TARTU ÜLIKOOL

ÕIGUSTEADUSKOND

Karistusõiguse osakond

Daniel Gortšinski

# SIDEANDMETE KASUTAMINE LUBATAVA TÕENDINA SÜÜTEOMENETLUSES

Magistritöö

Juhendajad

MA Vahur Verte

*PhD* Tambet Grauberg

Tartu

2025

# SISUKORD

# SISSEJUHATUS

Tänapäeva digiühiskonnas on võimatu kujutada ette tõhusat inimestevahelist suhtlust ilma elektroonilise sideta ja selleks kasutatavate vahenditeta - need on vahendid, mis võimaldavad kõne- või internetisidet. Aja möödudes muutusid sideteenused aina kättesaadavamaks ning tänaseks said sideteenused elanikkonna põhiliseks suhtlusvahendiks. Statistikaameti andmetel[1] oli 2016. aastal Eestis registreeritud 1 897 921 erinevat mobiilside kõneteenuse abonenti – abonentide arv on suurem kui Eesti rahvaarv 2016. aastal (1 315 944 inimest)[2]. 2024. aasta seisuga on internetiühendusega ühendatud umbes 544 800 Eesti leibkonda[3].

Paraku käib kuritegevus ajaga kaasas ning elektrooniline side on muutunud ka kurjategijate *modus operandi* lahutamatuks osaks. Mida enam kasutatakse igapäevaelus sidevahendeid, seda rohkem jätavad need vahendid endast maha jälgi – elektroonilise side andmeid, mis võivad osutuda väärtuslikeks tõenditeks süütegude uurimisel. Sideandmed annavad uurimisasutustele võimaluse kaardistada isikutevahelisi seoseid, tuvastada suhtluse ajaraame ning teatud juhtudel ka side osapoolte asukohti. Teadmine, et süütegude toimepanemine viib toimepanija varem või hiljem õigus- ja korrakaitseasutuste huviorbiiti, loob vajaduse kiireks suhtluseks, mida tänapäeva sidelahendused on võimelised pakkuma. Sideandmete analüüs võib aidata tuvastada kurjategijate vahel toimuva suhtlusega seotud seadmed, sideseansside asjaolud ning seeläbi ka suhtluse osapooled. Just seetõttu on elektroonilisel sidel oluline koht mitte ainult meie igapäevaelus, vaid ka uurimisasutuste tööriistakastis.

Järelikult on oluline võimaldada sideettevõtjalt saadud andmete (edaspidi ka: sideandmete) kasutamine kriminaal- ning väärteomenetlustes. Seda protsessi reguleerivad kriminaalmenetluse seadustik[4] (KrMS) ning väärteomenetluse seadustik[5] (VTMS). Menetlusõiguslik regulatsioon on seejuures seotud sideandmetena käsitletavate andmete ning nende kogumist ja säilitamist reguleeriva elektroonilise side seadusega[6] (ESS). Küll aga on sideandmete kasutamine lubatava tõendina süüteomenetluses muutunud töö koostamise aja

[1] Statistikaameti andmebaas. SI35: Elektroonilise side kliendid ja liinid (2011-2016). Veebis: https://andmed.stat.ee/et/stat/Lepetatud_tabelid__Majandus.%20Arhiiv__Infotehnoloogia%20ja%20side.%20Arhiiv__side/SI35 (01.02.2025).
[2] Statistikaameti andmebaas. RV021: Rahvastik, 1. Jaanuar. Veebis: https://andmed.stat.ee/et/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV021 (01.02.2025).
[3] Statistikaameti andmebaas. IT20: Arvuti ja koduse internetiühendusega leibkonnad. Veebis: https://andmed.stat.ee/et/stat/majandus__infotehnoloogia__infotehnoloogia-leibkonnas/IT20 (01.02.2025).
[4] Kriminaalmenetluse seadustik - RT I, 17.04.2025, 6.
[5] Väärteomenetluse seadustik - RT I, 17.04.2025, 12.
[6] Elektroonilise side seadus - RT I, 30.12.2024, 9.

seisuga pea võimatuks. Seda põhjusel, et Euroopa Kohus ning Riigikohus on pidanud õigusvastaseks sideandmete (eeskätt liiklus- ja asukohaandmete) säilitamise üldiselt ja vahet tegemata, nagu seda näeb ette ESS § 111[1], samuti selliselt säilitatud andmete lubatava tõendina kasutamise KrMS § 90[1] kontekstis.

Probleemi ei lahendanud ka see, et alates 01.01.2022 kehtiva KrMS § 90[1] redaktsiooni järgi lubati sideandmete väljanõudmine üksnes eeluurimiskohtuniku loal varasema prokuratuuri loa alusel. Nimelt asus Tartu Ringkonnakohus 2024. aasta maikuu kohtumäärusega seisukohale, et ei ole võimalik pidada lubatavaks olukorda, kus tõendina kasutatakse selliseid sideandmeid, mille säilitamine on toimunud õigusvastaselt[7]. Selle tulemusena andis Riigiprokuratuur asutuseülese korralduse loobuda sideandmete kasutamisest[1], mis omakorda kinnitab üleriigilist võimatust sideandmete tõendina kasutamiseks hetkel kehtiva regulatsiooni võtmes. Järelikult eeldab sideandmete efektiivne tõendina kasutamise tulevikus sideandmete regulatsiooni viimist kooskõlla EL õigusega.

Kuivõrd sideandmete kasutamine eeldab, et nii sideandmete säilitamise (ning säilitamise tarbeks kogumise) kui ka kasutamise (väljanõudmise ja juurdepääsu) regulatsioon vastaks nõuetele, tuleb antud töö raames analüüsida nii sideandmete säilitamist kui ka nende süüteomenetlustes kasutamist reguleerivat õigusnormistikku. Arvestades, et regulatsioon lubab sideandmete kasutamist nii kriminaal- kui ka väärteomenetlustes, tuleb säilitamise ja kasutamise regulatsiooni sobitada mõlema süüteomenetluse liigi võtmesse. Seejuures on tõenäoline, et kriminaalmenetluse puhul on sideandmete kasutamine lubatud palju laiemalt kui väärteomenetluses. Magistritöö fookuses on õiguslikud probleemid, mis tõusetuvad elektroonilise side seaduses oleva sideandmete säilitamise kohustuse regulatsiooni ning kriminaal- ning väärteomenetluse seadustikes oleva sideandmete väljanõudmise regulatsiooni rakendamisel praktikas.

