-b80c-7dcd6ae7ccf8#4ZeWIn6z, 12.03.2021.
[217] *Ibid.*
[218] *Ibid.*
[219] Vt täpsemalt alapeatükis 2.3.

ülesandeid on võitlus kuritegevusega. See on oluline muu hulgas ka üksikisikute põhiõiguste ja -vabaduste tagamise seisukohalt. Põhiõiguste kaitse ja põhiseadusliku korra kaitse näol ei ole tegemist mitte vastas- vaid samasuunalise protsessiga. Isikute põhiõiguste kaitse ja riigi julgeolek kujutavad endast teineteist täiendavaid väärtusi.[220] Selmet omavahel vastandada põhiõigusi ja julgeolekut, tuleks nende vahel hoopis leida tasakaal.[221]

3.2. Sideandmete säilitamise põhiseaduspärasus

Sideandmete säilitamise regulatsiooni põhiseaduspärasust on hinnanud nii õiguskantsler enda 2015. aasta seisukohas[222], 2016. aasta seisukohas[223] kui ka Riigikohus vahetu normikontrolli raames[224]. Nimetatud põhiseaduspärasuse kontrolle tuleb lugeda läbi kriitikafiltri, sest nendes väljendatud seisukohad ei ole praegusel ajal enam Euroopa Kohtu ja Euroopa Inimõiguste Kohtu lahendites väljendatud põhimõtetega kooskõlas. Euroopa Inimõiguste Kohus käsitles lahendis *Copland vs the United Kingdom* isiku telefonikõnede, e-posti ja internetikasutuse riigipoolset seiret. Kohus jõudis järeldusele, et sellist eraelu puutumatuse piirangut saab vajalikuks pidada üksnes sellisel juhul, kui selle aluseks on asjakohane riigisisene õigusakt.[225] Kuivõrd Eestis kehtib ESS, millega võeti üle käesolevaks hetkeks Euroopa Kohtu poolt seitse aastat tagasi kehtetuks tunnistatud direktiiv, on päevakohane küsimus, kas ESS-i näol on endiselt tegemist põhiseaduspärase ja asjakohase õigusaktiga.

Riigikohus viis läbi vahetu normikontrolli ja lahendas küsimust tõendi lubatavuse kohta. Nimelt leidsid kaitsjad, et jälitustoimingu protokoll, millele tugines süüdimõistev otsus, on õigusvastaselt saadud, sest elektroonilise side andmete säilitamist sätestav regulatsioon on vastuolus Euroopa Liidu õigusega ning täpsemalt lahendiga *Digital Rights Ireland*.[226] Seejuures on nimetatud lahendi puhul tähtis silmas pidada, et vaidlusalused menetlustoimingud tehti enne *Digital Rights Ireland* lahendit.

---

[220] Goold, B. J., Lazarus, L. *Security and Human Rights: The Search for a Language of Reconciliation – Oxford: Hart Publishing* 2007, lk 2. Vt ka Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis, 2015. Arvutivõrgus kättesaadav: https://www.riigikohus.ee/sites/default/files/elfinder/õigusalased%20materjalid/pkk_jlitustegevuse_anals.pdf, 01.04.2021.

[221] Virks, K. Sideandmed ja nende säilitamise olulisus. – Juridica VIII/2018.

[222] Madise. Õiguskantsleri seisukoht elektroonilise side seaduse § 111^1 põhiseaduspärasuse kohta 20.07.2015. Arvutivõrgus kättesaadav: https://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf, 24.03.2021.

[223] Madise. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus.

[224] RKKKo 3-1-1-51-14.

[225] EIKo 03.07.2007, 62617/00. *Copland vs the United Kingdom,* p 48.

[226] RKKKo 3-1-1-51-14, p 19.

Kaitsjate etteheite adresseerimiseks analüüsis kohus, kas tollel ajal kehtinud KrMS § 117 alusel andmete kogumine üldkasutatavate tehniliste sidekanalite kaudu edastatavate sõnumite kohta on vastuolus põhiseadusega osas, mis võimaldab taotleda ja kasutada sideettevõtja andmeid kriminaalmenetluses.

Kohus leidis esmalt, et direktiivi 2006/24/EÜ kehtetus ei too automaatselt kaasa riigisisese regulatsiooni kehtetust. Kohtu ülesanne oli hinnata kitsast olukorda ehk kas riigisisesed õigusnormid, mis võimaldavad kindlustuskelmuse süüdistust puudutavas kriminaalmenetluses taotleda ja kasutada vastavaid andmeid, on kooskõlas põhiseadusega. Lõppjäreldusena leidis kohus, et tollel ajal andmete säilitamisega seonduvat reguleerinud KrMS § 117 ei ole vastuolus põhiseadusega ulatuses, mis võimaldab taotleda ja kasutada sideettevõtja andmeid kriminaalmenetluses.[227]

Kohus leidis, et andmete säilitamine ja kriminaalmenetluses kasutamine riivab õigust eraelu puutumatusele (PS § 26), ent selle õiguse piiramine on lubatud põhiseaduses sätestatud juhul. Kriminaalasjas sideettevõtjalt andmete välja nõudmine on sobiv meede seetõttu, et on efektiivne viis andmete kogumiseks isikute suhtlemise fakti ja viibimiskoha osas olukorras, kus selliste andmete kogumine muul moel kindel ega tagatud pole näiteks seetõttu, et sündmusel puuduvad muud tunnistajad või süüdistatavad keelduvad ütluste andmisest.[228]

Teo toimepanemise ajal oli sideettevõtjalt andmete nõudmise näol tegemist jälitustoiminguga. Kohus sedastas, et kuigi kindlustuskelmus oli teise astme kuritegu, oli seadusandja seda sellegipoolest hinnanud piisavalt raskeks kuriteoks, mille puhul olid lubatud jälitustoimingud.[229] Kohus tugevdas enda positsiooni ka argumendiga, mille kohaselt andmete saamine sideettevõtjalt oli jälitustoiming ning sellest tulenevalt kohaldusid sellele jälitustoimingu ja tõendi lubatavuse üldpõhimõtted, sh *ultima ratio* ehk viimase abinõu põhimõte, kohtulik järelkontroll ja kohustus jälitustoimingu subjekti põhiõiguste riivest tagantjärele teavitada.[230]

Lõpetuseks selgitas kohus, et ESS § 111^1 lg 4 alusel võib andmeid säilitada ühe aasta jooksul alates side toimumise ajast, käesolevas asjas säilitati andmeid 9 kuu vältel. Menetlejal oleks võimalik olnud kriminaalmenetluses säilitatud andmeid taotleda ka sõltumata riigi poolt pandud

[227] *Ibid*., p 24.
[228] *Ibid*., p 22.
[229] *Ibid*., p 22.1.
[230] *Ibid*., p 22.2.

säilitamiskohustusest, sest ka ettevõtja äriliste eesmärkidel olnuks kõnealuse jälitustoimingu tegemise objektiks olnud andmeid säilitatud vähemalt sellises ulatuses, et tuvastada, et jälitusprotokollis nimetatud ajal toimusid kõned süüdistatavate vahel.[231]

Tõendi ehk sideettevõtjalt saadud andmete protokolli lubatavus on teravalt päevakorras ka praegusel ajal, mil Euroopa Kohus on vahetult teinud otsuse asjas *H.K. vs Prokuratuur* ning sellest lahendist tulenevalt spekuleeritakse, et tuhandetes kriminaalmenetlustes võib suur hulk tõendeid arvestamata jääda.[232] 2021. aasta märtsi lõpus tegi Tartu Ringkonnakohus lahendi, mis võttis arvesse Euroopa Kohtu seisukohti. Kõnealuses kriminaalasjas väljastas prokurör loa sideandmete välja nõudmiseks ja saadud sideandmete pinnalt tekkinud kahtluste tõttu kuulati isiku telefoni pealt. Ringkonnakohus viitas Euroopa Kohtu lahendile C-746/18 ja rõhutas, et prokurör ei oleks tohtinud kohtueelses menetluses otsustada sideandmete ligipääsu üle. Sellest seisukohast tulenevalt tunnistas kohus maakohtu poolt antud loa pealtkuulamiseks õigustühiseks.[233]

Konkreetse juhtumi puhul ei saa enam tugineda lahendis 3-1-1-51-14 toodud andmete säilitamise ja kriminaalmenetluses kasutamise põhiseaduspärasuse analüüsile, sest suur erinevus nimetatud lahendi ja praegu regulatsiooni võrdluses on asjaolu, et sideettevõtjale andmete saamiseks päringu tegemine ei ole enam jälitustoiming, mis tähendab, et sellele ei kohaldu ka kohtu järelkontroll, samuti ei teavitata inimest tagantjärgi tema suhtes kogutud sideandmetest. Praeguse regulatsiooni alusel saab § 90^1 lõikes 1 olevaid andmeid menetleja küsida otse sideettevõtjalt ja § 90^1 lõikes 2 olevaid andmeid küsida kohtueelses menetluses prokuröri loal. Prokuröri loa alusel andmete saamine sideettevõtjalt on Euroopa Kohtu kriitika alla langenud.[234]

Töö autori hinnangul võib sideettevõtjalt saadud andmete kui tõendi lubatavus ohtu sattuda eelkõige sellises olukorras, kus tegemist on peamise tõendiga, millele kohus enda otsuse rajab. Samasugusele järeldusele on jõudnud ka Tallinna Ringkonnakohus haldusasjas, sedastades, et sideettevõtjalt saadud andmete kui tõendite lubamatuse tõttu ei kuulu maksuotsus osaliselt ega täielikult tühistamisele, sest maksuotsuse järeldusteni on võimalik jõuda ka neid tõendeid

[231] *Ibid.*, p 22.3.
[232] Aaspõllu, H. Tuhanded tõendid võivad kriminaalasjadest kaduda – ERR 03.03.2021. Arvutivõrgus kättesaadav: https://www.err.ee/1608129400/tuhanded-toendid-voivad-kriminaalasjadest-kaduda, 12.03.2021.
[233] Vahter, T. Uskumatu: abipolitseiniku pealtkuulamine läks täielikult lörri, kuigi prokurör täitis kehtivat seadust. – Eesti Ekspress 14.04.2021. Arvutivõrgus kättesaadav: https://ekspress.delfi.ee/number/93055705/artikkel/93111013/uskumatu-abipolitseiniku-pealtkuulamine-laks-taielikult-lorri-kuigi-prokuror-taitis-kehtivat-seadust, 14.04.2021.
[234] EKo *H.K. vs Prokuratuur*, p 59.

arvestamata. Kohus täpsustas, et sideettevõtjalt saadud andmete näol ei ole tegemist asja lahendamisel keskset tähtsust omavate tõenditega. Tegemist on üksnes selliste tõenditega, mis lisaks muudele tõenditele kinnitavad maksuhalduri kahtluse põhjendatust.[235] Euroopa Kohus näeb ühe võimalusena tõendi ebaseaduslikkuse arvesse võtmist karistuse kindlaksmääramisel ehk karistust tuleks selle arvelt vähendada.[236]

Selgitamaks, kas sideandmete säilitamise regulatsioon on põhiseaduspärane, tuleb hinnata formaalset ja materiaalset õiguspärasust. Formaalne kooskõla põhiseadusega tähendab, et põhiõigusi piirav õigustloov akt peab vastama pädevus-, menetlus- ja vorminõuetele ning määratuse ja seadusereservatsiooni põhimõtetele.[237] Varasemalt ei ole ei õiguskantsler[238] ega ühegi muu põhiseaduspärasuse kontrolli raames elektroonilise side seaduse formaalset õiguspärasust kahtluse alla seatud. Ka töö autori hinnangul ei ole põhjust kahelda, et ESS ei vasta formaalse põhiseaduspärasuse nõudele. Riigikogu on seaduse vastu võtnud järgides selleks ette nähtud protseduurireegleid ja ESS-i sätted andmete säilitamise osas on piisavalt õigusselged. Eeltoodust tulenevalt hinnatakse käesoleva töö raames sisuliselt üksnes materiaalset õiguspärasust.

Materiaalne põhiseaduspärasus tähendab, et põhiõigusi riivav õigusakt on kehtestatud põhiseadusega lubatava eesmärgi saavutamiseks ja on selle saavutamiseks proportsionaalne abinõu.[239] PS § 11 järgi saab põhiõigusi piirata üksnes kooskõlas põhiseadusega, tingimusel, et piirangud on demokraatlikus ühiskonnas vajalikud, ega moonuta piiratavate vabaduste ja õiguste olemust. Sellest tulenevalt peab põhiõiguste riivel olema põhiseadusega kooskõlas olev legitiimne eesmärk.[240]

a) Andmete säilitamise legitiimine eesmärk

Eespool on selgitatud, et Eestis on direktiiv 2006/24/EÜ üle võetud elektroonilise side seadusega, mille vastav redaktsioon jõustus 17.12.2007. ESS hakkas muu hulgas sätestama, mis liiki andmeid ning mis perioodi vältel sideettevõtjad säilitama peavad. Direktiiv 2006/24/EÜ sätestas eesmärgina ühtlustada teenusepakkujate kohustusi säilitada teatavaid sideandmeid selliselt, et oleks tagatud nende kättesaadavus vastavalt liikmesriikide riigisisesele

[235] TlnRnKo 3-16-183, p 18.
[236] EKo *La Quadrature du Net*, p 225.
[237] RKPJKo 3-4-1-5-05, p 8.
[238] Madise. Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus, lk 4.
[239] RKPJKo 3-4-1-16-08, p 28.
[240] RKPJKo 5-20-7/12, p 57.

