Elektroonilise side andmete säilitamise põhiseaduspärasus[1]

Airiin Antson
Riigiprokuratuuri süüdistusosakonna konsultant

Sissejuhatus

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. Küberruumis ja elektroonilise side teenuseid kasutades jäävad maha andmed, mille põhjal saab teha olulisi järeldusi kuriteosündmuse aja, koha ja viisi kohta. On öeldud, et 21. sajandi tähtsaim vara on andmed[2], see arusaam kehtib ka kriminaalmenetluses. Andmetena käesolevas artiklis peetakse silmas elektroonilise side metaandmeid.

Sideandmete kasutamise võimalus võib mängida kuritegude lahendamisel olulist rolli. Menetleja pääseb aga ligi ainult sellistele andmetele, mis on olemas, seetõttu on vaja tagada teatava osa elektroonilise side andmete säilitamine. Seadused, mis panevad sideettevõtjatele kohustuse kõikide inimeste kohta andmeid säilitada, ohustavad inimeste privaatsust. Teisalt on selline andmete kogumise viis väga tõhus muu hulgas terrorismi ja raskete kuritegude vastases võitluses, mis on nende kuritegude tagajärgi arvestades hädavajalik, kaitsmaks inimeste õigust elule ja tervisele.

Sideandmete säilitamise ja kasutamise võimalus on kuritegude lahendamise seisukohalt väga oluline. Siiski on Euroopa Kohus teinud alates 2014. aastast sideandmete säilitamist puudutavaid lahendeid, mis on õiguskaitseasutusi kammitsenud. Kuigi Euroopa Kohus on enda seisukohti sideandmete säilitamise ja kasutamise kohta käsitlenud mitmes lahendis, puudub mitmes Euroopa riigis siiani ühtne arusaam sideandmete säilitamise ja selle lubatavuse kohta. Varem on sideandmete säilitamise regulatsiooni põhiseaduspärasust hinnanud Riigikohus ja õiguskantsler, kes leidsid, et sideandmete säilitamise regulatsioon on põhiseaduspärane. Siiski rõhutas õiguskantsler oma 2016. aasta analüüsis, et sideandmete töötlemise regulatsioon on ebaühtlane ja lünklik ning see tuleb terviklikult üle vaadata.[3] Pärast õiguskantsleri analüüse on jõustunud mitmed uued Euroopa Kohtu lahendid. Kuna praegu on Euroopa Kohtu lahendite valguses raske Riigikohtu ja õiguskantsleri järeldustega nõustuda, on siinse artikli eesmärk selgitada välja, kas kehtiv elektroonilise side seaduse[4] (ESS) § 111 on põhiseaduspärane ning kas ja kuidas võimaldab

[1] Artikkel põhineb autori magistritööl. Vt **A. Antson** 2021. Elektroonilise side andmete säilitamise ja põhiõiguste tagamise vahekord kriminaalmenetluses. Magistritöö. Tartu Ülikool, õigusteaduskond.
[2] **K. Bhagespur** 2019. Data Is The New Oil – And That's A Good Thing. – Forbes, 15. november.
[3] **Ü. Madise** 2016. Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus, lk 1.
[4] RT I, 22.10.2021, 15.

Euroopa Kohtu sidevaldkonna praktikast tulenev raamistik teha kriminaalmenetluses sideandmetega seonduvaid toiminguid, tagades samal ajal puudutatud isikute põhiõigused.

Elektroonilise side andmete mõiste

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.

Sideandmete säilitamise ja kasutamise puhul on vaja rõhutada sisuandmete ja metaandmete erinevust. Nimelt viitavad ühiskondliku debati käigus tõusetunud arutelud, et tavainimene ei erista nende kahe termini sisu. Aruteludest ja arvamusartiklitest nähtub, et tihtipeale ei eristata, milliste sideandmete puhul on sideettevõtjatel säilitamiskohustus. Seetõttu on kerge tekkima arusaam, et riigil on tegelikkusest laiemad õiguslikud hoovad andmetele ligi pääseda. Sõnapaariga *sideandmete kasutamine* võib esmalt silme ette kangastuda olukord, kus riik kogub isikute kohta valimatult kõiki andmeid või isegi kasutab sideandmeid isiku reaalajas jälgimiseks. Oluline on mõista, et sideandmete säilitamise ja kasutamise puhul ei ole tegemist jälitustoiminguga. Sideettevõtjale tehtava päringu alusel saadakse andmeid tagantjärgi juba aset leidnud sündmuste kohta ning seetõttu ei ole sideandmete säilitamine samastatav jälitustegevuse käigus tehtavate toimingutega. Kuigi päring sideettevõtjale ei ole alates 01.01.2013 enam käsitatav jälitustoiminguna, ei saa kõrvale jätta kriminaalmenetluse seadustiku[5] (KrMS) § 90[1] lõikes 3 sätestatud *ultima ratio* põhimõtet, mis tagab, et päringut sideettevõtjale ei saa teha igaks juhuks või et seda võimalust peaks tingimata iga kuriteo menetlemisel kasutama.[6]

Mis puudutab elektrooniliste sideandmete säilitamise reegleid, siis ESS käsitleb üksnes sideseansiga seotud metaandmeid, mitte sõnumi sisu.[7] See tähendab, et ESS-i alusel peavad sideettevõtjad säilitama abonendi- ehk kliendiandmeid (*subscriber information*), liiklusandmeid (*traffic data*), juurdepääsuandmeid (*access data*) ja asukohaandmeid (*location data*).