Magistritöö põhieesmärk on tuvastada kas ja kuidas peaks muutuma siseriiklik õigus selleks, et võimalik oleks sideandmete lubatav kasutamine tõendina süüteomenetlustes. Selleks tuleb esiteks analüüsida kehtivat sideandmete säilitamise ja kasutamise regulatsiooni ning tuvastada millistele Euroopa Liidu õigusest tulenevatele kriteeriumitele peab vastama sideandmete regulatsioon. Selle tulemusena saab tuvastada millistel tingimustel on sideandmete säilitamine

[7] Vahter, T. Prokuratuur sai kohtus nii valusa kaotuse, et loobus kuritegude uurimisel sideandmete kasutamisest. Eesti Ekspress 08.10.2024. https://ekspress.delfi.ee/artikkel/120327337/prokuratuur-sai-kohtus-nii-valusa-kaotuse-et-loobus-kuritegude-uurimisel-sideandmete-kasutamisest (03.02.2025).

ja kasutamine lubatav Euroopa Liidu õiguse kontekstis. Kuna Euroopa Kohtu otsused ei kohaldu ainult Eestile, tuvastab autor kuidas on teised Euroopa Liidu liikmesriigid (edaspidi ka: liikmesriigid) viinud oma sideandmete regulatsiooni kooskõlla EL õigusega. Selle tulemusena saab, tuginedes EL õigusest tulenevatele kriteeriumitele, sobitada teiste riikide lahendusi Eesti õiguse konteksti, pakkumaks reaalseid regulatiivseid lahendusi selleks, et täita töö põhieesmärk. Seejuures peavad need lahendused tasakaalustama süüteomenetluste huvid ning sideandmete säilitamise ja kasutamisega kaasneva põhiõiguste riive.

Eeltoodust tulenevalt on magistritöö uurimisküsimused püstitatud järgnevalt:

1. Kuidas on Eestis reguleeritud sideandmete kogumine, säilitamine ja kasutamine tõendina süüteomenetlustes?
2. Millistele Euroopa Kohtu ning Eesti kohtute praktikast tulenevatele kriteeriumitele peab vastama sideandmeid puudutav regulatsioon nende kasutamiseks lubatava tõendina süüteomenetlustes?
3. Kuidas on teised Euroopa Liidu liikmesriigid muutnud oma sideandmetega seonduvat regulatsiooni Euroopa Kohtu sideandmeid puudutava praktika valguses?
4. Millised regulatiivsed muudatused Eesti õiguses võimaldaks säilitada ning kasutada sideandmeid lubatava tõendina süüteomenetlustes kooskõlas Euroopa Liidu õigusega?

Töö on koostatud kolmes peatükis, lähtuvalt uurimisküsimustest. Esiteks käsitleb autor sideandmete säilitamist ja kasutamist puudutavat regulatsiooni ning analüüsib Eesti ning EL õigusest tulenevaid kriteeriume sideandmete õiguspäraseks säilitamiseks ja tõendina kasutamiseks. Teises peatükis analüüsib autor liikmesriikide sideandmeid puudutavat siseriiklikku õigust eesmärgiga tuvastada kuidas liikmesriigid viisid oma sideandmete regulatsiooni vastavusse EL õigusega. Kolmandas peatükis püüab autor leida regulatiivsed lahendused selleks, et sideandmete säilitamine ja kasutamine oleks kooskõlas EL õigusega ning sideandmeid saaks efektiivselt kasutada tõendina süüteomenetlustes. Järeldused uurimisküsimustele esitab autor konsolideeritult magistritöö kokkuvõttes.

Magistritöö teema aktuaalsus rajaneb vajadusel korrigeerida Eesti sideandmeid puudutavad regulatsioonid, et leida tasakaal sideandmete säilitamisega kaasneva põhiõiguste riive ning sideandmete süütegude menetlemiseks kasutamise vältimatu vajaduse vahel. Teema aktuaalsus kerkib eriti esile olukordades, kus käimasolevates menetlustes pole menetlejatel üldse võimalik kasutada sideandmeid seoses regulatsiooni vastuoluga EL õiguse suhtes.

Käesolev loometöö on uudne. Viimati kaitsti teaduskonnas sideandmete teemaline magistritöö 2021. aastal ning see keskendus sideandmete säilitamise ja kasutamisega riivatavatele põhiõigustele ja töö koostamise ajal kehtinud seadusandluse põhiseaduspärasusele[8]. Käesolev töö keskendub aga hetkel kehtiva regulatsiooni muutmise vajaduse tuvastamisele ning selliste lahenduste püstitamisele, mis tagavad sideandmete regulatsiooni kooskõla EL õigusega ja sideandmete tõhusa kasutamise tõendina. Selleks analüüsib autor liikmesriikide uusimat, so aastatel 2022-2024 kehtestatud sideandmete regulatsiooni. Töös tuuakse välja liikmesriikide unikaalseid ning Eesti õigusest eristuvaid lähenemisi sideandmete säilitamise regulatsiooni EL õigusega kooskõlla viimisel. Nende alusel pakutakse käesolevas töös regulatiivsete ettepanekutena uusi sideandmete säilitamise viise, mille kaudu loodab autor lahendada pikki aastaid väldanud probleemi seoses sideandmete säilitamise ja kasutamisena süüteomenetlustes.

Uurimisküsimuste lahendamiseks kasutatakse Eesti kohtute ning Euroopa Kohtu praktikat sideandmete säilitamise ning kasutamise teemadel. Kohtupraktika analüüs võimaldab autoril tuvastada konkreetsed kriteeriumid, millele peab vastama siseriiklik sideandmete regulatsioon. Euroopa Liidu riikide sideandmeid puudutavate regulatiivsete lahenduste uurimiseks ja võrdlemiseks kasutab autor liikmesriikide õigusakte. Analüüsiks valitud liikmesriigid paistsid silma teistest põhjalikuma sideandmete regulatsiooniga ning unikaalsete ja Eesti kehtivast regulatsioonist erinevate kriteeriumitega, mille alusel nendes sideandmeid säilitatakse. Samuti on kasutatud Euroopa Liidu asutuste raporteid, eesmärgiga tõhustada analüüsitavate liikmesriikide valikut ja kohtulahendite tõlgendamist. Regulatiivsed ettepanekud tuvastatakse läbi EL õigusest tulenevate kriteeriumite ja liikmesriikide näidete rakendamise Eesti õiguse kontekstis. Töö viimases peatükis kasutatakse võrdlusmõõdikuid, mis rajanevad Eesti ning välisriikide ametlikul statistikal.