õigusele määratletud raskete kuritegude uurimiseks, avastamiseks ja kohtus menetlemiseks.[241] Kuigi elektroonilise side seaduse muutmise eesmärk oli direktiivi üle võtmine riigisisesesse õigusesse, ei piirdunud seadusandja mitte üksnes direktiivi poolt ette nähtud miinimumnõuetega. Eesti seadusandja on lisaks raskete kuritegude uurimisele, avastamisele ja kohtus menetlemisele näinud ette võimaluse sideandmeid välja nõuda ka vähemraskete kuritegude tarbeks ning väärteo-, tsiviil- ja haldusmenetlustes.

Kuivõrd elektroonilise side andmete säilitamisega täidetakse vähemalt ühte andmete säilitamisega tagatavat eesmärki, milleks on raskete kuritegude uurimine, avastamine ja kohtus menetlemine, on tegemist legitiimse eesmärgiga.[242] Põhiõiguse riivet on võimalik õigustatuks pidada üksnes juhul, kui on järgitud proportsionaalsuse põhimõtet. Riive proportsionaalsuse hindamisel tuleb vaagida kolme aspekti, milleks on, kas riive on eesmärgi saavutamiseks sobiv, vajalik ja mõõdukas.[243]

a) Riive sobivus

Ebaproportsionaalne on selline abinõu, mis ei soodusta mitte ühegi eesmärgi saavutamist. Seega on sobiv meedet selline, mis soodustab eesmärgi saavutamist.[244] Kahtlemata saab pidada andmete säilitamist meetmeks, mis aitab kaasa raskete kuritegude uurimisele, avastamisele ja kohtus menetlemisele. Andmete säilitamine ESS §-s 111^1 sätestatud kujul on sobiv meede eespool nimetatud eesmärkide saavutamiseks.

b) Riive vajalikkus

Riigikohtu praktikast nähtub, et piirang on vajalik, kui eesmärki ei ole võimalik saavutada mõne teise sama efektiivse, ent isikut vähem koormava abinõuga.[245] Sellegipoolest on Euroopa Kohus ette heitnud, et võitlus raske kuritegevuse vastu on avaliku julgeoleku tagamiseks esmatähtis, ent selline eesmärk üksinda ei saa õigustada seda, et direktiiviga 2006/24/EÜ ette nähtud andmete säilitamist peetakse kuritegevusvastase võitluse jaoks vajalikuks.[246]

[241] Direktiiv 2006/24/EÜ, põhjenduspunkt 24, art 1 lg 1.
[242] Madise. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus., lk 5.
[243] RKPJKo 3-4-1-16-08, p 29.
[244] RKPJKo 3-4-1-1-02, p 15.
[245] *Ibid*.
[246] EKo *Digital Rights Ireland*, p 51.

Direktiivi 2006/24/EÜ kohaselt on sideandmed väärtuslikuks vahendiks kuritegevuse ja kuritegude, eriti organiseeritud kuritegevuse ennetamisel, uurimisel, avastamisel ja kohtus menetlemisel.[247] Euroopa Kohus nõustus selle seisukohaga, sedastades, et andmete säilimine pakub täiendavaid võimalusi raskete kuritegude lahendamiseks ning on seetõttu uurimise jaoks kasulik vahend.[248] Kohtuotsus *Digital Rights Ireland* on selle aspekti poolest langenud kriitika alla seetõttu, et sellisele järeldusele jõudmiseks ei kaalutud piisavalt andmete säilitamise regulatsiooni legitiimset eesmärki. Kohus ei tuginenud enda otsuses ei 2011. aasta Euroopa Nõukogu hindamisaruandele, ega muudele dokumentidele, mis andmete säilitamise efektiivsust analüüsivad.[249]

KrMS § 90^1 alusel tehtavat päringut võib teha üksnes siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Säilitatud andmete kasutamist kuritegude avastamise, uurimise ja kohtus menetlemise eesmärgil ei ole võimalik saavutada vähem riivava vahendiga.

c) Meetme mõõdukus

Õiguskantsler Ü. Madise on leidnud, et ESS-i §-st 111^1 tulenev eraelu puutumatuse riive on andmete säilitamise tasandil küllaltki kaalukas, ent kokkuvõtvalt siiski jõudnud järeldusele, et säilitamisest tulenevat riivet ei saa sideteenuse kasutaja jaoks lugeda väga intensiivseks.[250] Selline seisukoht on vastuolus Euroopa Kohtu praktikaga. Õiguskantsler Ü. Madise on muu hulgas põhistanud enda seisukohta sellega, et säilitamisele kuuluvate andmete liikide hulgas ei ole sõnumi sisu.[251] Euroopa Kohtu lahendite pinnalt saab muude kui sisuandmete säilitamise riivet ebaproportsionaalseks, ulatuslikuks ja raskeks pidada.

Euroopa Kohus on lahendi *Tele2 Sverige* punktis 99 leidnud, et sellised metaandmed nagu liiklus- ja asukohaandmed võimaldavad koostada väga täpse profiili sellest isikust, kelle andmeid säilitatakse. Liiklus- ja asukohaandmed sümbioosis võimaldavad teha väga täpseid järeldusi selliste isikute eraelu kohta, kelle andmeid säilitatakse. Näiteks on võimalik teha järeldusi nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad. Nii Euroopa Kohus kui ka kohtujurist Henrik Saugmandsgaard Øe on rõhutanud, et nende

[247] Direktiiv 2006/24/EÜ, põhjenduspunkt 7.
[248] EKo *Digital Rights Ireland*, p 49.
[249] Zubik, *et al.*, lk 22.
[250] Madise. Õiguskantsleri seisukoht elektroonilise side seaduse § 111^1 põhiseaduspärasuse kohta, lk-d 6 ja 9.
[251] *Ibid*., lk 9.

andmete põhjal on võimalik koostada asjaomaste isikute profiil, mis on õigust eraelu puutumatusele arvestades sama tundlik teave kui sideseansi sisu ise.[252]

Lahendis *La Quadrature du Net* kinnitas kohus varasemalt lahendis *Tele2 Sverige* väljendatud põhimõtet ning lisas, et liiklus- ja asukohaandmed võivad avaldada muu hulgas ka tundlikku teavet andmesubjektide kohta, nagu seksuaalne sättumus, poliitilised vaated, usulised, filosoofilised, ühiskondlikud või muud veendumused, samuti tervislik seisund.[253] Töö autori hinnangul omab liiklus- ja asukohaandmete säilitamine kahtlemata samasugust riivet nagu seda oleks sisuandmete säilitamise puhul, sest liiklus- ja asukohaandmete pinnalt on võimalik teha järeldusi sideseansi sisu kohta. Illustreerimaks eeltoodut, piisab järgmiste näidete puhul kõne sisu kohta järelduste tegemiseks ka üksnes kõne tegemise asukohta ja valitud numbreid analüüsides:

1. öösel kell 1:18 tehakse 25-minutiline kõne täiskasvanute teenuseid pakkuvale telefoniliinile. Kõne sisu koha saab järeldusi teha teadmata, mida täpselt räägiti;
2. kuigi kõnes räägitu jääb teadmata, on sellegipoolest võimalik teha järeldusi kahe järjestikkuse kõne sisu kohta, mis tehakse Türisalu pangalt esmalt eluliinile ning seejärel psühholoogilise kriisiabi telefonile;
3. on teada, et sama tunni jooksul helistas inimene nii günekoloogi numbrile kui seejärel Eesti Seksuaaltervise Liidu numbrile. Kuigi kõne sisuandmeid ei säilitata, on valitud numbrite põhjal tehtavad järeldused ühesed.

Samas leiab töö autor, et kõik Euroopa Kohtu otsustes väljendatud seisukohad ei pruugi Eesti tingimustes olulised olla. Ilmselt on Euroopa Kohus pidanud seksuaalse sättumuse kohta järelduste tegemise võimalikkuse all silmas neid suuri Euroopa linnu, kus on eraldi LGBT linnaosad ning sealsete mobiilmastide juures viibimine avaldab infot seksuaalsete sättumuste kohta. Kuivõrd Eestis selliseid linnaosasid ei ole, on raske Eesti oludes selle järeldusega nõustuda.

Abinõu mõõdukuse hindamisel tuleb kaaluda ühest küljest põhiõigusesesse sekkumise ulatust ja intensiivsust, teisest küljest aga eesmärgi tähtsust.[254] Õiguskantsler on riive mõõdukust õigustanud muu hulgas ka kuritegevuse vastase võitlusega.[255] Õiguskantsler ei ole analüüsinud

[252] EKo *Tele2 Sverige*, p 99. Kohtujuristi ettepanek, Henrik Saugmandsgaard Øe. Liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige*, p-d 253, 254 ja 257-259. 19.07.2016. Arvutivõrgus kättesaadav: https://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=5340634, 06.04.2021.
[253] EKo *La Quadrature du Net*, p 117.
[254] RKPJKo 3-4-1-1-02, p 15.
[255] Madise. Õiguskantsleri seisukoht elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta, lk 9.

kehtivat õiguslikku raamistikku, mis annab ESS § 111[1] laiad hoovad säilitatud sideandmete kasutamiseks ka muudel eesmärkidel peale kriminaalmenetluse. Kuivõrd andmete säilitamist oleks direktiivi 2006/24/EÜ kohaselt tohtinud ette näha üksnes raskete kuritegude avastamiseks ja ärahoidmiseks, siis ei saa lugeda andmete säilitamist proportsionaalseks meetmeks kõikide teiste ESS §-s 111[1] ettenähtud võimaluste[256] kasutamiseks. Elektroonilise side seaduse alusel säilitatud andmeid on lubatud kasutada ka väärteo- ja haldusmenetlustes, mis on tugevas vastuolus Euroopa Kohtu seisukohaga, mille kohaselt andmeid tohib säilitada ja kasutada üksnes raske kuritegevuse ja terrorismi vastu võitlemiseks. Säilitatud sideandmeid on lubatud Eestis kasutada ka näiteks kalakaitses, turvateenuse osutamiseks vajaliku tegevusloa taotlemiseks, finantsinspektsiooni järelevalve tegemiseks, maksudega seotud süüteomenetluses ja tsiviilõiguslike kindlustusvaidluste lahendamiseks.[257]

Eraldi kriitikat väärib juba mainitud õiguskantsleri seisukoht, mille kohaselt riive on tasakaalustatud objektiivse vajadusega kuritegevuse vastase võitluse osas. Võitlus kuritegevuse vastu on madal künnis, millega riivet õigustada. Ka Euroopa Kohus on selgitanud, liiklus- ja asukohaandmete säilitamist võib kasutada võitluses üksnes raske kuritegevusega ja andmete säilitamine on selle jaoks iseenesest sobiv vahend, ent direktiiviga 2006/24/EÜ seatud konkreetsed põhiõiguste piirangud on ebaproportsionaalsed.[258] Riive pole raske näiteks mobiilside seadme omaniku tuvastamisel ning selliste andmete kogumisel võib juurdepääsu põhjendada ka üldiselt kuritegude uurimise, ennetamise, avastamise ja menetlemise eesmärgiga.[259]

ESS-s puudub säte, mis kohustaks andmete töötlejat andmesubjekti töötlemise asjaolust teavitama. Kirjeldatud olukorda on teravalt kritiseerinud Euroopa Kohus, leides, et direktiiv 2006/24/EÜ kujutab endast harta artiklitega 7 ja 8 ette nähtud põhiõiguste ulatuste riivet, mida tuleb pidada eriti raskeks. Seda sel põhjusel, et andmesubjekti ei teavitata andmete säilitamisest ja nende hilisemast kasutamisest.[260]

[256] ESS § 111[1] lõike 4 kohaselt edastatakse andmeid väärteomenetluse seadustiku kohaselt ka Andmekaitse Inspektsioonile, Finantsinspektsioonile, Tarbijakaitse ja Tehnilise Järelevalve Ametile, Keskkonnaametile, Politsei- ja Piirivalveametile, Kaitsepolitseiametile ning Maksu- ja Tolliametile.
[257] Sehver, K, Ginter, C. Advokaadid: Kas teadsite, et Eesti riigiasutused koguvad ja kasutavad inimõigusi rikkudes suurt osa teie elektroonilise side andmeid? – Eesti Päevaleht 19.11.2017. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/80207790/advokaadid-kas-teadsite-et-eesti-riigiasutused-koguvad-ja-kasutavad-inimoigusi-rikkudes-suurt-osa-teie-elektroonilise-side-andmeid?, 03.01.2021.
[258] EKo *Digital Rights Ireland,* p 51.
[259] EKo *Ministerio Fiscal, p 57-58.*
[260] *Ibid*., p 37.