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. E-kirjade puhul säilitatakse meiliaadresse ning andmeid selle kohta, millal on e-kirju saadetud. Ei säilitata e-kirjade sisu ega nende pealkirju. Menetlejatele on olulise tähtsusega ka IP-aadressid, sest need võimaldavad kokku viia seadet seda kasutanud inimesega. Näiteks kui politsei avastab serveri, milles on lapspornot sisaldavad failid, on võimalik näha, millistelt IP-aadressidelt on seda serverit külastatud. Sellisel juhul saab sideettevõtjalt nõuda

[5] RT I, 22.12.2021, 45.

[6] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri (175 SE), lk 3.

[7] Elektroonilise side seaduse ja sellega seonduvalt teiste seaduste muutmise eelnõu väljatöötamiskavatsus (sideandmete säilitamine ja kasutamine), lk 2.

andmeid serverit kasutanud IP-aadresside kohta, et tuvastada isik, kes kasutas seda konkreetset IP-aadressi sel ajal, kui lapspornot sisaldanud serverile ligi pääseti.

Sideandmete liikide puhul on tähtis meeles pidada, et Euroopa Kohus käsitab kohtulahendites sideandmetena üksnes liiklus- ja asukohaandmeid.[8] Liiklus- ja asukohaandmed üldmõistena võimaldavad tuvastada, millal toimus sideseanss, kui pikk see oli ja kus helistaja või vastuvõtja liikus.[9]

Liiklusandmetena käsitatakse üldjuhul andmeid, mida töödeldakse side edastamiseks elektroonilises sidevõrgus või sellise edastamisega seotud arveldamiseks.[10] 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. Asukohaandmetena käsitatakse elektroonilises sidevõrgus või elektrooniliste sideteenuste töödeldavaid andmeid, mis näitavad üldkasutatavate elektrooniliste sideteenuste kasutaja lõppseadme geograafilist asukohta.[11]

Elektroonilise side andmete olulisus

Sideandmete säilitamise kohustus ja nende hilisem kriminaalmenetluses kasutamise võimalikkus on menetluste läbiviimise seisukohalt olulise tähtsusega. Sideandmete olulisust süütegude lahendamise kontekstis on sedastatud ka nii Euroopa Kohtu lahendites kui ka riigisiseses õiguses. Riigikohus on selgitanud, et riigil lasub kohustus kuritegusid avastada ja uurida, kaitstes nii kannatanute õigusi kui ka laiemalt avalikke huve.[12] Elektroonilise side andmete säilitamise tähtsust on Riigikohus tunnistanud ka hilisemas lahendis, sedastades, et elektroonilise side andmete kogumine sideettevõtjalt on tõhus meede saamaks objektiivseid tõendeid isikute suhtlemise fakti ja viibimiskoha kohta.[13] Sideandmete kasutamise olulisust illustreerib ka Veronika Dari mõrva juhtum ja Juri Ustimenko pommiplahvatuse kaasus, kus just kõneeristuse põhjal oli mõlemas menetluses võimalik lahenduseni jõuda.[14]

Sideettevõtjalt saadud andmeid on võimalik kasutada nii iseseisva tõendina kui ka koguda nende põhjal muid tõendeid. Kuigi sideandmete säilitamine ning nende hilisem kriminaalmenetluses kasutamine on menetluse jaoks märgilise tähtsusega, ei ole Euroopa Kohtu seisukohtadega kooskõlas praegune ESS-i alusel toimuv sideandmete üldise säilitamise süsteem. Euroopa Kohus

[8] EKo 08.04.2014 liidetud kohtuasjade otsus nr C-293/12 ja C-594/12: Digital Rights Ireland, p 16. EKo 21.12.2016 liidetud kohtuasjade otsus nr C-203/15 ja C-698/15: Tele2 Sverige AB, p 75. EKo 06.10.2020 liidetud kohtuasjade otsus nr C-511/18, C-512/18 ja C-520/18: La Quadrature du Net, p 96.
[9] **U. Lõhmus** 2021. Kaua tuleb oodata õiguse kooskõlla viimist põhiõiguste nõuetega? – ERR, 4. märts.
[10] EKo Tele2 Sverige (viide 8).
[11] Sealsamas, p 5.
[12] RK 18.06.2021 otsuse nr 1-16-6179 p 65.
[13] RK 23.02.2015 otsuse nr 3-1-1-51-14 p 22.
[14] **D. Lamp, A. Anvelt** 2021. Eesti roimad. Koolitüdruk Veronika Dari tapmise tõe paljastas üks pisiasi. – Postimees, 15. aprill.