Töös kasutatakse kvalitatiivset ning võrdlevat uurimismeetodit. Kvalitatiivset meetodit kasutab autor selleks, et analüüsida sideandmete säilitamist ja kasutamist puudutavat regulatsiooni ja sellele kohalduvaid EL õigusest tulenevaid kriteeriume. Liikmesriikide ning Eesti õiguse võrdlemise teel tuvastab autor lahendused, mis viiks sideandmete regulatsiooni kooskõlla EL õigusega ning võimaldaks kasutada sideandmeid lubatava tõendina süüteomenetlustes.

Tööd kirjeldavad järgmised märksõnad: süüteomenetlus, menetlusõigus, sideettevõtted, metaandmed, Euroopa Liidu õigus.

[8] Antson, A. Elektroonilise side andmete säilitamise ja põhiõiguste tagamise vahekord kriminaalmenetluses. Magistritöö. Juhendajad R. Kiris ja J. Ginter. Tartu: Tartu Ülikool 2021.

# 1. SIDEANDMETE SÄILITAMISE JA KASUTAMISE LUBATAVUS EESTIS EUROOPA LIIDU ÕIGUSE KONTEKSTIS

## 1.1. Sideandmete mõiste, liigid, säilitamine ning kasutamine Eesti süüteomenetlustes

Käesoleva töö uurimiseseme kontekstis saab sideandmete mõiste avada läbi ESS § 102 lõike 1. Selle kohaselt on sideettevõtja kohustatud hoidma saladuses kõiki talle sideteenuse osutamise käigus teatavaks saanud andmeid kliendi ja teiste isikute kohta, kes ei ole sõlminud lepingut sideteenuse osutamiseks, ent kes kasutavad sideteenust kliendi nõusolekul, eelkõige:

1. andmeid sideteenuse kasutamise üksikasjade kohta;
2. sidevõrgu kaudu edastatava sõnumi sisu ja vormi kohta;
3. andmeid sõnumi edastamise aja ja viisi kohta.

Kuna ESS § 102 lg 1 punktis 2 nimetatud sõnumi sisu andmeid saadakse kriminaalmenetluses KrMS § $126^7$ alusel läbi viidava jälitustoiminguga, ei käsitle autor neid andmeid käesoleva töö fookuses olevate sideandmetena. Seega on sideandmed käesoleval töö raames defineeritavad kui sideteenuse osutamise käigus tekkinud andmed sideteenuse kasutamise üksikasjade kohta ning sidevõrgu kaudu edastatava sõnumi vormi, aja ja viisi kohta.

Sideandmed on seotud sideteenustega. Sideteenusena saab käsitleda erinevaid igapäevaelust tuttavaid teenuseid. Nende seas on internetiühenduse teenus (ESS § 2 p 84), isikutevahelise side teenus (ESS § 2 p 91), kaabelleviteenus (ESS § 2 p 11), mobiiltelefoniteenus (ESS § 2 p 13), püsiliiniteenus (ESS § 2 p 37), telefoniteenus (ESS § 2 p 58) ja virtuaalvõrguteenus (ESS § 2 p 64). Sideandmeid saab sideteenuse osutamise käigus koguda, säilitada ning kasutada. Kuna sideandmete säilitamine eeldab nende eelnevat kogumist, peab autor edaspidiselt sideandmete säilitamiseks ka nende säilitamise tarbeks kogumist.

Sideandmete säilitamine saab toimuda üksnes elektroonilise side seaduses sätestatud alustel. Neid aluseid võib säilitusnormide sõnastusest tulenevalt jaotada kaheks kategooriaks – sideandmete säilitamine ärilistel eesmärkidel ning sideandmete säilitamine seadusega sätestatud kohustuse alusel. Esiteks kehtestab seadus sideettevõtjale andmete säilitamise ja töötlemise õigused eesmärkidel, mis võimaldavad temal tegutseda oma majandustegevuses (ärilistel eesmärkidel). Nendeks eesmärkideks on:

1. Sideandmete töötlemine kliendi nõusolekul turunduslikul eesmärgil ESS § 103 alusel;
2. Sideteenuse kliendi elektrooniliste kontaktandmete kasutamine kliendi nõusolekul otseturustuseks ESS § $103^1$ alusel;

3. Sideandmete töötlemine kliendi nõusolekuta sideteenuse arve esitamiseks ESS § 104 alusel;
4. Anonüümitud sideteenuse kliendi ja rändlusteenuse kasutaja asukohaandmete töötlemine ESS § 105 alusel;

Andmete töötlemine ärilisel eesmärgil on ESS § 106 lg 1 alusel lubatud üksnes sideettevõtjale ning tema volitusel tegutsevale isikule, kes osutab sideteenuse kasutamisega seotud teenuseid. Sellisteks teenusteks on näiteks klientide küsimustele vastamine, pettuste avastamine ning sideteenuse turustamine. Selline andmete säilitamine on vajalik sideettevõtja huvides, et tema saaks rakendada sideteenuse osutamisel oma lepingulisi õigusi ja kohustusi (nt arve esitamine kliendile) aga ka omada võimalust oma majandustegevuse arendamiseks ja selle tulususe suurendamiseks (nt teenuse turundamine).

Teiseks kehtestab seadus sideettevõtjale eraldiseisva kohustuse säilitada sideandmed selleks, et kasutada neid süütegude menetlemiseks ning riigi julgeoleku tagamiseks. Seda eesmärki täitvaks säilitamiskohustuse aluseks on ESS § $111^1$. Selle sätte esimese lõike kohaselt on sideettevõtja kohustatud säilitama kõik andmed sideseansi või -teenuse üksikasjade (va edastatava sõnumi sisu) kindlaksmääramiseks. ESS § $111^1$ lõiked 2 ja 3 sätestavad aga konkreetsed andmete liigid, mida ühe või teise teenuse osutamise korral säilitada tuleb.