Samuti ei saa mõõdukaks pidada meedet, mis kohustab sideettevõtjaid säilitama andmeid kõikide sideteenuseid kasutavate inimeste kohta, ilma et nad oleks enda käitumisega kaasa toonud olukorra, kus oleks alust järeldada, et nad on kas või kaudselt seotud raskete kuritegudega või ohtu seadnud riigi julgeoleku. Seejuures säilitatakse andmeid ka nende isikute kohta, kelle sideseansid puudutavad ametisaladust. Euroopa Kohus on direktiivile 2006/24/EÜ ette heitnud, et see ei piira andmete säilitamist andmetega, mis kuuluvad kindlasse geograafilisse piirkonda.[261] Sätestades andmete säilitamisele geograafilisele kriteeriumi, peavad pädevad ametiasutused leidma objektiivsete asjaolude pinnalt, et ühes või mitmes geograafilises piirkonnas esineb kõrgendatud oht raskete kuritegude ettevalmistamiseks või toimepanemiseks.[262]

Geograafilise kriteeriumi olulisust rõhutav seisukoht ei ole Eesti väiksuse tõttu Eestile hästi üle kantav. Euroopa Kohtu seisukohast tulenevalt tuleks Eesti mõistes andmeid säilitada üksnes n-ö ohtlikemates piirkondades nagu utreeritult Lasnamäe ja Narva[263]. Euroopa Kohtu soovitus säilitada andmeid kindlas piirkonnas ei ole väga efektiivne meede. Nimelt on sellistes kriminaalsetes piirkondades elavatel isikutel võimalik minna kuritegusid toime panema n-ö turvalistesse piirkondadesse ja selline lahendus hakkaks soodustama olukorda, kus kurjategijad hakkaksid oma kõnesid tegema teises piirkonnas. See tekitab küsimuse, kas n-ö turvalisse piirkonda liikunud kurjategija andmeid ei säilitatagi.[264] Samuti diskrimineerib andmete säilitamine üksnes konkreetses geograafilises paigas sealseid teisi elanikke, kes ei ole ühtegi kuritegu toime pannud.

Kokkuvõtteks saab jõuda järeldusele, et Eestis kehtiv regulatsioon sideandmete säilitamise osas ei ole Euroopa Kohtu ja Euroopa Inimõiguste Kohtu seisukohti arvesse võttes põhiseaduspärane. Euroopa Kohus on rõhutanud põhimõtet, mille kohaselt sideandmete säilitamine ei tohi demokraatlikus ühiskonnas saada reegliks olukorras, kus direktiivis 2002/58/EÜ kehtestatud süsteem nõuab, et andmete säilitamine oleks erand.[265] ESS § 111[1] ei ole materiaalselt põhiseaduspärane seetõttu, et andmete üldine ja vahet tegemata säilitamine kõikide sideteenuseid kasutavate inimeste osas, samuti andmete säilitamine võimalusega neid

[261] *Ibid*., p 59.
[262] EKo *Tele2 Sverige*, p 111.
[263] 2020. aastal oli kuritegude arv 10 000 inimese kohta kõige kõrgem Ida-Virumaal. Allikas: Kuritegevus Eestis 2020. Kuritegevuse ülevaade. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevus2020/, 20.02.2021.
[264] Virks, K. Sideandmed ja nende säilitamise olulisus.
[265] EKo *Tele2 Sverige*, p 104, EKo *La Quadrature du Net*, p 142.

kasutada lisaks kriminaalmenetlusele ka tsiviil-, väärteo- ja haldusmenetluses, ei ole proportsionaalne abinõu kuritegude avastamiseks, uurimiseks ja kohtus menetlemiseks.

3.3. Ettepanekud riigisisese regulatsiooni muutmiseks

Võttes arvesse, et senine ESS alusel andmete üldine ja vahet tegemata säilitamine on vastuolus direktiiviga 2002/58/EÜ ja ka põhiseadusega, ootab andmete säilitamise regulatsiooni ees kauaoodatud reform. Eesti senine püüdlus elektroonilise side andmete säilitamisega seotud valdkonda reguleerida, on elektroonilise side seadusega direktiivi 2006/24/EÜ ülevõtmine. Kuigi 2014. aasta *Digital Rights Ireland* lahendiga tunnistati nimetatud direktiiv kehtetuks ning pärast *Digital Rights Ireland* lahendit on jõustunud veel mitu põhimõttelise tähtsusega lahendit Euroopa tasemel, on Eesti võtnud lähenemise mitte kiirustada seaduse muutmisega. Justiitsministeerium on väljendanud seisukohta, mille kohaselt enne seaduse muutmist soovitakse ära oodata Euroopa Liidu kohtu lõplik seisukoht[266] ning lõplikud juhised liikmesriikidele.[267] Sellest tulenevalt püsib endiselt jõus elektroonilise side seadus, mis on mitmete Euroopa Kohtu poolt sätestatud põhimõtetega vastuolus.

Nii Eesti kui ka iga teise Euroopa Liidu liikmesriigi eesmärk peaks olema luua regulatsioon, mis tagab tasakaalu ühest küljest isikute eraelu kindla kaitse ja teisest küljest efektiivse menetluse vahel. Euroopa Kohtu kohtupraktikast lähtuvalt tuleb riigisisese regulatsiooni muutmisel analüüsida järgmisi nüansse:

1) kuidas määratleda kuritegude raskusaste, millest alates on andmetele juurdepääs põhjendatud;

Euroopa Kohus on läbivalt enda lahendites juurutanud põhimõtet, millest johtuvalt on andmete säilitamine põhjendatud raskete kuritegude uurimiseks, avastamiseks ja ennetamiseks. Seejuures ei ole kohus andnud suuniseid, mis kvalifitseerub raske kuriteona ja mis mitte. Lahendis *Digital Rights Ireland* on sellegipoolest kohus pidanud raskeks kuriteoks organiseeritud kuritegevuse ja terrorismiga seotud kuritegusid.[268] Sarnane peata olek raske kuriteo künnise defineerimise osas valitses ka siis, kui liikmesriikidele nähti ette kohustus

[266] Käesoleval hetkel oodatakse veel näiteks Euroopa Kohtu lahendit liidetud kohtuasjades C-793/19 ja C-794/19 *SpaceNet* ning asjas C-140/20 *Commissioner of the Garda Síochána.*
[267] Süldre, L. A. Parmas: Euroopa Kohtu otsus võib mõjutada tuhandeid kriminaalmenetlusi – ERR 02.03.2021. Arvutivõrgus kättesaadav: https://www.err.ee/1608128344/parmas-euroopa-kohtu-otsus-voib-mojutada-tuhandeid-kriminaalmenetlusi, 16.03.2021.
[268] EKo *Digital Rights Ireland*, p 24.

direktiiv 2006/24/EÜ üle võtta riigisisesesse õigusesse. Mitmed riigid laiendasid raske kuriteo mõistet ka vähemohtlikele kuritegudele.[269]

Lahendis *Ministerio Fiscal* lahendati Hispaania eelotsusetaotlust. Tulenevalt ebaselgest olukorrast raskete kuritegude künnise osas, esitas Hispaania 14. aprillil 2016 Euroopa Kohtule eelotsusetaotluse, milles muu hulgas täpsustati, kas harta artiklites 7 ja 8 nimetatud põhiõiguste piiramise kriteerium kui kuritegude piisav raskus saab olla määratud lähtudes ainuüksi kuriteo eest ette nähtud karistustest või on lisaks vaja tuvastada ka asjaolu, et süüline tegevus on individuaalseid ja kollektiivseid õigushüvesid eriliselt kahjustava iseloomuga.[270] Hispaania karistusseadustikus on sätestatud, et rasked kuriteod on need, mille eest on seaduses ette nähtud rasked karistused. Seejuures on rasketeks karistusteks kas ennetähtaegse vabanemise võimalusega eluaegne vangistus või enam kui viieaastane vangistus.[271]

Euroopa Kohus ei andnud täpsemaid suuniseid, vaid üksnes leidis, et proportsionaalsuse põhimõtte järgi saab põhjendada rasket riivet kuritegude ennetamisel, uurimisel, avastamisel ja menetlemisel üksnes võitlusega sellise kuritegevuse vastu, mida tuleb samuti pidada „raskeks".[272] Võttes arvesse Euroopa Kohtu konservatiivset lähenemist andmete säilitamise osas, siis ei pruugi Eesti karistusseadustikus ka kõik I astme kuriteod kvalifitseeruda rasketeks kuritegudeks, rääkimata II astme kuritegudest või väärtegudest.

Välistatud ei ole variant, et raskete kuritegude piiritlemisel lähtub seadusandja Euroopa Liidu nõukogu raamotsusest Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta.[273] Nimetatud raamotsuses loetletud kuriteod on toodud lisas 1. Seejuures tuleb tähele panna, et kõik raamotsuses toodud kuriteod ei ole Eesti karistusseadustikus I astme kuriteod.[274] Seisukohale, et raamotsuses nr 2002/584/JSK toodud kuritegude loetelu võidakse aluseks võtta raskete kuritegude piiritlemisel, on võimalik asuda näiteks selle pinnalt, et mitmed muud õigusaktid on samuti sellele loetelule tuginenud.[275]

---

[269] Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. – Juridica X/2015.
[270] EKo *Ministerio Fiscal*, p 26, küsimus 1.
[271] *Ibid*., p 13 ja 14.
[272] *Ibid*., p 56.
[273] Nõukogu raamotsus 2002/584/JSK, 13.06.2002 Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta, L 190/1.
[274] Näiteks on loetelus mitmeid II astme kuritegusid nagu kelmus (KarS § 209) ja rahapesu (KarS § 394 lg 1).
[275] Näiteks Nõukogu raamotsus 2006/783/JSK, 6.10.2006, konfiskeerimisotsuste suhtes vastastikuse tunnustamise põhimõtte kohaldamise kohta, Nõukogu raamotsus 2008/947/JSK, 27.11.2008, vastastikuse tunnustamise põhimõtte kohaldamise kohta kohtuotsuste ja vangistuse tingimisi kohaldamata jätmist käsitlevate otsuste suhtes, et teostada tingimuslike meetmete ja alternatiivsete mõjutusvahendite järelevalvet, Nõukogu raamotsus 2008/909/JSK, 27.11.2008, vastastikuse tunnustamise põhimõtte kohaldamise kohta kriminaalasjades tehtud

Võttes arvesse, et elektroonilise side andmeid peaks saama säilitada ja kasutada üksnes raskete kuritegude uurimiseks, avastamiseks ennetamiseks ja julgeoleku tagamiseks, siis muutub teatud kuritegude tõendamine tulevikus keerukaks. Raske kuriteo kriteeriumist lähtudes kaob pärast Eesti riigisiseste seaduste Euroopa Kohtu praktikaga kooskõlla viimist ära võimalus kasutada elektroonilise side andmeid selliste kuritegude lahendamiseks nagu näiteks ahistav jälitamine[276]. Autori hinnangul lahendatakse ahistava jälitamise kaasused tavapäraselt tuginedes kõneeristusele, ent tulevikus muutub selle kuriteoliigi tõendamine väga keeruliseks, kuivõrd kõneeristus on nendes kaasustes üks väheseid objektiivseid tõendeid. Samuti on tulevikus ilmselt välistatud nn koeravorsti varaste püüdmine sideandmete abil.

2) kuidas täpsustada objektiivseid kriteeriume, mille alusel tuleks määrata andmete säilitamise aeg, et tagada selle piirdumine vältimatult vajalikuga;

Üks võimalik variant andmete säilitamise perioodi määramiseks on andmete konfidentsiaalsusaste. Euroopa Kohus on rõhutanud, et liiklus- ja asukohaandmete järgi on võimalik teha isiku ja tema eraelu kohta väga täpseid järeldusi ning sellest tulenevalt on need sama tundlikud kui sisuandmed. Abonendiandmed on võrreldes teiste andmete liikidega kõige vähem tundlikud. Üks lahendus oleks määrata erinevate andmete säilitamise ajad nende tundlikkusastme järgi selliselt, et abonendiandmeid kui vähem tundlikku liiki on võimalik säilitada nii pikema perioodi vältel kui ka nende kuritegude uurimise jaoks, mis ei kvalifitseeru raskete kuritegudena. Abonendiandmeid (näiteks nagu kliendi nimi, tema aadress ja kliendi kasutuses olev telefoninumber) peab sideettevõtja niigi säilitama terve kliendisuhte perioodi vältel, teadmaks, kes on teenust kasutanud ja kellele tuleb arve esitada[277]. Ka pärast kliendisuhte lõpetamist säilitavad sideettevõtjad andmeid teatud perioodi vältel, et lahendada näiteks võlgnevuste sissenõudmisega seonduvaid vaidlusi.[278] Seevastu liiklus- ja asukohaandmeid kui tundlikumat andmete liiki tuleks säilitada lühema perioodi jooksul.