on läbivalt rõhutanud, et sideandmeid tohib paari erandiga säilitada ja kasutada üksnes raske kuritegevuse vastu võitlemisel ja riigi julgeoleku tagamisel, ent ka neil juhtudel ei ole põhjendatud andmete üldine ja vahet tegemata säilitamine (*general and indiscriminate retention*).[15]

Võttes arvesse, et elektroonilise side andmeid peaks saama säilitada ja kasutada üksnes raskete kuritegude avastamiseks, uurimiseks ja ennetamiseks ning 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 ahistav jälitamine.[16] Autori hinnangul lahendatakse ahistava jälitamise kaasused tavapäraselt kõneeristusele tuginedes, ent tulevikus muutub selle kuriteoliigi tõendamine väga keeruliseks, kuna kõneeristus on nendes kaasustes üks väheseid objektiivseid tõendeid. Samale seisukohale on jõudnud ka õigusteadlane Jaan Ginter, kelle hinnangul jäävad tulevikus paljud kuriteod lahendamata või muutub politsei jaoks nende kuritegude tõendamine oluliselt keerukamaks.[17]

Elektroonilise side andmete säilitamise põhiseaduspärasus

Pikalt kestnud elektroonilise side andmete säilitamise lõpetamata saagale viidati õiguskirjanduses juba 2015. aastal.[18] See saaga ei ole ka praeguseks lõpule jõudnud. Selle olukorra on osaliselt põhjustanud asjaolu, et Euroopa Kohtu seisukohad sideandmete säilitamise ja kasutamise kohta ei ole üheselt mõistetavad. Seda väidet illustreerib olukord, kus mitmed riigid on Euroopa Kohtule eelotsusetaotlusi esitanud.[19] Ka artikli kirjutamise ajal on oodata paari Euroopa Kohtu lahendit sideandmete säilitamisega seotud kaasuses, kus eelotsusetaotlus on esitatud.[20]

Andmete säilitamise suhtes ei ole polariseerunud seisukohtadel ainult Euroopa riigid, seda on ka muud riigid. Direktiiv 2006/24/EÜ[21], mis reguleeris säilitamistähtaegasid, jõudis enne selle kehtetuks tunnistamist olla jõus kaheksa aastat. Selle direktiivi järgi lasus liikmesriikidel kohustus säilitada sideandmeid minimaalselt kuue kuu ning kõige rohkem kahe aasta vältel side toimumise kuupäevast arvates. Praegu varieeruvad säilitamise tähtajad olenevalt riigist.

ESS-i § 111[1] lõike 4 järgi lasub sideettevõtjatel kohustus säilitada sama paragrahvi lõigetes 2 ja 3 nimetatud andmeid ühe aasta vältel side toimumise ajast arvates. Seevastu Austraalias on

[15] EKo La Quadrature du Net (viide 8), p 168.
[16] KarS § 157[3], mis on teise astme kuritegu.
[17] **H. Sarv** 2021. Professor: kuritegude tõendite otsimine muutub keerulisemaks. – ERR, 3. märts.
[18] **U. Lõhmus** 2015. Elektroonilise side andmete säilitamise lõpetamata saaga. – Juridica, nr 10, lk 735–745.
[19] 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).
[20] Liidetud kohtuasjad C-793/19 ja C-794/19 SpaceNet ning C-140/20 Commissioner of the Garda Síochána.
[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 (ELT L 105, 13.4.2006, lk 54–63).

kohustuslik säilitada andmeid kaks aastat.[22] Sellele pakuvad kontrasti mitmed Euroopa riigid, kus sideettevõtjatel puudub kohustus õiguskaitseasutuste tarbeks andmeid säilitada. Sellised on näiteks Austria, Saksamaa ja Sloveenia. Nendes kolmes riigis saavad õiguskaitseasutused menetluste tarbeks välja nõuda üksnes neid andmeid, mida sideettevõtjad on enda tarbeks ärilistel eesmärkidel talletanud.[23]

Sideandmete säilitamise puhul tuleb mõista, et ühel kaalukausil on need inimesed, kelle õigusi andmete säilitamisega riivatakse. Teisel kaalukausil on inimesed, kes on huvitatud andmete säilitamisest ja kelle huve riivatakse andmete säilitamata jätmisega. See, et andmeid säilitatakse, aitab riigil ja eri institutsioonidel täita oma põhiseaduslikku kohustust tagada oma rahva elu ja tervise ning vara kaitse.