Antud õigusnormist võib järgnevat analüüsi silmas pidades jagada sideandmed kolmeks erinevaks liigiks, mis on järjestatud nende säilitamise või kasutamisega kaasneva eraelu puutumatuse riive intensiivsuse järgi. Esimene ning leebemat riivet kaasa toov liik on identifitseerimisandmed ehk andmed, mis võimaldavad tuvastada sideteenuse lõppkasutaja identiteet või lähteabonendile omistatud IP-aadress – nende andmete hulka ei kuulu andmed sideseansi toimumise fakti kohta. Näiteks kuulub nende andmete hulka teave selle kohta, kelle nimele on sõlmitud konkreetse mobiiltelefoni numbriga seotud teenuseleping. Teine sideandmete liik on liiklusandmed ehk andmed, mis võimaldavad tuvastada sideseansi toimumise või sideteenuse kasutamise fakt ning sellega seotud asjaolud (välja arvatud andmed edastatud sõnumi sisu kohta). Näiteks kuulub nende andmete hulka kõneeristus ehk detailne ülevaade ühe telefoninumbri sissetulevatest ja väljaminevatest kõnedest ja sõnumitest. Viimane ja kõige intensiivsemat riivet kaasa toov sideandmete liik on asukohaandmed ehk andmed, mis võimaldavad tuvastada kus asus sidevahend sideteenuse osutamise või sideseansi kestuse ajal. Näiteks kuulub nende andmete hulka teave selle kohta, mis asukohaga tugijaamadele tegi sideteenust kasutav mobiiltelefon levi tugevuse tuvastamispäringuid.

Eeltoodud sideandmed tuleb kehtiva õiguse kohaselt säilitada ühe aasta jooksul side toimumisest, andmete tekkimisest või nende töötlemisest. Säilitamist on põhjendatud vajadusega kasutada neid andmeid põhjendatud korral süütegude menetlemiseks, julgeoleku tagamiseks ning ESS § $111^1$ lg 11 punktides 4-6 nimetatud spetsiifiliste haldusmenetluste ja tsiviilkohtumenetluste läbiviimiseks. Seejuures ei erista ESS § $111^1$ kelle, mis teenuseosutaja või mis piirkonna sideandmeid tuleb säilitada – kohtupraktikas nimetatakse taolist säilitamist üldiseks ning vahet tegemata säilitamiseks, mis on aga Euroopa Kohtu hinnangul liiklus- ja asukohaandmete kontekstis eraelu puutumatust ning isikuandmete kaitse põhiõigust ebaproportsionaalselt piirav (vt lähemalt ptk 1.2).

Lisaks säilitamise regulatsioonile eeldab sideandmete tõendina kasutamine ka sideandmete kasutamise regulatsiooni olemasolu ning nõuetele vastavust. Eestis reguleerib sideandmete kasutamist süüteomenetlustes kriminaalmenetluse seadustiku § $90^1$ ning väärteomenetluse seadustiku § $31^2$.

KrMS § $90^1$ annab kriminaalmenetluse läbiviijale õiguse teha iseseisvalt päring sideettevõtjale identifitseerimisandmete saamiseks. Teiste sideandmete puhul tuleb andmete väljanõudmise päringu jaoks saada eeluurimiskohtuniku luba prokuratuuri taotlusel – kohtuliku kontrolli nõue tuleneb Euroopa Kohtu praktikast (vt lähemalt ptk 1.5). Ligipääs on õigustatud üksnes juhul, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Seejuures on taolised päringud lubatud üksnes võitluseks raske kuritegevusega.

VTMS § $31^2$ annab lõikes 1 nimetatud täidesaatva riigivõimu asutustele ehk kohtuvälisele menetlejale õiguse teha iseseisvalt päring sideettevõtjale identifitseerimisandmete saamiseks. Teiste sideandmete liikide puhul tuleb nendel asutustel saada kohtu luba üksikpäringu teostamiseks. Üksikpäring tähendab sideandmete väljanõudmist konkreetse telefonikõne, elektronkirja, elektroonilise kommentaari või muu üksiksõnumi edastamisega seotud sideseansi kohta. Ka väärteomenetluse puhul võib ligipääs sideandmetele olla õigustatud üksnes vältimatu vajaduse korral väärteomenetluse eesmärgi kontekstis.

Eelnevatel alustel välja nõutavaid sideandmeid saab kasutada süüteomenetluses tõendina. Sideandmed nõutakse välja ning analüüsitakse uurimistoimingute raames ning toimingu kohta koostatakse ka vastav protokoll, mis on tõend KrMS § 63 lg 1 mõistes. Sellisele tõendile kohalduvad tõendi lubatavuse tingimused. Riigikohtu praktika kohaselt loetakse tõend

lubamatuks siis, kui tõendi kogumise korda on oluliselt rikutud. Tõend tuleb tõendikogumist kõrvaldada näiteks juhul, kui rikutud on kriminaalmenetluse aluspõhimõtteid või menetlustoimingust puudutatud isiku põhiõigusi[9]. Sideandmete kasutamiseks lubatava tõendina tagada järelikult tagada see, et need koguti, säilitati ning kasutati (nõuti välja) õiguspäraselt. See aga eeldab elektroonilise side seadusest tulenevate säilitamisnormide ja kriminaal- ning väärteomenetluse seadustikest tulenevate kasutamisnormide õiguspärasust, mida autor hiljem ka analüüsib.

Sideandmete puhul on oluline tagada, et nende kogumine ja kasutamine on proportsionaalne eraelu puutumatuse riivele, mida taoliste toimingutega tekitatakse. Üheks proportsionaalsust tagavaks kriteeriumiks on sideandmete kasutamise regulatsioonis olev vältimatu vajalikkuse kriteerium. See tagab, et menetleja ei asu tõendama süütegu sideandmetega mugavusest, vaid reaalsest vältimatust vajadusest ehk tõdemusest, et süüteo tõendamine muude väiksemat riivet kaasatoovate toimingutega on äärmiselt raskendatud. Teine viis tagada riive proportsionaalsus on kehtestada erikriteeriumid privaatsemate sideandmete liikide ehk liiklus- ja asukohaandmete säilitamiseks ja kasutamiseks. Vajadus sellise lahenduse järgi tuleneb järgnevalt analüüsitavatest Euroopa Kohtu lahenditest.