3) arvesse tuleb võtta, et sõltumatu asutusena sideandmetele juurdepääsuks loa andmiseks ei saa käsitleda prokuratuuri;

---

otsuste suhtes, millega määratakse vabadusekaotuslikud karistused või vabadust piiravad meetmed, nende Euroopa Liidus täideviimise eesmärgil.

[276] KarS § 157[3].

[277] Elisa kliendiandmete töötlemise põhimõtted. Isikuandmete töötlemise õiguslik alus ja eesmärgid, p 3.3.1.8. Arvutivõrgus kättesaadav: https://www.elisa.ee/files/elisast/tingimused-ja-hinnakirjad/mobiilside-teenused/andmekaitse/ELISA_KLIENDIANDMETE_TOOTLEMISE_POHIMOTTED.pdf, 06.04.2021.

[278] Telia Eesti AS üldtingimused. Lisa: Telia Eesti AS-i andmete kasutamise põhimõtted, p 6.1.14. Arvutivõrgus kättesaadav: https://www.telia.ee/images/documents/lepingud/lepingud-ja-tingimused/telia_eesti_as_andmete_kasutamise_pohimotted_est.pdf, 06.04.2021.

Lahendis *H. K. vs Prokuratuur* vaagis Euroopa Kohus küsimust, kas direktiiviga 2002/58/EÜ ja hartaga on vastuolus riigisisesed õigusnormid, mis annavad prokurörile pädevuse anda ametiasutusele kriminaaluurimise läbiviimiseks liiklus- ja asukohaandmetele juurdepääsu luba.[279] Juba varasemas lahendis on kohus selgitanud, et juurdepääsu tagamine andmetele sõltumatu asutuse poolt on oluline tegur üksikisikute kaitsmisel.[280] Sellegipoolest ei olnud kuni lahendini *H. K. vs Prokuratuur* võimalik jõuda seisukohale, kas Eesti prokuratuur on selline sõltumatu asutus Euroopa Kohtu seisukohtade mõttes. Liikmesriikidel on väga erinevad õiguskaitsesüsteemid ning ühes riigis sõltumatuks asutuseks peetav asutus ei pruugi kvalifitseeruda sõltumatu asutusena teises riigis. Lahendis *H. K. vs Prokuratuur* lahendas Euroopa Kohus sõltumatu asutuse kriteeriumite küsimust konkreetselt Eesti prokuratuuri pinnalt, hinnates prokuratuuri ülesandeid ja kohustusi.

Lahendis *La Quadrature du Net* on kohus selgitanud, et riigi pädevate asutuste juurdepääs säilitatud andmetele peab olema allutatud kohtu või sõltumatu haldusasutuse teostatavale eelkontrollile.[281] Selline sõltumatu eelkontrolli teostav asutus peab olema andmetele juurdepääsu taotleva asutuse suhtes kolmas isik.[282] Kohtujurist G. Pitruzzella arvamuse kohaselt tagab asutuse sõltumatuse kaks nõuet. Esiteks ei tohi see asutus olla allutatud väljastpoolt tulenevale survele, mis võiks otsuseid mõjutada. Teiseks peab sellise asutuse poolt teostatav kontroll olema objektiivne ja peab olema tagatud asutuse erapooletus.[283] Kohtujurist lisas, et andmete juurdepääsu eelneva kontrolli eest vastutav asutus ei tohiks olla seotud kõnealuse kriminaaluurimisega ja ta peab omama kriminaalmenetluse poolte suhtes neutraalset positsiooni.[284] Nimetatud põhimõtteid rõhutas ka Euroopa Kohus enda lahendis.[285] Eesti tundub liikuvat selle variandi suunas, mis mitmes teises Euroopa riigis kasutusel on – lubade väljastamine eeluurimiskohtuniku poolt.[286]

Võttes arvesse, et Euroopa Kohus leidis, et Eesti prokuratuur ei ole see sõltumatu haldusasutus, mis tohiks kohtueelses menetluses otsustada sideandmete väljanõudmiseks vajaminevate lubade andmise üle, siis tõstatab see küsimuse, kas tuleks üle vaadata kehtiv regulatsioon ka

[279] EKo *H.K. vs Prokuratuur*, p 46.
[280] EKo *Digital Rights Ireland*, p 68.
[281] EKo *La Quadrature du Net*, p 188.
[282] EKo *H.K. vs Prokuratuur*, p 54.
[283] Kohtujuristi ettepanek, Giovanni Pitruzzella. Kohtuasi C-746/18, *H.K. vs Prokuratuur*. 21.01.2020 Arvutivõrgus kättesaadav: https://curia.europa.eu/juris/document/document.jsf?text=&docid=222421&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=2250180, 15.03.2021.
[284] Kohtujuristi ettepanek, G. Pitruzzella. Kohtuasi C-746/18, *H. K. vs Prokuratuur*, p 125.
[285] EKo *H. K. vs Prokuratuur*, p-d 52 ja 54.
[286] Aaspõllu, H. Tuhanded tõendid võivad kriminaalasjadest kaduda.

muus osas. Nimelt on prokuratuuril KrMS § 126^5 kohaselt õigus anda luba kaheks kuuks isiku, asja või paikkonna varjatud jälgimiseks, võrdlusmaterjali varjatud kogumiseks ja esmauuringute tegemiseks ning asja varjatud läbivaatamiseks või asendamiseks. Kui Euroopa Kohtu hinnangul ei ole prokuratuur sõltumatu haldusasutus sideettevõtjalt andmete nõudmiseks antavate lubade osas, siis Euroopa Kohtu seisukohtade kohaselt ei tohiks prokuratuur ilmselt anda lubasid ka varjatud jälgimise teostamise jaoks.

4) reguleerimist vajab andmete kustutamine pärast seda kui on ära langenud nende säilitamise vajadus;

Direktiivist 2002/58/EÜ tuleb kohustus liiklus- ja asukohaandmed kustutada või anonüümseks muuta pärast seda, kui on ära langenud vajalikkus edastuse toimumiseks. Ka kohtupraktikas on rõhutatud andmete kustutamist pärast säilitamisperioodi lõppu kui ühte olulist tagatist.

5) andmesubjekti teavitamine andmete säilitamisest ja kasutamisest;

Kehtivate seaduste kohaselt on andmesubjektil võimalus teada saada tema kohta säilitatud andmetest ja nende edasisest kasutamisest, ent teavitamiskohustust seadus ei sätesta. Nimelt saab andmesubjekt tema osas tehtud päringust teada vaid siis, kui päringust saadav info vormistatakse tõendina ning see lisatakse kriminaalasja materjalide juurde. Kui päring tehakse, ent saadud andmeid kriminaaltoimikusse ei lisata, siis ei saa andmesubjekt ka tema kohta kogutud andmetest teada. Selline olukord ei ole kooskõlas Euroopa Kohtu praktikaga, kus on rõhutatud andmesubjekti tema kohta käivate andmete säilitamise ja kasutamise teavitamise olulisust.

Olukorras, kus andmete säilitamine pärast riigisiseste õigusnormide Euroopa Liidu õigusega kooskõlla viimist siiski alles jääb, peaks andmete üldisest säilitamisest teavitamine sideettevõtja poolt olema kirjas kliendilepingus. Juhul, kui säilitatud andmeid kasutatakse kriminaalmenetluses, tuleks igal juhul kehtestada kohustus andmesubjekti teavitamisest andmete kasutamisest menetluse lõpetamisel ja ka siis, kui andmeid on kogutud, ent mitte kriminaaltoimikusse lisatud. Kui menetlus peaks jõudma kohtumenetluse faasi, siis saab andmesubjekt teada tema kohta kogutud andmetest kriminaaltoimikuga tutvumisel. Kui aga menetlus lõpetatakse, siis puudub andmesubjektil kriminaaltoimikuga tutvumise etapp ning sellest tulenevalt on oluline ka sellise stsenaariumi puhul andmesubjekti teavitamine.

Kuigi alates 2013. aastast ei ole ettevõtjale sideandmete andmete saamiseks päringu tegemine enam käsitletav jälitustoiminguna, tuleb seaduse Euroopa Kohtu põhimõtetega kooskõlla viimiseks kehtestada osaliselt samad menetlusgarantiid, mis kehtivad ka jälitustoimingute puhul. Riigikohus on sedastanud, et põhiõiguste riive kaasneb lisaks jälitustoimingu tegemisega ka jälitustoimingust saadud andmete töötlemisega (sh säilitamisega) ja jälitustoimingust teavitamata jätmisega.[287] Pärast seda kui sideettevõtjale päringu tegemine ei ole enam käsitletav mitte jälitus- vaid menetlustoiminguna, kadus ära teavitamiskohustus, ent Euroopa Kohtu põhimõtted toovad teavitamiskohustuse riigisisesesse õigusesse tagasi.

6) millised sideandmete säilitamise põhimõtted peaksid rakenduma, et oleks tagatud sideandmete säilitamisega kaasneva riive proportsionaalsus.

Eelkõige peaks seadusandja kaaluma etteheiteid, mida tegi Euroopa Kohus direktiivile 2006/24/EÜ. Kuigi nimetatud direktiivi eesmärgiks oli võitlus raske kuritegevuse vastu, ei nõudnud direktiiv mingi seose olemasolu säilitatavate andmete ja ohu vahel avalikule julgeolekule. Etteheite kohaselt ei piiranud see "andmete säilitamist andmetega, mis kuuluvad kindlasse ajavahemikku ja/või kindlasse geograafilisse piirkonda ja/või teatavatele isikutele, kes võivad olla mingil viisil seotud raske kuriteoga, või isikutega, kelle andmete säilitamine võib muul põhjusel kaasa aidata raskete kuritegude ennetamisele, avastamisele või menetlemisele."[288]

Andmete säilitamise alternatiivina on võimalik kaaluda andmete kiirsalvestamist (ingl ka *quick freeze*). Andmete kiirsalvestamise puhul on sideettevõtjal kohtumääruse esitamise korral kohustus säilitada ainult konkreetsete, kuritegevuses kahtlustatavate isikute andmed alates kuupäevast, mil andmete kiirsalvestamise määrus esitati. Samuti on välja töötatud *quick-freeze plus,* mis on andmete kiirsalvestamisest ulatuslikum, sest kohtuniku korraldusel on võimalik juurde pääseda ka sellistele andmetele, mida sideettevõtjad veel kustutanud ei ole. Ühest küljest on leitud, et andmete kiirsalvestamine riivab õigust eraelu puutumatusele vähem kui andmete säilitamine. Teisest küljest ei suuda andmete kiirsalvestamine piisavalt andmete säilitamist asendada. Andmete kiirsalvestamine ei taga võimalust koguda tõendeid piisava perioodi kohta enne kiirsalvestamise väljastamist. Samuti ei võimala kiirsalvestamine koguda tõendeid kuriteo ohvrite või tunnistajate liikumise kohta.[289]

[287] RKPJKo 3-4-1-42-13, p 57.
[288] EKo *Digital Rights Ireland,* p 59.
[289] *European Commission. Report from the commission to the council and the European Parliament. Evaluation report on the Data Retention Directive* (*Directive* 2006/24/EC).

Kuivõrd Euroopa Kohus on sedastanud, et sideandmete laussäilitamine on liidu õigusega kooskõlas ja piiratud üksnes väga piiritletud juhtudel[290], tuleb Eesti seadusandjal kaaluda muid variante nagu *quick freeze* ja isikuliselt, ajaliselt ning geograafiliselt eristatud andmete säilitamine. Viimasena mainitud lähenemise kitsaskoht on see, et praktikas ei ole teada, kuidas võiks välja näha andmete sihistatud kogumine, sest ei ole ette teada, kes ja millal paneb toime kuriteo, et saaks just selle konkreetse inimese andmeid salvestada.[291] Mitte ükski riik ei suuda ette näha, milliseid andmeid raskete kuritegude lahendamiseks vaja võib minna ja sellest tulenevalt neid eelnevalt säilitada.