Euroopa Kohtu senistes lahendites on analüüsitud üksnes säilitatud sideandmete andmesubjekti riivatavaid õigusi. Käsitlemata on jäänud sideandmete säilitamise olulisus andmete töötlemisest huvitatud poolte vaatenurgast, kõrvutades julgeoleku ja turvalisuse aspekti. Riigi üks ülesandeid on võitlus kuritegevusega. See on oluline muu hulgas üksikisikute põhiõiguste ja -vabaduste tagamise seisukohalt. Põhiõiguste kaitse ja põhiseadusliku korra kaitse ei ole mitte vastas-, vaid samasuunaline protsess. Isikute põhiõiguste kaitse ja riigi julgeolek kujutavad endast teineteist täiendavaid väärtusi.[24] Selmet omavahel põhiõigusi ja julgeolekut vastandada, tuleks nende vahel hoopis tasakaal leida.[25]

Sideandmete säilitamise regulatsiooni põhiseaduspärasust on varem hinnanud nii õiguskantsler 2015. aastal[26] ja 2016. aastal[27] kui ka Riigikohus vahetu normikontrolli käigus[28]. Nendesse põhiseaduspärasuse kontrollidesse tuleb suhtuda kriitiliselt, sest nendes väljendatud seisukohad ei ole praegu enam Euroopa Kohtu ja Euroopa Inimõiguste Kohtu lahendites väljendatud põhimõtetega kooskõlas. Euroopa Inimõiguste Kohus käsitles lahendis Copland *vs.* 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.[29] Kuna Eestis kehtib ESS, millega võeti üle praeguseks Euroopa Kohtu poolt 2014. aastal kehtetuks tunnistatud direktiiv, on päevakohane küsimus, kas ESS on endiselt põhiseaduspärane ja asjakohane.

---

[22] Telecommunications (Interception and Access) Act 1979 § 187C 1 (b) (ii).
[23] **European Commission** 2020. Study on the retention of electronic communications non-content data for law enforcement purposes. Final report, lk 39–40.
[24] **B. J. Goold, L. Lazarus** 2007. Security and Human Rights: The Search for a Language of Reconciliation. – Oxford: Hart Publishing, lk 2. Vt ka **A. Lott** 2015. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis.
[25] **K. Virks** 2018. Sideandmed ja nende säilitamise olulisus. – Juridica, nr 8, lk 581–596.
[26] **Ü. Madise** 2015. Õiguskantsleri seisukoht elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta.
[27] **Ü. Madise** (viide 3).
[28] RKo otsus nr 3-1-1-51-14 (viide 13).
[29] EIKo 03.07.2007 otsus nr 62617/00: Copland vs United Kingdom, p 48.

Samuti on teravalt päevakorras tõendi ehk sideettevõtjalt saadud andmete protokolli lubatavus praegusel ajal, mil Euroopa Kohus on teinud otsuse asjas H. K. *vs.* prokuratuur[30]. Selle lahendi tõttu spekuleeritakse, et tuhandetes kriminaalmenetlustes võib suur hulk tõendeid arvestamata jääda.[31] 2021. aasta märtsi lõpus tegi Tartu Ringkonnakohus lahendi, mis võttis arvesse Euroopa Kohtu seisukohti. Kõnealuses kriminaalasjas väljastas prokurör loa sideandmete väljanõudmiseks ja saadud sideandmete põhjal tekkinud kahtluste tõttu kuulati jälitustoimingu käigus isiku telefoni pealt. Ringkonnakohus viitas Euroopa Kohtu lahendile C-746/18 ja rõhutas, et prokurör ei oleks tohtinud kohtueelses menetluses sideandmetele ligipääsu üle otsustada. Selle seisukoha tõttu tunnistas kohus maakohtu antud loa isiku telefoni pealt kuulata õigustühiseks.[32]

Sideandmete tõendina lubatavuse asjus võttis Riigikohus 2021. aasta suvel seisukoha ka teises lahendis. Üldise põhimõttena leidis kohus, et enne Euroopa Kohtu 02.03.2021 lahendit H. K. *vs.* prokuratuur ei saanud prokuratuuril sideandmete päringute jaoks lubade andjana olla tõsikindlat teadmist, et prokuratuurile antud õigus lubada sideandmete kasutamist on vastuolus EL-i õigusega. Kolleegiumi hinnangul valitses kuni Euroopa Kohtu 06.10.2020 otsuseni La Quadrature du Net[33] sideandmete säilitamise ja kasutamisviiside küsimuses märkimisväärne teadmatus.[34] Teisisõnu, kohus tõmbas sideandmete tõendina lubatavuse hindamisel punase joone La Quadrature du Net lahendi juurde. Load, mis on antud sideandmete päringuks pärast seda lahendit, ei ole tõendina kriminaalmenetluses lubatud. Nende lubade puhul, mis anti enne viidatud lahendit, tõi Riigikohus välja kriteeriumid, mille järgi on võimalik hinnata prokuratuuri loal sideandmetele juurdepääsu võimaldamisega toimunud rikkumise olulisust.[35]