Sideandmetega seonduva regulatsiooni ülevaatamine on vajalik lisaks eelselgitatud proportsionaalsuse tagamisele vajadusele ka seetõttu, et sarnast eesmärki täitvatest toimingutest on sideandmete väljanõudmine põhiõigusi vähim riivavam toiming. Alternatiivselt sideandmete väljanõudmisele on uurimisasutusel võimalik pääseda ligi nendele andmetele sideseansis osalenud seadmete (nt telefonide) äravõtmise ning analüüsimise teel või teabe salajasel pealtkuulamisel või -vaatamisel ehk teostades KrMS § 126[7] lõikes 1 kirjeldatud jälitustoimingut. Eelduslikult pääseb jälitusasutus viimasega ligi ka pealtkuulatava seansi üldandmetele ehk käesolevas töös läbivalt käsitletud sideandmetele.

Seadmete analüüsiga võib uurimisasutus pääseda ligi isikute muule eraelulisele teabele riivates potentsiaalselt perekonna- ja eraelu puutumatust (isikuandmed, fotod, edastatud sõnumid jm) omandipuutumatust (seadme äravõtmine). Seadmete analüüs ei riiva sõnumi saladust, kuivõrd Riigikohtu hinnangul pole selle põhiõiguse kaitsealas kommunikatsiooniprotsessi läbinud sõnumid[10]. Pealtkuulamise või -vaatamisega teostatakse aga isiku suhtes sõnumisaladust

[9] RKÜKo 1-17-2359, p 48.
[10] RKKKo 3-1-1-93-15, p 100.

äärmiselt riivav jälitustoiming, mida oleks üksnes sideandmetele ligi pääsemise vajaduse korral saanud vältida sideandmete väljanõudmise toiminguga.

Õiguslik olukord seoses sideandmete säilitamise ning väljanõudmisega tõstatavad põhjendatud küsimuse, kas selle toimingu asemel ei hakatud kasutama sagedamini eelkirjeldatud põhiõigusi suuremas mahus riivavaid alternatiive. Kui seadmete analüüsi kohta puudub avalik statistika, siis teabe salajase pealtkuulamise või -vaatamise kohta on see olemas. Nimelt avaldab prokuratuur iga-aastaselt oma aastaraamatu, mille kriminaalmenetluse statistika plokis tuuakse välja ka jälitustoimingute statistika, kus on nimetatud nii jälitustoiminguteks antud lubade arv kui ka ülevaadet toimingutest, milleks anti luba esmakordsetes jälitustoimingute taotlustes. Seejuures tuleb arvestada, et üks jälitustoimingu luba võib hõlmata ka mitut eriliigilist jälitustoimingut. Eeltoodust tulenevalt on võimalik koostada alljärgnev tabel:

Tabel 1. Registreeritud kuriteod, jälitustoimingu load ja KrMS § 126[7] jälitustoimingute arv aastatel 2021-2024.

| Allikas ja aasta | Registreeritud kuritegusid | Jälitustoimingu lube (rahuldatud load) | KrMS § 126[7] toiminguid |
|---|---|---|---|
| Prokuratuuri aastaraamat 2024[11] | 28345 | 753 | 942 |
| Prokuratuuri aastaraamat 2023[12] | 27418 | 999 | 666 |
| Prokuratuuri aastaraamat 2022[13] | 25663 | 1228 | 1027 |
| Prokuratuuri aastaraamat 2021[14] | 25982 | 1360 | 890 |

*Lahtris „KrMS § 126[7] toiminguid" nimetatud arv saadakse liites kokku aastaraamatute statistikas olevad lahtrites „telefoni pealtkuulamine" ja „muu teabe salajane pealtkuulamine või -vaatamine" väljatoodud arvud.*

Esitatud andmete puhul tuleb silmas pidada ka asjaolu, et registreeritud kuritegude arv on igal aastal erinev, mistõttu on korrektseks võrdluseks oluline korrigeerida jälituslubade ja -toimingute arv registreeritud kuritegude arvuga. Selleks arvutas autor välja jälitustoimingu lubade ja KrMS § 126[7] toimingute sagedus aastas registreeritud kuritegude arvu suhtes (valem: JT lubade või KrMS § 1267 toimingute arv ÷ registreeritud kuritegude arv · 100%). Saadud tulemused ümardati kahe komakohani ning esitati alloleva tabelina, tuues välja ka sageduse protsendi muutus võrreldes eelneva aastaga:

[11] Nahkur-Tammiksaar, D.; Zautin, V. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2024. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2024/kriminaalmenetluse-statistika (14.04.2025).
[12] Nahkur-Tammiksaar, D.; Pern, T; Uku; H. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2023. Veebis: https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2023/kriminaalmenetluse-statistika (14.04.2025).
[13] Nahkur-Tammiksaar, D.; Uku; H. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2022. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2022/kriminaalmenetluste-statistika (14.04.2025).
[14] Nahkur-Tammiksaar, D.; Uku; H. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2021. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2021/kriminaalmenetluse-statistika (14.04.2025).

Tabel 2. Registreeritud kuritegude, jälitustoimingu lubade ja KrMS § 126[7] jälitustoimingute sageduse protsent

| Aasta | Registreeritud kuritegusid | JT lube antud | KrMS § 127[7] toimingut | Jälitustoimingu lubade sagedus | KrMS § 126[7] toimingute sagedus |
|---|---|---|---|---|---|
| 2024 | 28345 | 753 | 942 | 2,66% (-0,98%) | 3,32% (+0,89%) |
| 2023 | 27418 | 999 | 666 | 3,64% (-1,15%) | 2,43% (- 1,57%) |
| 2022 | 25663 | 1228 | 1027 | 4,79% (-0,44%) | 4,00% (+ 0,57%) |
| 2021 | 25982 | 1360 | 890 | 5,23% | 3,43% |

Tabelite andmetest võib järeldada, et iga järgneva aastaga on vähenenud nii väljastatud jälitustoimingu lubade arv kui ka jälitustoimingute lubade sagedusprotsent. Seega teostatakse iga aastaga aina vähem jälitustoiminguid nii üleüldiselt kui ka korrigeerituna registreeritud kuritegude arvule. Samas on tabelist näha KrMS § 126[7] toimingute osakaalu järsku tõusu võrreldes eelneva aastaga aastatel 2022 ja 2024, kuigi jälitustoimingute lubade arv registreeritud kuritegude kohta on jäänud stabiilsesse langustrendi. Sellest tulenevalt võib järeldada, et nendel aastatel oli uurimisasutustel ja prokuratuuril suurem vajadus teabe salajaseks pealtkuulamiseks ja -vaatamiseks. Selline vajadus võis olla tingitud võimatusest teostada sideandmete päringuid.