Lahendist *La Quadrature du Net* tulenevate seisukohtade järgi on andmete üldine ja vahet tegemata säilitamine siiski lubatud järgnevatel põhjustel:

a) IP-aadresse võib üldiselt ja vahet tegemata säilitada riigi julgeoleku kaitsmise, raskete kuritegude vastu võitlemise ja avalikku julgeolekut ähvardava suure ohu ennetamise eesmärgil ajavahemikuks, mis on piiratud tingimata vajalikuga;
b) elektroonilise side vahendite kasutajate identiteediga seotud andmeid (nt nimi, kontaktandmed, e-postiaadress ja aadress) võib üldiselt ja vahet tegemata säilitada riigi julgeoleku kaitsmise, kuritegevuse vastu võitlemise ja avaliku julgeoleku kaitsmise eesmärgil;
c) sideettevõtjale võib riigi julgeoleku kaitse eesmärgil teha ettekirjutuse säilitada liiklus- ja asukohaandmeid üldiselt ja vahet tegemata olukordades, kus liikmesriik seisab silmitsi riigi julgeolekut ähvardava suure ohuga, mis osutub tõeliseks ja vahetuks või ettearvatavaks.[292]

Samuti on lahendi *Ministerio Fiscal* kohaselt lubatud välja nõuda mobiilside seadme omaniku tuvastamiseks vajalikke andmeid nagu ees- ja perekonnanimi ning aadress, ilma et nendele andmetele juurdepääsu peaks põhistama raske kuritegevuse vastase võitluse eesmärgiga. Kuna nimetatud andmetele juurdepääsuga ei kaasne rasket riivet, siis piisab nende välja nõudmiseks ka üldisest eesmärgist kuritegusid ennetada, uurida, avastada ja menetleda.

Euroopa Kohtu seisukohtadest lähtuvalt peab Eesti seadusandja otsustama seadust muutes, kas ja millist liiki sideandmete säilitamine on vajalik ning millised sideandmete säilitamise

[290] Seisukohad lahendis *La Quadrature du Net,* p 229.
[291] Siitam-Nyiri, K. Kristel Siitam-Nyiri: advokaadid kasutavad sideandmete kogumisest rääkides kunstilisi liialdusi – Eesti Päevaleht, 20.11.2017. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/80211168/kristel-siitam-nyiri-advokaadid-kasutavad-sideandmete-kogumisest-raakides-kunstilisi-liialdusi, 02.02.2021.
[292] EKo *La Quadrature du Net,* p 229.

põhimõtted peaksid kehtima, et oleks tagatud kuldne kesktee andmete säilitamise ja põhiõiguste tagamise vahel ning et sideandmete säilitamisega kaasnev riive oleks proportsionaalne.

KOKKUVÕTE

21. sajandi tähtsaim vara on andmed. See printsiip kehtib ka kriminaalmenetluses, kus andmetena käesoleva magistritöö raames peetakse eelkõige silmas elektroonilise side metaandmeid. Seejuures on omakorda tähtis silmas pidada, et Euroopa Kohus on elektroonilise side andmetena käsitlenud liiklus- ja asukohaandmeid.

Elektroonilise side seansi jooksul saavad tekkida nii sisu- kui ka metaandmed ning selleks, et menetleja saaks metaandmetele ligi, on esmalt vaja tagada, et üldse oleks olemas need andmed, millele juurdepääsu tahetakse. Selle jaoks on seadusandja riigisisesesse õigusesse direktiivi 2006/24/EÜ üle võtnud 17.12.2007 jõustunud elektroonilise side seadusega, millega on telekommunikatsioonieettevõtjatele kehtestatud kohustus säilitada kõiki sideandmeid (välja arvatud sisuandmeid) ühe aasta jooksul alates side tekkimise ajast.

Euroopa Kohus kuulutas 2014. aasta lahendiga *Digital Rights Ireland* direktiivi 2006/24/EÜ tagasiulatuvalt kehtetuks. Ka seitse aastat pärast nimetatud lahendit on Eesti nende riikide seas, kes ei ole riigisisest õigusakti, millega direktiiv üle võeti, kehtetuks tunnistanud või vähemalt sideandmete säilitamist puudutavaid sätteid Euroopa Liidu õigusega kooskõlla viinud.

Kehtetuks tunnistatud direktiiv 2006/24/EÜ nägi ette, et liikmesriigid saavad sideettevõtjatele panna kohustuse säilitada metaandmeid perioodil kuus kuud kuni kaks aastat. Magistritöö kirjutamise hetkel on mitte üksnes riigid Euroopa tasemel, vaid ka maailma mastaabis andmete säilitamise osas polariseerunud seisukohtadel. Seda väidet illustreerib olukord Austraalias, kus sideettevõtjad on kohustatud metaandmeid säilitama kaks aastat. Seevastu Euroopas puudub mitmetes riikides nagu Austria, Saksamaa ja Sloveenia sideettevõtjatel kohustus õiguskaitseorganite tarbeks andmeid säilitada ja õiguskaitseorganid saavad välja nõuda üksnes neid andmeid, mida sideettevõtjad on enda tarbeks ärilistel eesmärkidel talletanud. Kontrastina – enne lahendit *Privacy International* kehtis Suurbritannias sideettevõtjatele kohustus automaatselt edastada kõik säilitatud sideandmed julgeoleku- ja luureteenistustele.

Magistritöö eesmärgiks oli välja selgitada, kas kehtiv elektroonilise side seadus on põhiseaduspärane ja kas ning kuidas võimaldab Euroopa Kohtu sidevaldkonna praktikast tulenev raamistik tulemuslikult läbi viia menetlusi, samas tagades puudutatud isikute põhiõigused. Püstitatud hüpoteesi kohaselt riivab käesoleval hetkel kehtiv elektroonilise side seadus ebaproportsionaalselt isikute põhiõigusi ja ei ole sellest tulenevalt põhiseaduspärane ega kooskõlas Euroopa Liidu õigusega. Euroopa Kohtu sideandmete säilitamist puudutavad

lahendid on peamise fookuse seadnud põhiõiguste tagamisele ja õiguskaitseasutustele väga laiasid hoovasid kätte ei anna.

Erinevalt senisest õiguskantsleri ja Riigikohtu seisukohast tuleks leida, et tänasel päeval ei saa ESS-i põhiseaduspärasust jaatada. Puutuvalt andmete säilitamisega riivatavatesse põhiõigustesse ei tohi ära unustada, et kuigi andmete säilitamisega riivatakse andmesubjektide õigusi, siis andmete säilitamata jätmisega riivatakse teisest küljest andmete töötlemisest kasu saavate osapoolte huvisid. Kuivõrd riigil lasub kohustus tagada enda rahva ja nende elude kaitse ja võttes arvesse, et isikute põhiõiguste kaitse ning riigi julgeolek kujutavad endast täiendavaid väärtusi, siis selmet vastandada põhiõigusi ja julgeolekut, tuleks nende vahel hoopis leida tasakaal.

Andmete säilitamise regulatsioon ei ole põhiseaduspärane, sest andmete säilitamisega kaasnev riive on ebamõõdukas. Direktiiv 2006/24/EÜ, mis võeti üle elektroonilise side seadusega, nägi ette andmete säilitamist üksnes raskete kuritegude avastamiseks ja ärahoidmiseks. Kuigi elektroonilise side andmete säilitamine aitab tagada ka raskete kuritegude avastamist ja kohtus menetlemist, ei ole laussäilitamine selle jaoks siiski proportsionaalne meede. Samuti puudub ESS-s säte, mis kohustaks andmete töötlejat andmesubjekti töötlemise asjaolust teavitama. Demokraatlikus ühiskonnas ei tohi saada reegliks üldine andmete säilitamine olukorras, kus direktiivis 2002/58/EÜ kehtestatud süsteem nõuab, et andmete säilitamine oleks erand.

Metaandmete säilitamise kohustus ja nende hilisem kriminaalmenetluses kasutamise võimalikkus on menetluste läbiviimise seisukohalt olulise tähtsusega. Euroopa Kohus on sedastanud, et sideandmed on uurimise jaoks kasulik vahend, sest need pakuvad riigisisestele õiguskaitseorganitele täiendavaid võimalusi raskete kuritegude lahendamiseks.[293] Ka Riigikohus on rõhutanud elektroonilise side metaandmete säilitamise tähtsust, leides, et elektroonilise side andmete kogumine sideettevõtjalt on efektiivne meede saamaks objektiivseid tõendeid isikute suhtlemise fakti ja viibimiskoha kohta.[294] Metaandmete kasutamise olulist illustreerib ka Veronika Dari mõrva juhtum ja Juri Ustimenko pommiplahvatuse kaasus, kus just kõneeristuse tegemise pinnalt oli võimalik mõlemas menetluses lahenduseni jõuda.[295]

[293] EKo *Digital Rights Ireland*, p 49.
[294] RKKKo 3-1-1-51-14, p 22.
[295] Lamp, Anvelt. Eesti roimad. Koolitüdruk Veronika Dari tapmise tõe paljastas üks pisiasi – Elu24 15.04.2021. Arvutivõrgus kättesaadav: https://www.elu24.ee/7224532/koolitudruk-veronika-dari-morva-poleks-ehk-avastatud-kui-poleks-olnud-uht-pisiasja, 16.04.2021.

Sideettevõtjalt saadud metaandmeid on võimalik kasutada kas iseseisva tõendina või nende pinnalt koguda muid tõendeid. Kuigi metaandmete säilitamine ning nende hilisem kriminaalmenetluses kasutamine on menetluse jaoks märgilise tähtsusega, ei ole Euroopa Kohtu seisukohtadega kooskõlas praegune elektroonilise side alusel sideandmete üldise säilitamise süsteem. Euroopa Kohus on läbivalt rõhutanud, et sideandmeid tohib paari erandiga säilitada ja kasutada üksnes raske kuritegevuse vastu võitlemisel ja riigi julgeoleku tagamisel, ent ka nimetatud juhtudel ei ole põhjendatud andmete üldine ja vahet tegemata säilitamine (*general and indiscriminate retention*).

Magistritöö kirjutamise hetkel kehtiv elektroonilise side seadus on liidu õigusega vastuolus järgmise aspekti poolest. Elektroonilise side andmeid tohiks Euroopa Kohtu lahendites väljendatud seisukohtade kohaselt säilitada ja kasutada raske riive korral raskete kuritegude vastu võitlemiseks ning riigi julgeoleku tagamiseks. Eestis säilitatakse sideandmeid kõikide elektroonilise side teenust kasutavate isikute kohta, sõltumata sellest, kas nad on enda käitumisega põhjustanud olukorra, kus neid saab seostada raske kuritegevuse või riigi julgeoleku ohtu seadmisega või mitte. Seda enam on liidu õigusega vastuolus olukord, kui säilitatud andmeid asuda kasutama ka vähemraskete kuritegude ja väärtegude ning tsiviil- ja halduskohtumenetluste tarbeks. Näiteks on Eestis tavapärane, et tsiviilmenetluses kohustab kohus sideettevõtjat välja andma andmeid, et tuvastada solvava internetikommentaari jätnud autori isikut.

Käesoleval hetkel puuduvad selged suunised, mis kvalifitseerub Eesti seaduste mõttes raske kuriteona ja mis mitte. Ometi Euroopa Kohus sellist eristamist nõuab. Kuigi Euroopa Kohtul on mitmetes lahendites olnud võimalus anda suuniseid, millest lähtuda raskete kuritegude vahele joone tõmbamiseks, ei ole kohus seda teinud. Sellegipoolest on lahendis *Digital Rights Ireland* pidanud Euroopa Kohus raskeks kuriteoks näiteks organiseeritud kuritegevuse ja terrorismiga seotud kuritegusid.[296] Kui Euroopa Kohus peab andmete säilitamist proportsionaalseks meetmeks selliste raskete kuritegude nagu terrorismi ja organiseeritud kuritegevuse avastamiseks, siis sellise lähenemise pinnalt ei ole välistatud, et raskete kuritegude sõelale ei jää pidama kõik karistusseadustikus sätestatud teise astme kuriteod. Seda enam, et ühe võimalusena saab raskete kuritegude piiritlemisel lähtuda Nõukogu raamotsuses nr 2002/584/JSK toodud kuritegude loetelust, mis sisaldab endas ainult osa teise astme kuritegudest.[297]

[296] EKo *Digital Rights Ireland,* p 24.
[297] Näiteks kelmus (KarS § 209) ja rahapesu (KarS § 394 lg 1).

Euroopa Kohtu lahenditest tulenevate põhimõtete kohaselt on liidu õigusega vastuolus need riigisisesed õigusnormid, mis lubavad andmete üldist ja vahet tegemata säilitamist; mis ei nõua mingi seose olemasolu säilitatavate andmete ja raske kuritegevuse või ohu vahel avalikule julgeolekule; mis ei piira andmete säilitamist andmetega, mis kuuluvad kindlasse ajavahemikku, geograafilisse piirkonda või teatavatele isikutele, kes võivad olla mingil viisil seotud raske kuriteoga või isikutega, kelle andmete säilitamine võib muul põhjusel kaasa aidata raskete kuritegude ennetamisele, avastamisele või menetlemisele; mis ei näe ette andmetele ligipääsu andmist sõltumatu asutuse poolt, mis ei nõua andmete kustutamist pärast säilitusperioodi lõppu ja mis ei sätesta andmesubjekti teavitamist andmete säilitamisest ja kasutamisest. Nimetatud etteheidetega on vastuolus ka praegusel hetkel Eestis kehtivad riigisisesed õigusnormid.