Selgitamaks, kas sideandmete säilitamise regulatsioon on põhiseaduspärane, tuleb hinnata formaalset ja materiaalset õiguspärasust. Formaalne kooskõla Eesti Vabariigi põhiseadusega[36] tähendab, et põhiõigusi piirav õigustloov akt peab vastama pädevus-, menetlus- ja vorminõuetele ning määratuse ja seadusereservatsiooni põhimõtetele.[37] Ühegi varasema põhiseaduspärasuse kontrolli käigus ei ole ESS-i formaalset õiguspärasust kahtluse alla seatud. Ka autori hinnangul ei ole põhjust kahelda, et ESS vastab formaalse põhiseaduspärasuse nõudele. Riigikogu järgis seadust vastu võttes selleks ettenähtud protseduurireegleid ja ESS-i sätted andmete säilitamise kohta on piisavalt õigusselged. Seetõttu hinnatakse siinses artiklis sisuliselt üksnes materiaalset õiguspärasust.

[30] EKo 02.03.2021 kohtuasja otsus nr C-746/18: H. K. vs prokuratuur.
[31] **H. Aaspõllu** 2021. Tuhanded tõendid võivad kriminaalasjadest kaduda. – ERR, 3. märts.
[32] **T. Vahter** 2021. Uskumatu: abipolitseiniku pealtkuulamine läks täielikult lörri, kuigi prokurör täitis kehtivat seadust. – Eesti Ekspress, 14. aprill.
[33] EKo La Quadrature du Net (viide 8).
[34] RK 18.06.2021 otsuse nr 1-16-6179 p 62.
[35] Sealsamas, p-d 59–68.
[36] RT I, 15.05.2015, 2.
[37] RK 13.06.2005 otsuse nr 3-4-1-5-05 p 8.

Materiaalne põhiseaduspärasus tähendab, et põhiõigusi riivav õigusakt on kehtestatud põhiseadusega lubatava eesmärgi saavutamiseks ja on selle saavutamiseks proportsionaalne abinõu.[38] Põhiseaduse § 11 järgi saab põhiõigusi piirata üksnes kooskõlas põhiseadusega, tingimusel et piirangud on demokraatlikus ühiskonnas vajalikud ning ei moonuta piiratavate vabaduste ja õiguste olemust. Seetõttu peab põhiõiguste riivel olema põhiseadusega kooskõlas olev legitiimne eesmärk.[39]

Andmete säilitamise legitiimine eesmärk

Eestis on direktiiv 2006/24/EÜ üle võetud ESS-iga, mille vastav redaktsioon jõustus 17.12.2007. ESS hakkas muu hulgas reguleerima, mis liiki andmeid ning mis perioodi vältel sideettevõtjad säilitama peavad. Direktiiv 2006/24/EÜ sätestas eesmärgina ühtlustada teenusepakkujate kohustusi säilitada teatud sideandmeid selliselt, et oleks tagatud nende kättesaadavus liikmesriikide riigisisese õiguse kohaselt määratletud raskete kuritegude avastamiseks, uurimiseks, ja kohtus menetlemiseks.[40] Kuigi ESS-i muutmise eesmärk oli võtta direktiiv üle riigisisesesse õigusesse, ei piirdunud seadusandja üksnes direktiivis ettenähtud miinimumnõuetega. Eesti seadusandja on lisaks raskete kuritegude uurimisele, avastamisele ja kohtus menetlemisele näinud ette võimaluse nõuda sideandmed välja ka vähem raskete kuritegude tarbeks ning väärteo-, tsiviil- ja haldusmenetlustes.

Kuna elektroonilise side andmete säilitamisega täidetakse vähemalt ühte andmete säilitamisega tagatavat eesmärki, milleks on raskete kuritegude uurimine, avastamine ja kohtus menetlemine, on tegemist legitiimse eesmärgiga.[41] 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.[42]

a. Riive sobivus – ebaproportsionaalne on selline abinõu, mis ei soodusta mitte ühegi eesmärgi saavutamist. Seega on sobiv meede selline, mis soodustab eesmärgi saavutamist.[43] Kahtlemata saab pidada andmete säilitamist meetmeks, mis aitab kaasa raskete kuritegude uurimisele, avastamisele ja kohtus menetlemisele. Andmete säilitamine ESS-i §-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 tõhusa, ent isikut vähem koormava abinõuga.[44] Sellegipoolest on Euroopa Kohus ette heitnud, et võitlus raske kuritegevuse vastu on avaliku julgeoleku