Jälitustoimingute kasutamisele on seatud rangemad kriteeriumid, seda nii *ultima ratio* põhimõtte kui ka toimingu proportsionaalsuse osas. See tähendab, et jälitusasutused ja prokuratuur ei saaks kasutada jälitustoiminguid kõikides nendes olukordades, kus oleks põhjendatud väiksem põhiõiguste riive sideandmete väljanõudmise näol. Samas räägib selle vastu asjaolu, et viimase 3 aasta lõikes on tõusnud kohtu poolt rahuldamata jäetud KrMS § 126[7] toimingute taotluste arv – 2024. aastal jäeti rahuldamata 42 taotlust, 2023. aastal 25 taotlust ning 2022. aastal 23 taotlust. Selle põhjuseks võib olla jälitusasutuste ja prokuratuuri vajadus kasutada rohkem jälitustoiminguid sideandmete väljanõudmise asemel.

Eeltoodu statistika alusel saaks püstitada hüpoteesi, et KrMS § 126[7] toimingute osakaalu järsk tõus on tingitud uurimisasutuste ja prokuratuuri vajadusest asendada sideettevõtjale tehtavad päringud muu asjakohase toiminguga, nagu seda on teabe pealtkuulamine ja -vaatamine. Seda kinnitab ka prokuratuur ise. Riigi peaprokurör sõnas 11.04.2025 prokuratuuri üldkogul, et „*vildaka sideandmete regulatsiooni tõttu ei või jääda massiliselt kelmused tuvastamata. Samas peaks vältima olukorda, kus kuritegude avastamiseks ei ole muu võimalust, kui hakata sideandmete kogumise ja kasutamise asemel tegema massiliselt toiminguid, mis on*

*lõppkokkuvõttes isikute õigusi oluliselt rohkem piiravad*“[15]. Selline väide omakorda viitab sideandmete väljanõudmise asendamisele intensiivsemate toimingutega.

Tagamaks proportsionaalset ning põhjendatud ligipääsu sideandmetele üksnes vältimatult vajalikus ulatuses tuleb Eesti sideandmete säilitamise ja kasutamise regulatsioon viia kooskõlla Euroopa Liidu õigusega. Selleks tuleb aga esmalt tuvastada, milles seisnevad regulatsiooni vastuolud Euroopa Liidu õigusega ning milliste kriteeriumite alusel saab paika panna regulatiivsed muudatused.

### 1.2. Sideandmete üldise ning vahet tegemata säilitamise direktiivi tühistamine

Järgnevalt tutvustab autor olulisemaid arenguid Euroopa Kohtu ning Eesti kohtusüsteemi praktikas puutuvalt nii sideandmete säilitamise kui ka kasutamise regulatsiooni. Käsitletavate kohtulahendite paremaks mõistmiseks Eesti õiguse kontekstis tuleb esmalt tutvuda sideandmete laussäilitamist kohustava ESS § $111^1$ kehtestamise ajendiga.

ESS § $111^1$ sisenes Eesti õiguskorda 2008. aastal. Kehtestamise ajendiks oli Euroopa Parlamendi ja nõukogu direktiivi 2006/24/EÜ[16] ülevõtmine. Andmete säilitamise direktiivi (ingl k *Data Retention Directive*) nime kandev direktiiv 2006/24/EÜ käsitles üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist. Antud raamistik kohustas EL liikmesriike kehtestama siseriiklikud normid, mis kohustavad kõikide sideandmete säilitamist vähemalt 6 ning maksimaalselt 24 kuud pärast nende tekkimist, tulenevalt direktiivi artiklist 6. Säilitamise eesmärgiks oli direktiivi artikli 1 alusel tagada uurimis- ja julgeolekuasutuste tõhus ligipääs kõikidele sideandmetele selleks, et avastada, uurida ning menetleda raskeid kuritegusid, sealhulgas võidelda julgeolekuohtude ning terrorismiga. Seejuures ei nähtud direktiivis ette vajadust kehtestada eeluurimiskohtuniku kontroll enne sideandmete väljanõudmist. Andmete säilitamise direktiivi artiklist 5 tuleneb ka säilitatavate andmete valdkonnapõhine loetelu, mis sõnastati ESS § $111^1$ lõigetes 2 ja 3.

[15] Prokuratuur. Riigi peaprokuröri kõne refereering sotsiaalvõrgustikus Facebook. Veebis: https://www.facebook.com/prokuratuur.ee/posts/pfbid03zkbszfpVokmJ6LKVYK7dEh98yKJg5HtSgirjgdR5uw7YwgM2AfaQB2gkvZnjWFEl (14.04.2025).

[16] 15. märtsi 2006 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.

Sideandmete laussäilitamist lubanud direktiivi 2006/24/EÜ ja selle harmoniseerimise tulemusena tekkinud siseriiklikke õigusnorme, nagu seda on ka ESS § 111[1], on korduvalt kritiseeritud kõikide isikute sideandmete vahet tegemata laussäilitamise lubamise eest. Laussäilitamise regulatsiooni kritiseerinud Iirimaa privaatsusõigusi kaitsev ühendus *Digital Rights Ireland* esitas kaebuse Iiri esimese astme kohtule *High Court* mitme Iirimaa ministeeriumi vastu küsimuses, kas sideandmete üldine ning vahet tegemata säilitamine on õiguspärane[17]. Sarnase sisuga vaidlus leidis aset ka Austria Vabariigis. Nimelt esitas Kärnteni liidumaa valitsus ning 11130 eraisikut kaebuse Austria Vabariigi põhiseaduskohtule *Verfassungsgerichtshof* föderaalvalitsuse vastu, paludes tühistada föderaalseadusega kehtestatud sideandmete laussäilitamise kohustus[18]. Mõlema riigi kohtud esitasid Euroopa Kohtule eelotsusetaotlused, mis liideti Euroopa Kohtu presidendi 11.06.2013 määrusega üheks menetluseks. Nõnda, pärast kirjalikku menetlust ja 09.07.2013 toimunud istungit langetas Euroopa Kohtu suurkoda 08.04.2014 otsuse liidetud kohtuasjades C-293/12 ja C-594/12 (*Digital Rights Ireland et al)*.