Sideandmete säilitamisega kaasneva riive proportsionaalsuse tagamiseks on võimalik rakendada mitmeid meetmeid. Võttes arvesse, et üldine ja vahet tegemata säilitamine on lubatud väga kitsastel tingimustel, saab seadusandja alternatiivselt kaaluda näiteks andmete kiirsalvestamise (*quick freeze*), isikuliselt, ajaliselt ja geograafiliselt eristatud andmete säilitamise ja erinevatele andmeliikidele erineva säilitamisperioodi määramise vahel. Pidades silmas, et Euroopa Kohus on sedastanud, et liiklus- ja asukohaandmed võimaldavad isiku kohta teha väga täpseid järeldusi siis kõrgest konfidentsiaalsusastmest tulenevalt tuleks seda liiki andmeid lühemat aega säilitada. Seevastu abonendiandmed kui vähem tundlik andmete liik on midagi, mida sideettevõtjad säilitavad ärilistel eesmärkidel, st lepingu esitamiseks ja võimalike hilisemate vaidluste lahendamiseks, siis seda liiki andmete säilitamise jaoks saaks määrata pikema tähtaja. Samuti on võimalik sideettevõtja poolt enda äriliseks otstarbeks säilitatud andmeid välja nõuda raskete kuritegude vastu võitlemise ja terrorismi ohu korral.

Lisaks eespool mainitud kitsaskohtadele, tuleb riigisiseses õiguses muuta ka neid sätteid, mis lubavad prokuratuuril kohtueelses menetluses otsustada sideandmetele juurdepääsu üle. Euroopa Kohus leidis lahendis *H. K. vs Prokuratuur,* et Eesti prokuratuur ei ole selline sõltumatu haldusasutus, mis tohiks kohtueelses menetluses otsustada sideandmete väljanõudmiseks vajaminevate lubade andmise üle. Euroopa Kohus on juba varasemalt rõhutanud, et andmetele ligipääsu andmine peaks toimuma sõltumatu asutuse poolt. Sellegipoolest ei olnud võimalik enne lahendit *H.K. vs Prokuratuur* võimalik jõuda seisukohale, et Eesti prokuratuur ei ole sõltumatu asutus Euroopa Kohtu seisukohtade mõttes. Liikmesriikidel on väga erinevad õiguskaitsesüsteemid ning ühes riigis sõltumatuks asutuseks peetav asutus ei pruugi seda olla teises riigis. Kuivõrd prokuratuuril on pädevus anda ka muid

lubasid lisaks sideandmetele juurdepääsemisele, ei ole välistatud, et riigisisene regulatsioon kuulub üle vaatamisele ka muus osas. Kehtiva KrMS § 126^5 kohaselt on prokuratuuril õigus anda luba varjatud jälgimise teostamiseks. Kui Euroopa Kohtu hinnangul ei ole prokuratuur sõltumatu haldusasutus sideettevõtjalt andmete nõudmiseks antavate lubade osas, siis tuleb kaaluda, kas varjatud jälgimiseks antavaid lubasid saab endiselt anda prokuratuur.

Balance Between Metadata Retention and Fundamental Rights in Criminal Proceedings

Abstract

Wide spread of cryptocurrencies and dark web have given more options for criminals to carry out crime and conceal illegal proceeds. In addition to criminals, more people are using internet on a daily basis. Due to worldwide digitalization, more and more people are using different services and social media. That has created a situation where an increased amount of data is being stored at different service providers. Given that the use of electronic communications can play a key role in solving serious crime, it is important to make sure that data is retained and that law enforcement agencies have proper access to retained data. Electronic evidence plays a fundamental role in a huge number of criminal investigations and the need for such evidence is no longer limited to solving cyber crime. The importance of electronic evidence is on a rise, this statement is supported by the fact that in the year of 2020, electronic evidence played a crucial role in 85% of criminal cases in the European Union countries.[298]

These days, oil is no longer the most valuable resource. Instead – data is the new oil. [299] This statement is backed up by the data volume of collected data in the United States of America. In 2019, the National Security Agency accessed more than 534 million records of phone calls and text messages from different service providers such as AT&T and Verizon. This number is three times bigger than what was collected in 2016.[300]

One of the consequences of digitalization is a bigger amount of data being stored and therefore, the state is responsible for protecting its citizens and making sure that the data retention is carried on proportionally to the interference with the fundamental rights concerned. Legislation has to weigh in that the law enforcement agencies stay within legal boundaries when it comes to data collection and that on the other side citizens are protected from possible abuse by different service providers. Regulation has to be established to give clear guidelines on what kind of data, for how long and on what grounds can be retained to protect the rights of citizens.

[298] *SIRIUS EU Digital Evidence Situation Report, 2nd Annual Report*, 2020, page 5. Accessible: https://www.europol.europa.eu/sites/default/files/documents/sirius_desr_2020.pdf

[299] Bhagespur, K. *Data Is The New Oil – And That's A Good Thing – Forbes* 15.11.2019. Accessible: https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=2e1fdec17304, 21.02.2021.

[300] Savage, C. *N.S.A Triples Collection of Data From U.S. Phone Companies – The New York Times* 04.05.2018. Accessible: https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html, 03.02.2021.

As electronic evidence is not only limited to cybercrime, it is important to establish what are the limits for law enforcement agencies to carry out criminal proceedings and at the same time guarantee that nobody's rights are disproportionally interfered.

In the light of the case-law of the The European Court of Justice, many European countries need to reform their legislation. The European Court issued its first decision in 2014 in case *Digital Rights Ireland*. This decision has been followed by many landmark cases in every two years up until 2021 when the two-year interval was intervened. The second important decision was the case of *Tele2 Sverige* which has been followed by another important decision in 2016: *Ministerio Fiscal.* The European Court of Justice issued two decisions in 2020: *La Quadrature du Net* and *Privacy International*. The latest decision was issued in March 2021 which was *H. K. vs Prokuratuur*. Many European countries are puzzled when it comes to interpreting what the European Court of Justice has ruled in its landmark cases on data retention. Numerous references for a preliminary ruling have been submitted by Member States which illustrates how difficult it is for Member States to interpret the decisions.

The aim of this thesis was to find out whether the current Electronic Communications Act is in accordance with the Constitution of the Republic of Estonia and to what extent the European Court case law allows access to communication metadata to carry out criminal proceedings while still following fundamental rights of the concerned individuals. In case the European Court case law does not allow that in the extent it is practiced currently in Estonia and many other EU Member States, then what would be the solution that on one hand allows to carry out efficient criminal proceedings and on the other hand protects concerned individuals. The author proposed a hypothesis according to which the current Electronic Communications Act infringes fundamental rights disproportionally and is therefore not in accordance with the Constitution of the Republic of Estonia nor with the European Court of Justice case law.

The first chapter provides an overview of different types of data in criminal proceedings and explains what the different types of metadata are and what is the Estonian legal framework for retaining metadata. Additionally, the first chapter analyses relevant provisions of the Electronic Communications Act. When it comes to metadata, it is important to keep in mind that the European Court has narrowed it down to only traffic and location data.

The second chapter focuses on the situation regarding metadata retention in other countries than Estonia. The author of this thesis has concluded that different countries have very different attitudes when it comes to regulating metadata retention. Not only have countries different

views in Europe but in the whole world. For instance, Australia has a polarized perception compared to the European countries. The European Court has concluded that national legislation which allows general and indiscriminate retention of all traffic and location data of all subscribers and registered users with respect to all means of electronic communications is not in accordance with the EU law. According to the now invalidated directive 2006/24/EC, European countries were able to retain metadata from 6 months up to 2 years. Australia has set an obligation for telecommunication service providers to retain metadata for 2 years and their laws that allow general and indiscriminate retention are still in force. This is the opposite to some European countries – such as Germany, Austria and Slovenia – which have not set any obligations for their telecommunication service providers to retain data for law enforcement agencies.

The first half of the third chapter provides an overview of different fundamental rights that are infringed by metadata retention. It is important to keep in mind that the metadata retention infringes the rights of people whose data gets retained but on the other hand in case the telecommunication service providers do not retain metadata, the rights of those people, who are interested in the retention, are infringed. The state has an obligation to protect its citizens' life, health and property. In case the state does not have proper measures to fulfil the named obligations then those rights are essentially not ensured. The second half of the chapter analyses whether the Electronic Communications Act is in accordance with Constitution of the Republic of Estonia and provides suggestions on how to improve the national law.

The author affirmed the hypothesis that the current legislation is not in accordance with Constitution of the Republic of Estonia nor with the European Court case law. The European Court has declared in many of its landmark cases that the data should only be retained for the purpose of prevention, investigation, detection and prosecution of serious crime and for the interest of State security. The Electronic Communications Act allows the retained metadata to be used also in for misdemeanour, civil and administrative proceedings.

The European Court of Justice has emphasised that access to retained data should be subject to a prior review carried out either by a court or by an independent administrative body. In Estonia, the body that grants authorisations for obtaining data in pre-trial procedures is the prosecutor's office. This system can no longer be continued in the light of the most recent decision *H. K. vs Prokuratuur*. The reason why the prosecutor's office is not considered as an independent administrative body is because the prosecutor's office directs the investigation procedure and

brings the public prosecution. An independent administrative body who grants authorisation for obtaining data must be a third party in relation to the authority which requests access to the data. Such independent administrative body cannot be involved in the conduct of the criminal investigation. It has been predicted that instead of the prosecutor's office, a preliminary investigation judge will most likely be in charge of granting authorisation for obtaining data in the future.

The European Court of Justice has stated that such national law is in conflict with the European Union law that contains the following elements: permits general and indiscriminate data retention; does not require a link to serious crime; does not require retained data to be restricted to a particular time period and/or a particular geographical zone and/or to a circle of particular persons likely to be involved, in one way or another, in a serious crime; does not require supervision by an independent authority, does not require informing the data subject and does not require destruction of data. The Estonian national law is in conflict with those requirements.

Member States have not been able to interpret what constitutes a serious crime. Although the European Court of Justice has had many options to provide some guidelines, none have been provided. When it comes to predicting what constitutes a serious crime in Estonia, it is possible that not all first- and second-degree crimes qualify. What will most likely not qualify as a serious crime is harassing pursuit. In the future when the legislation has been amended, it will be difficult to prove cases of harassing pursuit when it is not possible to have access to retained metadata.

It has been established that the general and indiscriminate retention cannot continue and therefore, the state has to amend the relevant legislation. The legislator can for instance implement quick freeze instrument and retain data based on geographical zone, particular people and particular time period. Additionally, as some data is more sensitive than other, different periods for different types of data can be set forth. Member States as well as Estonia must keep on mind what the European Court of Justice highlighted in the case *Tele2 Sverige*. The European Court of Justice emphasized that the retention of traffic and location data cannot become a rule because the system established by Directive 2002/58/ sets forth that the retention of the data must remain an exception. Retaining data as an exception is how it should be in democratic societies when taking into account the seriousness of the interference entailed in the general and indiscriminate retention of traffic and location data.

KASUTATUD LÜHENDID

ADSL	*Asymmetric Digital Subscriber Line*
EIK	Euroopa Inimõiguste Kohus
EIÕK	Euroopa inimõiguste ja põhivabaduste kaitse konventsioon
EK	Euroopa Kohus
ESS	elektroonilise side seadus
GPRS	*General Packet Radio Service*
KrMS	kriminaalmenetluse seadustik
NSA	*National Security Agency*
OTT	*over-the-top*
RKKK	Riigikohtu kriminaalkolleegium
RKPJK	Riigikohtu põhiseaduslikkuse järelevalve kolleegium
TlnRnK	Tallinna Ringkonnakohus
U.S. Code	*United States Code*
VoIP	*Voice over Internet Protocol*
VoLTE	*Voice over LTE*

KASUTATUD ALLIKAD

Kirjandus

1. Benedizione, L., Paris, E. – *Preliminary Reference and Dialogue Between Courts as Tools for Reflection on the EU System of Multilevel Protection of Rights: The Case of the Data Retention Directive. – German Law Review* 2015/6.
2. De Hert, P. Belgium, *Courts, Privacy and Data Protection. An Inventory of Belgian Case Law from the pre-GDPR regime* (1995-2015) – *Brussels Privacy Hub* 2019.
3. Fenelly, D. *Data retention: the life, death and afterlife of a directive* – Springer VII/2018.
4. Goold, B. J., Lazarus, L. *Security and Human Rights: The Search for a Language of Reconciliation – Oxford: Hart Publishing* 2007.
5. Kergandberg, E. *Per aspera ad fair trial.* – Juridica I/2011.
6. Lõhmus, U. Elektroonilise side andmete säilitamise lõpetamata saaga. – Juridica X/2015.
7. Madise, Ü (peatoimetaja) jt. Eesti Vabariigi põhiseadus. Kommenteeritud väljaanne. Kolmas, täiendatud väljaanne. Tallinn: Juura 2012.
8. Sarre, R. *Metadata Retention as a Means of Combatting Terrorism and Organised Crime: A Perspective from Australia. University of South Australia – ResearchGate* 2017.
9. Tene, O., Polonetsky, J. *Big Data for All: Privacy and User Control in the Age of Analytics. – Northwestern Journal of Technology and Intellectual Property* V/2013.
10. Thompson II, R. M. *The Fourth Amendment Third-Party Doctrine – Congressional Research Service* VI/2014.
11. Vaile, D., Wijeyaratne, S., Churches, G., Zalneriutne, M. *Submission Telecommunications Data Review. University of New South Wales Law Research Series – Researchgate* VII/ 2019.
12. Vedaschi, A., Lubello, V. *Data Retention and its Implications for the Fundamental Right to Privacy. Tilburg Law Review*: 2015.
13. Virks, K. Sideandmed ja nende säilitamise olulisus. – Juridica VIII/2018.
14. Zubik, M., Podkowik, J., Rybski R. *European Constitutional Courts Towards Data Retention Laws. – Springer International Publishing*: 2021.