[38] RK 26.03.2009 otsuse nr 3-4-1-16-08 p 28.
[39] RK 16.03.2021 otsuse nr 5-20-7/12 p 57.
[40] Direktiiv 2006/24/EÜ (viide 21), punkt 24, art 1 lg 1.
[41] **Ü. Madise** (viide 3), lk 5.
[42] RKPJKo 3-4-1-16-08 p 29.
[43] RK 06.03.2002 otsuse nr 3-4-1-1-02 p 15.
[44] Sealsamas.

tagamiseks esmatähtis, ent selline eesmärk üksinda ei saa õigustada seda, et direktiiviga 2006/24/EÜ ettenähtud andmete säilitamist peetakse kuritegevusvastase võitluse jaoks vajalikuks.[45]

Direktiivi 2006/24/EÜ kohaselt on sideandmed väärtuslik vahend kuritegevuse ja kuritegude, eriti organiseeritud kuritegevuse ennetamisel, uurimisel, avastamisel ja kohtus menetlemisel.[46] Euroopa Kohus nõustus selle seisukohaga, sedastades, et andmete säilimine pakub raskete kuritegude lahendamiseks lisavõimalusi ning on seetõttu uurimise jaoks kasulik vahend.[47] 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 oma otsuses ei 2011. aasta Euroopa Nõukogu hindamisaruandele ega muudele dokumentidele, mis andmete säilitamise tõhusust analüüsivad.[48]

KrMS § 90[1] alusel võib päringu 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 Ülle Madise on leidnud, et ESS-i §-st 111[1] tulenev eraelu puutumatuse riive on andmete säilitamise tasandil küllaltki kaalukas. Kokkuvõtvalt on ta siiski jõudnud järeldusele, et andmete säilitamisest tulenevat riivet ei saa sideteenuse kasutaja jaoks lugeda väga intensiivseks.[49] Selline seisukoht on vastuolus Euroopa Kohtu praktikaga. Õiguskantsler on muu hulgas põhistanud oma seisukohta sellega, et säilitatavate andmete liikide hulgas ei ole sõnumi sisu.[50] Euroopa Kohtu lahendite valguses ei saa selle seisukohaga päri olla.

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 koos võimaldavad teha andmesubjektide kohta väga täpseid järeldusi. Näiteks on võimalik teha järeldusi nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja nende ühiskonnarühmade kohta, kellega nad läbi käivad. Nii Euroopa Kohus kui ka kohtujurist Henrik Saugmandsgaard Øe on rõhutanud, et nende andmete põhjal on võimalik koostada asjaomaste isikute profiil, mis on õigust eraelu puutumatusele arvestades sama tundlik teave kui sideseansi sisu ise.[51]

---

[45] EKo Digital Rights Ireland (viide 8), p 51.
[46] Direktiiv 2006/24/EÜ (viide 21), punkt 7.
[47] EKo Digital Rights Ireland (viide 8), p 49.
[48] **M. Zubik, J. Podkowik, R. Rybski** 2021. European Constitutional Courts Towards Data Retention Laws. Springer International Publishing, lk 22.
[49] **Ü. Madise** (viide 3), lk-d 6 ja 9.
[50] Sealsamas, lk 9.
[51] EKo Tele2 Sverige (viide 8), 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.

Lahendis La Quadrature du Net kinnitas kohus varem lahendis Tele2 Sverige väljendatud põhimõtet. Samuti lisas kohus, et liiklus- ja asukohaandmed võivad avaldada andmesubjektide kohta muu hulgas sellist delikaatset teavet nagu seksuaalne sättumus, poliitilised vaated, usulised, filosoofilised, ühiskondlikud või muud veendumused, samuti tervislik seisund.[52] Autori hinnangul omab liiklus- ja asukohaandmete säilitamine kahtlemata samasugust riivet, nagu oleks sisuandmete säilitamise puhul, sest liiklus- ja asukohaandmete põhjal on võimalik teha järeldusi sideseansi sisu kohta. Selle illustreerimiseks on allpool esitatud mõned näited, kus isikute ja nende kõnede sisu kohta on võimalik teha järeldusi ka üksnes mobiilimastis läheduses viibimise, kõne tegemise asukoha või valitud numbri põhjal.

1. Öösel kell 1.18 tehakse 25-minutiline kõne täiskasvanute teenuseid pakkuvale telefoniliinile. Kõne sisu kohta saab teha järeldusi, teadmata, mida täpselt räägiti.
2. Türisalu pangalt tehti esmalt kõne Eluliinile ning seejärel psühholoogilise kriisiabi telefonile. Kuigi kõnes räägitu jääb teadmata, on sellegipoolest võimalik teha järeldusi kahe järjestikuse kõne sisu kohta.
3. On teada, et sama tunni jooksul helistas inimene günekoloogi numbril ning seejärel Eesti Seksuaaltervise Liidu numbril. Kuigi kõne sisuandmeid ei säilitata, on valitud numbrite põhjal tehtavad järeldused ühesed.
4. Isikute rühm viibis LGBT paraadi ajal sealsete mobiilimastide juures. Euroopa Kohus on sedastanud sideandmete pinnalt seksuaalse sättumuse kohta järelduste tegemise võimalikkust ja seda illustreerib näiteks olukord, kus isikud viibivad LGBT linnaosades või vastavatel paraadidel ja laagrites.