Euroopa Kohus leidis, et sideandmete säilitamine on sobiv meede täitmaks andmete säilitamise direktiiviga 2006/24 taotletavat eesmärki (võitlus raske kuritegevusega)[19]. Samas mõõdukuse kontekstis sõnas kohus viitega varasemale praktikale, et igasugune eraelu puutumatuse riive ning seda eriti isikuandmete kaitse valdkonnas peab olema piiritletud üksnes rangelt vajaliku riivega[20]. Otsuses leiti, et direktiiv 2006/24 sätestas üldise kohustuse säilitada kõikide isikute kõiki sideandmeid ning ei kehtestanud mingisugust erisust säilitatavate andmete suhtes, näiteks arvestades eesmärki võidelda raske kuritegevusega[21]. See tähendab, et direktiiv kohaldus ka sellistele isikutele, kelle kohta puuduvad viited või tõendid sellele, et nende tegevus on mingilgi moel seotud raskete kuritegude toimepanemisega[22].

Kohus kritiseeris ka seda, et direktiiv ei nõua seose olemasolu säilitatavate andmete ning avalikule korrale või julgeolekule esineva ohu vahel. Selleks võinuks direktiiv piirata andmete säilitamist üksnes nende andmetega, mis on seotud ajaliselt, geograafiliselt või isikuliselt mõne raske kuriteoga. Äärmisel juhul võinuks säilitamine olla piiratud ka isikutega, kelle sideandmete säilitamine võib mingil muul põhjusel aidata kaasa võitlusele raske

[17] EKo C-293/12 ja C-594/12, *Digital Rights Ireland et al*, ECLI:EU:C:2014:238, p 17-18.
[18] *Ibid*, p 19-21.
[19] *Ibid*, p 49.
[20] *Ibid*, p 52.
[21] *Ibid*, p 57.
[22] *Ibid*, *p* 58.

kuritegevusega[23]. Direktiivile heideti ette ka seda, et raske kuriteo mõiste jääb iga liikmesriigi enda defineerida.[24]

Kohus adresseeris ka sideandmete üldise säilitamisega kaasnevat põhiõiguste riivet. Kokkuvõtvalt asus kohus seisukohale, et direktiiv 2006/24 ei sätesta selgeid ja täpseid reegleid, mis reguleeriksid Euroopa Liidu põhiõiguste harta[25] (edaspidi ka: harta) artiklites 7 ja 8 ette nähtud põhiõiguste riive ulatust[26]. Nendeks õigusteks on era- ja perekonnaelu, kodu ja sõnumite puutumatusele (sõnumite saladusele) vastavalt harta artiklile 7 ning õigusele isikuandmete kaitsele vastavalt harta artiklile 8. Kuigi põhiõiguste harta artikli 8 lõige 2 nõuab isikuandmete töötlemist asjakohaselt ning kindlaksmääratud eesmärkidel leidis Euroopa Kohus, et direktiiv 2006/24 ei näe ette piisavas ulatuses tagatisi sideandmetele ebaseadusliku ligipääsu või õigustatud ligipääsu kuritarvitamise eest. Nimelt ei sisalda direktiiv erireegleid suure andmehulga või delikaatsete andmete töötlemise korral, samuti ei näe direktiiv ette erireegleid andmete säilitamise taristu küberturbe reeglite osas ning ei nõudnud nende andmete säilitamist EL territooriumil[27].

Eeltoodud probleemid kujutavad kohtu hinnangul põhiõiguste harta artiklite 7 ja 8 ebaproportsionaalset riivet ehk harta artikli 52 lõikes 1 olevate põhiõiguste piiramise nõuete rikkumist. Seetõttu tunnistas Euroopa Kohus andmete laussäilitamist nõudva direktiivi 2006/24/EÜ[28] kehtetuks. Seejuures mõjutas otsus vaid EL õigusest tulenevat kohustust sideandmete säilitamist – otsusega ei mõjutatud otseselt liikmesriikide siseriiklikus õiguses olevaid sideandmete säilitamist ettenägevaid norme.

Käesolevast kohtuotsusest juurdus ka Euroopa Kohtu praktika sideandmetega kaasneva eraelu puutumatuse riive kohta. Nimelt selgitas kohus, et sideandmed kogumis võimaldavad teha väga täpseid järeldusi isikute eraelu kohta, näiteks isikute harjumuste, elukoha, harrastatavate tegevuste, sotsiaalsete tegevuste ja grupikuuluvuse kohta[29]. Samuti tõi kohus esmakordselt välja ka võimalikud alternatiivid üldisele ning vahet tegemata säilitamisele. Euroopa Kohtu hinnangul peab esinema mingi seos säilitatavate andmete ja avalikku julgeolekut ohustava ohu vahel – selleks peaks regulatsioon piirama sideandmete säilitamist andmetega konkreetse

[23] *Ibid*, p 59.
[24] *Ibid*, p 61.
[25] Euroopa Liidu põhiõiguste harta, 2016/C 202/02.
[26] *Ibid*, p 65.
[27] *Ibid*, p 66-68.
[28] *Ibid*, p 69.
[29] *Ibid*, p 27.

ajavahemiku, geograafilise piirkonna või raskete kuritegude toimepanemisega seotud isikute kohta[30].