Õigusaktid

15. *Council of Europe. Convention on Cybercrime – European Treaty Series no*. 185.

16. Elektroonilise side seadus. – RT I 2004, 87, 593...RT I, 20.05.2020, 34.
17. Euroopa inimõiguste ja põhivabaduste kaitse konventsioon. Euroopa Nõukogu, 4 november 1950. – RT II 2010, 14, 54.
18. Euroopa Liidu põhiõiguste harta. 2010/C 83/02.
19. Euroopa Liidu toimimise lepingu konsolideeritud versioon. – ELT C 326, 26.10.2002.
20. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12.07.2002., milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv).
21. Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ.
22. Isikuandmete kaitse seadus. – RT I, 04.01.2019, 11.
23. Karistusseadustik. – RT I 2001, 61, 364...RT I, 20.07.2020, 18
24. Kriminaalmenetluse seadustik. – RT I 2003, 27, 166...RT I, 29.12.2020, 10.
25. Nõukogu 13.06.2002 raamotsus nr 2002/584/JSK Euroopa vahistamismääruse ja liikmesriikidevahelise üleandmiskorra kohta, L 190/1.
26. Euroopa Liidu põhiõiguste harta. 2010/C 83/02.
27. Nõukogu raamotsus 2006/783/JSK, 6.10.2006, konfiskeerimisotsuste suhtes vastastikuse tunnustamise põhimõtte kohaldamise kohta.
28. Nõukogu raamotsus 2008/909/JSK, 27.11.2008, vastastikuse tunnustamise põhimõtte kohaldamise kohta kriminaalasjades tehtud otsuste suhtes, millega määratakse vabadusekaotuslikud karistused või vabadust piiravad meetmed, nende Euroopa Liidus täideviimise eesmärgil.
29. Nõukogu raamotsus 2008/947/JSK, 27.11.2008, vastastikuse tunnustamise põhimõtte kohaldamise kohta kohtuotsuste ja vangistuse tingimisi kohaldamata jätmist käsitlevate otsuste suhtes, et teostada tingimuslike meetmete ja alternatiivsete mõjutusvahendite järelevalvet.
30. *U.S. Constution Amendment IV*. Arvutivõrgus kättesaadav: https://constitution.congress.gov/constitution/.
31. *United States. Congress. House. Committee on the Judiciary. USA Freedom Act: Report Together with Additional Views (to Accompany H.R. 3361) (Including Cost Estimate of the Congressional Budget Office). [Washington, District of Columbia]: [U.S. Government Printing Office]*, 2014.
32. *Telecommunications (Interception and Access) Act* 1979.

33. Väärteomenetluse seadustik. – RT I 2002, 50, 313...RT I, 10.12.2020, 37.

Kohtupraktika

Eesti Vabariigi kohtute praktika

34. RKKKm 1-16-6179.
35. RKKKo 3-1-1-93-15.
36. RKKKo 3-1-1-51-14.
37. RKPJKo 3-4-1-1-02.
38. RKPJKo 3-4-1-5-05.
39. RKPJKo 5-20-7/12.
40. RKPJKo 3-4-1-42-13.
41. RKPJKo 3-4-1-16-08.
42. TlnRnKo 3-16-183.
43. TlnRnKo 1-06-2292.

Ameerika Ühendriikide kohtute praktika

44. *California v. Greenwood*, 486 U.S. 35, 43-44 (1988).
45. *Carpenter v. United States*, 585 US 1 (6th Cir. 2018).
46. *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979).
47. *United States v. Gratkowski*, 964 F.3d (5th Cir. 2020).
48. *United States v. Knotts*, 460 U.S. 276, 285 (1983).
49. *United States v. Miller*, 425 U.S. 435 (1976).

Euroopa Inimõiguste Kohtu praktika

50. EIKo 03.07.2007, 62617/00. *Copland vs the United Kingdom*.
51. EIKo 04.12.2008, 30562/04 ja 30566/04. *S. and Marper vs the United Kingdom*.
52. EIKo 05.11.2002, 48539/99. *Allan vs the United Kingdom.*
53. EIKo 12.05.2000, 35394/97. *Khan vs the United Kingdom*.
54. EIKo 13.09.2019, 58179/13, 62322/14 ja 24960/15. *Big Brother Watch vs the United Kingdom.*

Euroopa Kohtu praktika*:*

55. EKo 02.03.2021, C-746/18. *H.K. vs Prokuratuur*.
56. EKo 02.10.2018, C-207/16. *Ministerio Fiscal.*

57. EKo 06.03.2001, C-274/99. P. *Bernard Conolly vs Commission of the European Communities.*
58. EKo 06.09.2011, C-163/10. *Aldo Patriciello.*
59. EKo 06.10.2020, C-623/17. *Privacy International.*
60. EKo 06.10.2020, liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18. *La Quadrature du Net.*
61. EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12. *Digital Rights Ireland.*
62. EKo 12.06.2003, C-112/00. *Eugen Schmidberger, Internationale Transporte und Planzüge vs Austria.*
63. EKo 16.07.2020, C-311/18. *Facebook Ireland.*
64. EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-203/15. *Tele2 Sverige.*

Muud allikad:

65. Aaspõllu, H. Tuhanded tõendid võivad kriminaalasjadest kaduda – ERR 03.03.2021. Arvutivõrgus kättesaadav: https://www.err.ee/1608129400/tuhanded-toendid-voivad-kriminaalasjadest-kaduda, 12.03.2021.
66. Andmekaitse inspektsioon. Eraelu kaitse 31.10.2019. Arvutivõrgus kättesaadav: https://www.aki.ee/et/eraelu-kaitse/eraelu-kaitse.
67. Ansi, T. *Network and Customer Installation Interfaces - Asymmetric Digital Subscriber Line (ADSL) Metallic Interface – Network Scholar*. 1998. Arvutivõrgus kättesaadav: https://www.semanticscholar.org/paper/Network-and-Customer-Installation-Interfaces-Line-Ansi/f1338fe5d9e583cde4901e49f35ca21bfbd0acbc, 01.02.2021.
68. Australian *Government Attorney-General's Department. Data Retention,* 2015. Arvutivõrgus kättesaadav: https://www.homeaffairs.gov.au/nat-security/files/data-retention-industry-faqs.pdf, 06.03.2021.
69. *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Data set.* Arvutivõrgus kättesaadav: https://www.homeaffairs.gov.au/nat-security/files/dataset.pdf, 02.03.2021.
70. *Australian Government, Department of Home Affairs. Lawful access to telecommunications. Data retention obligations. Service Provider Obligations*. Arvutivõrgus kättesaadav: https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations, 02.03.2021.
71. *Australian Government Department of Home Affairs. Parliamentary Joint Committee on Intelligence and Security. Review of the mandatory data retention regime. Home*

Affairs Portfolio submission. Arvutivõrgus kättesaadav: https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024394/toc_pdf/Reviewofthemandatorydataretentionregime.pdf;fileType=application%2Fpdf, 06.03.2021.

72. Berendson, R. Pavlihhini uurimine ja IP-aadresside teabenõue olid eri asjad – Postimees 24.01.2014. Arvutivõrgus kättesaadav: https://www.postimees.ee/2673656/pavlihhini-uurimine-ja-ip-aadresside-teabenoue-olid-eri-asjad, 07.02.2021.
73. Bhagespur, K. *Data Is The New Oil – And That's A Good Thing – Forbes* 15.11.2019. Arvutirvõrgus kättesaadav: https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/?sh=2e1fdec17304, 21.02.2021.
74. Churches, G., Zalnieriute, M. – A *Window for Change: Why the Australian Metadata Retention Scheme Lags Behind the EU and USA* – Australian Public Law 26.02.2020. Arvutivõrgus kättesaadav: https://auspublaw.org/2020/02/a-window-for-change-why-the-australian-metadata-retention-scheme-lags-behind-the-eu-and-usa/, 02.04.2021.
75. Cole, D. „*We Kill People Based on Metadata" – The New Yorker* 10.05.2014. Arvutivõrgus kättesaadav: https://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/, 15.03.2021.
76. *Council of Europe. Electronic Evidence in Civil and Administrative Proceedings* 2019. Arvutivõrgus kättesaadav: https://rm.coe.int/guidelines-on-electronic-evidence-and-explanatory-memorandum/1680968ab5, 08.01.2021.
77. *Commission of the European Communities. Extended Impact Assessment: Annex to theproposal for a directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC. SEC*(2005) 1131, 21.09.2015. Arvutivõrgus kättesaadav: https://ec.europa.eu/transparency/regdoc/rep/2/2005/EN/2-2005-1131-EN-1-0.Pdf, 09.03.2021.
78. 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 kättesaadav: https://eelnoud.valitsus.ee/main/mount/docList/0226101f-9cd8-46e9-b80c-7dcd6ae7ccf8#4ZeWIn6z, 12.03.2021.

79. Elisa kliendiandmete töötlemise põhimõtted. Isikuandmete töötlemise õiguslik alus ja eesmärgid. kättesaadav: https://www.elisa.ee/files/elisast/tingimused-ja-hinnakirjad/mobiilside-teenused/andmekaitse/ELISA_KLIENDIANDMETE_TOOTLEMISE_POHIMOTTED.pdf, 06.04.2021.
80. *Eucrim, the European Criminal Law Associates Forum – 2016/4. Focus: Anti-Money Laundering. Data Protection. CJEU Opposes General Data Retention Regimes (Case Tele2 Sverige).* Arvutivõrgus kättesaadav: https://eucrim.eu/media/issue/pdf/eucrim_issue_2016-04.pdf#page=14, 16.03.2021.
81. *Eurojust's analysis of EU Member States' legal framework and current challenges on data retention,* 26.10.2015. Arvutivõrgus kättesaadav: https://www.statewatch.org/media/documents/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf, 07.03.2021.
82. *European Commission. Frequently Asked Questions: New EU rules to obtain electronic evidence* 17.04.2018. Arvutivõrgus kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_3345, 06.01.2021.
83. *European Commission. Migration and Home Affairs. Europeans' attitudes towards cyber security.* 19.11.2017. Arvutivõrgus kättesaadav: https://ec.europa.eu/home-affairs/news/europeans'-attitudes-towards-cyber-security_en. 14.03.2021.
84. *European Commission. Report from the commission to the council and the European Parliament. Evaluation report on the Data Retention Directive (Directive 2006/24/EC).* COM(2011) 225 final, 18.04.2011. Arvutivõrgus kättesaadav: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF, 10.03.2021.
85. *European Commission. Study on the retention of electronic communications non-content data for law enforcement purposes. Final report. 2020. Arvutivõrgus kättesaadav*: https://www.statewatch.org/media/1453/eu-com-study-data-retention-10-20.pdf, 20.03.2021.
86. Euroopa Liidu Nõukogu, 12.01.2016. Aruanne Eesti kohta - vastastikuste hindamiste seitsmenda vooru hindamisaruanne „Küberkuritegevuse ennetamise ja sellega võitlemise Euroopa poliitika praktiline rakendamine ja toimimine". Arvutivõrgus kättesaadav: https://data.consilium.europa.eu/doc/document/ST-10953-2015-DCL-1/et/pdf, 06.01.2021.
87. Euroopa Liidu Nõukogu. Vastastikuste hindamiste seitsmes voor – küberkuritegevuse ennetamise ja sellega võitlemise Euroopa poliitika praktiline rakendamine ja toimimine,

09.06.2017. Arvutivõrgus kättesaadav: https://data.consilium.europa.eu/doc/document/ST-9986-2017-INIT/et/pdf, 25.01.2021.