Abinõu mõõdukuse hindamisel tuleb kaaluda ühest küljest põhiõigusesesse sekkumise ulatust ja intensiivsust, teisest küljest aga eesmärgi tähtsust.[53] Õiguskantsler on riive mõõdukust õigustanud muu hulgas kuritegevusvastase võitlusega.[54] Õiguskantsler ei ole analüüsinud kehtivat õiguslikku raamistikku, mis annab ESS-i §-le 111[1] laiad hoovad kasutada säilitatud sideandmeid ka muudel eesmärkidel peale kriminaalmenetluse. Kuna 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-i §-s 111[1] ettenähtud võimaluste[55] kasutamiseks. ESS-i alusel säilitatud andmeid on lubatud kasutada ka väärteo- ja haldusmenetlustes, ent selline olukord on tugevas vastuolus Euroopa Kohtu seisukohaga, mille kohaselt tohib andmeid säilitada ja kasutada üksnes raske kuritegevuse ja terrorismi vastu võitlemiseks. Säilitatud sideandmeid on lubatud Eestis kasutada lisaks näiteks kalakaitses,

[52] EKo La Quadrature du Net (viide 8), p 117.
[53] RKPJKo 3-4-1-1-02, p 15.
[54] **Ü. Madise** (viide 3), lk 9.
[55] ESS-i § 111[1] lõike 11 punkti 3 kohaselt edastatakse andmeid väärteomenetluse seadustiku kohaselt ka Andmekaitse Inspektsioonile, Finantsinspektsioonile, Tarbijakaitse ja Tehnilise Järelevalve Ametile, Keskkonnaametile, Politsei- ja Piirivalveametile, Kaitsepolitseiametile ning Maksu- ja Tolliametile.

turvateenuse osutamiseks vajaliku tegevusloa taotlemiseks, Finantsinspektsiooni järelevalve tegemiseks, maksudega seotud süüteomenetluses ja tsiviilõiguslike vaidluste lahendamiseks.[56]

Eraldi kriitikat väärib juba mainitud õiguskantsleri seisukoht, mille kohaselt riive on tasakaalustatud objektiivse vajadusega kuritegevusvastaseks võitluseks. Võitlus kuritegevuse vastu on madal künnis, millega riivet õigustada. Euroopa Kohus on selgitanud, et 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.[57] Riive pole raske näiteks mobiilsideseadme omaniku tuvastamisel ning selliste andmete kogumisel võib juurdepääsu põhjendada ka üldiselt kuritegude uurimise, ennetamise, avastamise ja menetlemise eesmärgiga.[58]

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 Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8 ette nähtud põhiõiguste ulatuslikku riivet, mida tuleb pidada eriti raskeks. Seda sel põhjusel, et andmesubjekti ei teavitata andmete säilitamisest ja nende hilisemast kasutamisest.[59]

Lisaks ei saa pidada mõõdukaks 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 seadnud ohtu riigi julgeoleku. Seejuures säilitatakse andmeid ka nende isikute kohta, kelle sideseansid puudutavad ametisaladust. Lisaks on Euroopa Kohus direktiivile 2006/24/EÜ ette heitnud, et see ei piira andmete säilitamist andmetega, mis kuuluvad kindlasse geograafilisse piirkonda.[60] Sätestades andmete säilitamisele geograafilise kriteeriumi, peavad pädevad ametiasutused leidma objektiivsete asjaolude põhjal, et ühes või mitmes geograafilises piirkonnas esineb kõrgendatud oht raskete kuritegude ettevalmistamiseks või toimepanemiseks.[61] Lisaks geograafilisele sihistamisele saab seadusandja teoorias kaaluda ka isikuliselt ja ajaliselt eristatud andmete säilitamist. 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.[62] See seisukoht viitab artiklis varem sedastatule, et Euroopa Kohtu seisukohad sideandmete säilitamiseks ei ole üheselt

[56] **K. Sehver, C. Ginter** 2017. Advokaadid: Kas teadsite, et Eesti riigiasutused koguvad ja kasutavad inimõigusi rikkudes suurt osa teie elektroonilise side andmeid? – Eesti Päevaleht, 19. november.
[57] EKo Digital Rights Ireland (viide 8), p 51.
[58] EKo Ministerio Fiscal (viide 8), p 57–58.
[59] Sealsamas, p 37.
[60] Sealsamas, p 59.
[61] EKo Tele2 Sverige (viide 8), p 111.
[62] **K. Siitam-Nyiri** 2017. Advokaadid kasutavad sideandmete kogumisest rääkides kunstilisi liialdusi. – Eesti Päevaleht, 20. november.

mõistetavad, sest mitte ükski riik ei suuda ette näha, milliseid andmeid raskete kuritegude lahendamiseks vaja võib minna, ja seetõttu ei suuda neid eelnevalt säilitada.

Geograafilise kriteeriumi olulisust rõhutav seisukoht ei ole Eesti väiksuse tõttu Eestile hästi üle kantav. Euroopa Kohtu seisukoha järgi tuleks Eesti mõistes andmeid säilitada üksnes n-ö ohtlikemates piirkondades, nagu utreeritult Lasnamäe ja Narva.[63] Euroopa Kohtu soovitus säilitada andmeid kindlas piirkonnas ei ole väga tõhus meede. Nimelt on sellistes kriminaalsetes piirkondades elavatel isikutel võimalik minna kuritegusid toime panema n-ö turvalistesse piirkondadesse. Seega hakkaks selline lahendus soodustama olukorda, kus kurjategijad hakkaksid oma kõnesid tegema teises piirkonnas. See tekitab küsimuse, kas n-ö turvalisse piirkonda liikunud kurjategija andmeid ei säilitatagi.[64] Samuti diskrimineerib andmete säilitamine üksnes konkreetses geograafilises paigas sealseid teisi elanikke, kes ei ole ühtegi kuritegu toime pannud ning kellel ei ole seost terrorismiga.

Kokkuvõtteks võib jõuda järeldusele, et Eestis kehtiv regulatsioon sideandmete säilitamiseks ei ole Euroopa Kohtu ja Euroopa Inimõiguste Kohtu seisukohti arvesse võttes põhiseaduspärane. Euroopa Kohus on juurutanud põhimõtet, mille kohaselt ei tohi sideandmete säilitamine demokraatlikus ühiskonnas saada reegliks olukorras, kus direktiivis 2002/58/EÜ kehtestatud süsteem nõuab, et andmete säilitamine oleks erand.[65] ESS-i § 111[1] ei ole materiaalselt põhiseaduspärane seetõttu, et andmete üldine ja vahet tegemata säilitamine kõikide sideteenuseid kasutavate inimeste kohta, samuti andmete säilitamine võimalusega neid kasutada lisaks kriminaalmenetlusele ka tsiviil-, väärteo- ja haldusmenetluses ei ole proportsionaalne abinõu kuritegude avastamiseks, uurimiseks ja kohtus menetlemiseks.

Kokkuvõte

Kuigi Euroopa Kohus kuulutas 2014. aasta lahendiga Digital Rights Ireland direktiivi 2006/24/EÜ tagasiulatuvalt kehtetuks, on kaheksa aastat hiljem Eesti endiselt nende riikide seas, kes ei ole kehtetuks tunnistanud riigisisest õigusakti, millega direktiiv üle võeti, või vähemalt sideandmete säilitamist puudutavaid sätteid Euroopa Liidu õigusega täies mahus kooskõlla viinud.

Artiklis esitatud analüüsi kohaselt riivab praegu kehtiv ESS ebaproportsionaalselt isikute põhiõigusi ja ei ole seetõttu põhiseaduspärane ega kooskõlas Euroopa Liidu õigusega. Euroopa Kohtu sideandmete säilitamist puudutavad lahendid on peamise fookuse seadnud põhiõiguste tagamisele ning õiguskaitseasutustele väga laiasid hoovasid kätte ei anna. Samas ei tohi andmete säilitamise tõttu riivatavate põhiõigustega seoses ära unustada, et kuigi andmete säilitamisega riivatakse andmesubjektide õigusi, siis andmete säilitamata jätmisega riivatakse teisest küljest andmete töötlemisest kasu saavate poolte huvisid. Kuna riigil lasub kohustus tagada oma rahva

[63] 2020. aastal oli kuritegude arv 10 000 inimese kohta kõige kõrgem Ida-Virumaal. Vt **Justiitsministeerium**. Kuritegevus Eestis 2020. Kuritegevuse ülevaade.
[64] **K. Virks** 2018. Sideandmed ja nende säilitamise olulisus. – Juridica, nr 8, lk 581–596.
[65] EKo Tele2 Sverige (viide 8), p 104, EKo La Quadrature du Net (viide 8), p 142.

ning elu ja tervise kaitse ning võttes arvesse, et isikute põhiõiguste kaitse ning riigi julgeolek kujutavad endast lisaväärtusi, 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 ESS-iga, 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-is 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.

Artikli kirjutamise ajal kehtiv ESS on Euroopa Liidu õigusega vastuolus järgmiste aspektide 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, kus säilitatud andmeid saab asuda kasutama ka vähem raskete kuritegude ja väärtegude ning tsiviil- ja haldusmenetluste tarbeks.