88. *Federal Communications Commission. Voice Over Internet Protocol.* Arvutivõrgus kättesaadav: https://www.fcc.gov/general/voice-over-internet-protocol-voip, 02.03.2020.
89. Jacques, L., Cavez, B. *National Intelligence authorities and surveillance in the EU: FUndamental rights safeguards and remedies*. 13.06/2016. Arvutivõrgus kättesaadav: https://staging-new.fra.europa.eu/sites/default/files/fra_uploads/belgium-study-data-surveillance-ii-be.pdf, 15.03.2021.
90. Jõesaar, C. Elektroonilise side andmete säilitamine ja kasutamine kriminaalmenetluses. Magistritöö. – Tartu: Tartu Ülikool, 2019.
91. Kohtujuristi ettepanek, Giovanni Pitruzzella. Kohtuasi C-746/18, *H.K. vs Prokuratuur* 21.01.2020 Arvutivõrgus kättesaadav: https://curia.europa.eu/juris/document/document.jsf?text=&docid=222421&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=2250180, 15.03.2021.
92. Kohtujuristi ettepanek, Henrik Saugmandsgaard Øe. Liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige* 19.07.2016. Arvutivõrgus kättesaadav: https://curia.europa.eu/juris/document/document.jsf?text=&docid=181841&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=5340634, 06.04.2021.
93. Kohtujuristi ettepanek, Pedro Cruz Villalón. Liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland* 12.12.2013. Arvutivõrgus kättesaadav: https://curia.europa.eu/juris/document/document.jsf?text=&docid=145562&pageIndex=0&doclang=ET&mode=lst&dir=&occ=first&part=1&cid=3594439, 10.03.2021.
94. Kuritegevuse ülevaade 2018, Justiitsministeerium. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/02_kuritegevuse_ylevaade.pdf.
95. Kuritegevus Eestis 2019. Varavastased kuriteod. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevuse-statistika/varavastased-kuriteod.html, 17.12.2020.
96. Kuritegevus Eestis 2020. Kuritegevuse ülevaade. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevus2020/, 20.02.2021.
97. Kuritegevus Eestis 2020. Küberkuriteod. Arvutivõrgus kättesaadav: https://www.kriminaalpoliitika.ee/kuritegevus2020/, 20.02.2021.

98. Laks, L. Eesti jälitamisseadused said Euroopa kohtult löögi – Postimees 04.03.2021. Arvutivõrgus kättesaadav: https://leht.postimees.ee/7193284/euroopa-kohtu-otsus-voib-mojutada-eestis-tuhandeid-kriminaalmenetlusi, 04.03.2021.
99. Lamp, D., Anvelt, A. Eesti roimad. Koolitüdruk Veronika Dari tapmise tõe paljastas üks pisiasi – Elu24 15.04.2021. Arvutivõrgus kättesaadav: https://www.elu24.ee/7224532/koolitudruk-veronika-dari-morva-poleks-ehk-avastatud-kui-poleks-olnud-uht-pisiasja, 16.04.2021.
100. Lott, A. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis, 2015. Arvutivõrgus kättesaadav: https://www.riigikohus.ee/sites/default/files/elfinder/õigusalased%20materjalid/pkk_jlitustegevuse_anals.pdf, 01.04.2021.
101. Lõhmus, U. Uno Lõhmus: kaua tuleb oodata õiguse kooskõlla viimist põhiõiguste nõuetega? – ERR 04.03.2021. Arvutivõrgus kättesaadav: https://www.err.ee/1608129820/uno-lohmus-kaua-tuleb-oodata-oiguse-kooskolla-viimist-pohioiguste-nouetega, 04.03.2021.
102. Lõugas, H. Kommentaar: Teie andmed salvestatakse! – Eesti Päevaleht 22.03.2011. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/51294003/kommentaar-teie-andmed-salvestatakse, 05.01.2021.
103. Madise, Ü. Elektroonilise side seaduse § 111^1 alusel sideandmete töötlemise põhiseaduspärasus 22.04.2016. Arvutivõrgus kättesaadav: https://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf, 13.01.2021.
104. Madise, Ü. Õiguskantsleri seisukoht elektroonilise side seaduse § 111^1 põhiseaduspärasuse kohta 20.07.2015. Arvutivõrgus kättesaadav: https://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf, 24.03.2021.
105. Mazzetti, M., Schmidt, M. S. *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance. The New York Times*. 09.06.2013. Arvutivõrgus kättesaadav: https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html, 15.03.2021.
106. Mihkels, D. Näitlejanna ristiretk. Anonüümne mõnitamine läks Perekooli „kägudele“ kalliks maksma – Eesti Päevaleht 01.10.2018. Arvutivõrgus kättesaadav:

https://epl.delfi.ee/artikkel/83856517/naitlejanna-ristiretk-anonuumne-monitamine-laks-perekooli-kagudele-kalliks-maksma, 02.03.2021.

107. Milos reklaam. Eestlaste internetikasutus. 2019. Arvutivõrgus kättesaadav: https://milos.ee/eestlaste-internetikasutus-aastal-2019/, 12.02.2021.

108. *National Institute of Justice – Digital Evidence and Forensics*. Arvutivõrgus kättesaadav: https://nij.ojp.gov/digital-evidence-and-forensics, 07.02.2021.

109. Nixon, R. *U.S. Postal Service Logging All Mail for Law Enforcement – The New York Times* 03.07.2013. Arvutivõrgus kättesaadav: https://www.nytimes.com/2013/07/04/us/monitoring-of-snail-mail.html, 18.02.2021.

110. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters* 2018/0108(COD). Arvutivõrgus kättesaadav: https://eur-lex.europa.eu/legal-content/EN-ET/TXT/?from=EN&uri=CELEX%3A52018PC0225, 22.01.2021.

111. Registreeritud kuriteod maakondades aastatel 2018-2020. Arvutivõrgus kättesaadav: https://kriminaalpoliitika.ee/kuritegevus2020/data/kuritegevuse-ulevaade-2020.xlsx, 20.02.2021

112. Reichert, C. *Germany moves closer to data retention – ZDNet* 19.10.2015. Arvutivõrgus kättesaadav: https://www.zdnet.com/article/germany-moves-closer-to-data-retention/, 04.02.2021.

113. Reilly, C. *The metadata debate: What you need to know about data retention – Cnet* 13.08.2014. Arvutivõrgus kättesaadav: https://www.cnet.com/news/what-you-need-to-know-about-data-retention/, 04.02.2021.

114. Savage, C. *N.S.A Triples Collection of Data From U.S. Phone Companies – The New York Times* 04.05.2018. Arvutivõrgus kättesaadav: https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html, 03.02.2021.

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

116. Sehver, K., Ginter, C. Advokaadid: Kas teadsite, et Eesti riigiasutused koguvad ja kasutavad inimõigusi rikkudes suurt osa teie elektroonilise side andmeid? – Eesti Päevaleht 19.11.2017. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/80207790/advokaadid-kas-teadsite-et-eesti-riigiasutused-koguvad-ja-kasutavad-inimoigusi-rikkudes-suurt-osa-teie-elektroonilise-side-andmeid?, 03.01.2021.

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

118. Siitam-Nyiri, K. Kristel Siitam-Nyiri: advokaadid kasutavad sideandmete kogumisest rääkides kunstilisi liialdusi – Eesti Päevaleht, 20.11.2017. Arvutivõrgus kättesaadav: https://epl.delfi.ee/artikkel/80211168/kristel-siitam-nyiri-advokaadid-kasutavad-sideandmete-kogumisest-raakides-kunstilisi-liialdusi, 02.02.2021.

119. *SIRIUS EU Digital Evidence Situation Report, 2nd Annual Report*, 2020. Arvutivõrgus kättesaadav: https://www.europol.europa.eu/sites/default/files/documents/sirius_desr_2020.pdf, 15.12.2020.

120. Süldre, L. Parmas: Euroopa Kohtu otsus võib mõjutada tuhandeid kriminaalmenetlusi – ERR 02.03.2021. Arvutivõrgus kättesaadav: https://www.err.ee/1608128344/parmas-euroopa-kohtu-otsus-voib-mojutada-tuhandeid-kriminaalmenetlusi, 16.03.2021.

121. Taro, K. Külli Taro: jälitamisest ja jälgimisest – ERR 04.10.2018. Arvutivõrgus kättesaadav: https://www.err.ee/866452/kulli-taro-jalitamisest-ja-jalgimisest, 15.03.2021.

122. Taylor, J. *Australian government blames Snowden for data retention – ZDNet* 22.01.2015. Arvutivõrgus kättesaadav: https://www.zdnet.com/article/australian-government-blames-snowden-for-data-retention/, 15.03.2021.

123. Tehver, J. Digitaalsete tõendite kasutamise võimaldamine, 2016. Arvutivõrgus kättesaadav: https://www.just.ee/sites/www.just.ee/files/digitaalsed_toendid_j._tehver.pdf, 24.01.2021.

124. Telia Eesti AS üldtingimused. Lisa: Telia Eesti AS-i andmete kasutamise põhimõtted. Arvutivõrgus kättesaadav: https://www.telia.ee/images/documents/lepingud/lepingud-ja-tingimused/telia_eesti_as_andmete_kasutamise_pohimotted_est.pdf, 06.04.2021.

125. Telia. Kõned 4G võrgus. Arvutivõrgus kättesaadav: https://www.telia.ee/era/mobiil/muud-lisateenused/volte/, 02.03.2021.

126. *UNODC E4J University Module Series: Cybercrime, Digital Evidence*. Arvutivõrgus kättesaadav: https://www.unodc.org/e4j/en/cybercrime/module-4/key-issues/digital-evidence.html, 07.01.2021.

127. Vahter, T. Uskumatu: abipolitseiniku pealtkuulamine läks täielikult lörri, kuigi prokurör täitis kehtivat seadust. – Eesti Ekspress 14.04.2021. Arvutivõrgus kättesaadav: https://ekspress.delfi.ee/number/93055705/artikkel/93111013/uskumatu-abipolitseiniku-pealtkuulamine-laks-taielikult-lorri-kuigi-prokuror-taitis-kehtivat-seadust, 14.04.2021.

128. *Viber DMCA Policy*. Arvutivõrgus kättesaadav: https://www.viber.com/en/terms/dmca/, 21.04.2021.

Õigusloome

129. Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine). Arvutivõrgus kättesaadav: http://eelnoud.valitsus.ee/main/mount/docList/947260b9-64e7-4190-9319-32ecac6e6f83?activity=1#fVKzRoTp, 11.01.2021.

130. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri 175 SE. Arvutivõrgus kättesaadav: https://www.riigikogu.ee/download/2c393ed9-49bc-4438-9496-df52ecdf3560, 15.12.2020.

131. Euroopa Parlamendi ja nõukogu määruse, milles käsitletakse eraelu austamist ja isikuandmete kaitset elektroonilise side puhul ning millega tunnistatakse kehtetuks direktiiv 2002/58/EÜ (privaatsust ja elektroonilist sidet käsitlev määrus) ettepaneku seletuskiri. Arvutivõrgus kättesaadav: https://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX:52017PC0010, 13.12.2020.

LISAD

Lisa 1. Euroopa Liidu Nõukogu raamotsuses nr 2002/584/JSK artikli 2 punktis 1 loetletud kuriteod.

- kuritegelikus ühenduses osalemine,
- terrorism,
- inimkaubandus,
- laste seksuaalne ekspluateerimine ja lapsporno,
- narkootiliste ja psühhotroopsete ainete salakaubavedu,
- ebaseaduslik relva-, laskemoona- ja lõhkeainetega kauplemine,
- korruptsioon,
- pettus, sealhulgas pettus, mis kahjustab Euroopa ühenduste finantshuve 26. juuli 1995. aasta Euroopa ühenduste finantshuvide kaitse konventsiooni tähenduses,
- kuritegelikul teel saadud tulu rahapesu,
- raha võltsimine, sealhulgas eurode võltsimine,
- arvutikuriteod,
- keskkonnakuriteod, sealhulgas eriti ohustatud looma- ja taimeliikide ning taimesortide salakaubavedu,
- kaasa aitamine ebaseaduslikule piiri ületamisele ja elamisele,
- tahtlik tapmine, raske kehavigastuse tekitamine,
- ebaseaduslik kauplemine inimorganite ja -kudedega,
- inimröövv, ebaseaduslik vabadusevõtmine ja pantvangi võtmine,
- rassism ja ksenofoobia,
- organiseeritud või relvastatud röövimine,
- kultuuriväärtuste, sealhulgas antiik- ja kunstiesemete salakaubavedu,
- kelmus,
- väljapressimine ja rahaväljapressimine,
- toodete võltsimine ja piraatkoopiate valmistamine,
- haldusdokumentide võltsimine ja nendega kaubitsemine,
- maksevahendi võltsimine,
- ebaseaduslik kauplemine hormoonpreparaatide ja muude kasvukiirendajatega,
- tuumamaterjalide ja radioaktiivsete ainete salakaubavedu,
- varastatud sõidukitega kauplemine,
- vägistamine,
- süütamine,

- Rahvusvahelise Kriminaalkohtu alluvusse kuuluvad kuriteod,
- õhusõiduki või laeva kaaperdamine,
- sabotaaž.