Sisuliselt oli *Digital Rights Ireland et al* otsuse järel kujunenud ka esimene Riigikohtu seisukoht sideandmete kui tõendi lubatavuse kohta süüteomenetluses. Sideandmete säilitamise regulatsiooni suhtes oli Riigikohus avaldanud esimest arvamust juba 2015. aasta algul. Nimelt käsitles Riigikohtu kriminaalkolleegium sideandmete tõendina kasutamise problemaatikat 23.02.2015 otsuses 3-1-1-51-14. Koos otsusega esitasid oma eriarvamuse ka riigikohtunikud Saale Laos ja Eerik Kergandberg[31]. Otsuses selgitas Riigikohus, et kuigi Euroopa Kohus tunnistas direktiivi 2006/24/EÜ kehtetuks, ei tähenda see automaatselt vastava siseriikliku õiguse kehtetust. Nimelt on iga EL liikmesriigi seadusandjal teatud kaalutlusõigus oma siseriikliku regulatsiooni kujundamisel. Sellest tulenevalt asus Riigikohus kontrollima kas sideandmete kriminaalmenetluses kasutamist võimaldavad õigusnormid on kooskõlas põhiseadusega[32]. Kolleegium avas põhiseaduspärasuse küsimuse eeskätt läbi toimingu tegemise ajal kehtinud KrMS § 117 ning leidis, et nii antud õigusnorm kui ka ESS § $111^1$ seavad piisavas ulatuses piiranguid andmetele ligi pääsemiseks ning nende kasutamiseks, et kogu toimingut võiks lugeda põhiseaduspäraseks. Seejuures on oluline, et kolleegiumi lahendis on põhifookus suunatud hetkel kehtetule KrMS §-le 117, mitte ESS §-le $111^1$.

Eriarvamuses tõid riigikohtunikud aga välja, et sideandmete kasutamist puudutava regulatsiooni põhiseaduspärasuse hindamisel ei ole põhirõhk mitte andmete kasutamist käsitleva õigusnormil (KrMS § 117), vaid andmete säilitamist ja selle tingimusi reguleerival ESS regulatsioonil. Eriarvamuse esitanud riigikohtunike hinnangul on vähemalt kaheldav see, kas kriminaalmenetluses kehtivad kitsendused ja piirangud aitavad tagada elektroonilise side seaduse alusel laussäilitatud andmete kasutamise põhiseaduspärasust[33].

### 1.3. Sideandmete üldise ning vahet tegemata säilitamise lubatavus liikmesriikide õiguses

Euroopa Kohtu otsus *Digital Rights Ireland et al* asjas tunnistas kehtetuks direktiivi 2006/24/EÜ, kuid selle alusel kehtestatud siseriiklike norme mõjutas eeskätt hilisem lahend, so 21.12.2016 Euroopa Kohtu suurkoja otsus liidetud kohtuasjades C-203/15 ja C-698/15 (*Tele2 Sverige AB et al)*[34].

[30] *Ibid*, p 59.
[31] RKKKm 3-1-1-51-14 koos riigikohtunike Saale Laose ja Eerik Kergandbergi eriarvamusega.
[32] RKKKm 3-1-1-51-14, p 21.
[33] RKKKm 3-1-1-51-14, riigikohtunike Saale Laose ja Eerik Kergandbergi eriarvamuse p 6.
[34] EKo C-203/15 ja C-698/15, *Tele2 Sverige AB et al*, ECLI:EU:C:2016:970.

Käesolevas kohtuasjas on olulisel kohal direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris[35]. Antud direktiiv seab liikmesriikidele kohustuse tagama siseriikliku õigusega:

1. üldkasutatava elektroonilise side ja sellega seotud liiklusandmete konfidentsiaalsuse (artikkel 5);
2. liiklusandmete kustutamise või anonümiseerimise pärast seda, kui neid ei ole enam vaja side edastuseks (artikkel 6);
3. võimaluse helistajale loobuda tema numbri edastamisest kõnepõhiselt (artikkel 7);
4. asukohaandmete töötlemise üksnes anonümiseeritult või klientide nõusolekul lisateenuse osutamiseks (artikkel 9).

Direktiiv loob ka võimaluse eelnevate privaatsustagatiste piiramiseks. Nimelt võivad liikmesriigid võtta artikli 15 lõike 1 alusel vastu seadusandlikke meetmeid eeltoodud õiguste ja kohustuste piiramiseks. Seda juhul, kui see on otstarbekas ja proportsionaalne abinõu riigi julgeoleku, riigikaitse või avaliku korra tagamiseks, samuti kuritegude või elektroonilise side süsteemide väärkasutamise avastamiseks, ennetamiseks, uurimiseks ning menetlemiseks.

Rootsi Kuningriigi sideettevõte Tele2 Sverige ning Rootsi Kuningriigi Posti- ning Telekomiameti vahel tekkis vaidlus, kuna Tele2 Sverige teatas viimasele sideandmete säilitamise lõpetamisest ning juba säilitatud sideandmete kustutamisest. Sideandmete säilitamise kohustus tulenes, sarnaselt Eestile, direktiivist 2006/24/EÜ ülevõetud siseriiklikust normist. Tele2 Sverige põhjendas oma otsust sellega, et Rootsi siseriiklik õigusnorm on vastuolus EL põhiõiguste hartaga ning ei täida direktiivis 2002/58/EÜ sätestatud eesmärke eraelu puutumatuse piiramisel[36]. Rootsi Kuningriigis asja menetlenud kohus esitas eelotsusetaotluse, milles küsis Euroopa Kohtult kas liiklus- ja asukohaandmete vahet tegemata sideandmete säilitamist kohustav siseriiklik õigusnorm on kooskõlas direktiivi 2002/58 artikli 15 lõikega 1[37], mille kohaselt on direktiivi eesmärgiks tagada võrdväärne eraelu puutumatuse kaitse isikuandmete töötlemise puhul elektroonilise side sektoris.

Teine vaidlus tekkis UK-s, kus mitmed eraisikud palusid kontrollida UK siseriikliku sideandmete säilitamist nõudva normi õiguspärasust, eeskätt EL põhiõiguste harta artiklite 7 ja

[35] 12.07.2002 Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) - EÜT L 201, 31.07.2002, p. 37–47.
[36] *Ibid*, p 44-50.
[37] EKo C-203/15 ja C-698/15, *Tele2 Sverige AB*, p 51.

8 ning Inimõiguste ja põhivabaduste kaitse konventsiooni[38] artikli 8 suhtes[39]. Seega olid mõlema riigi eelotsusetaotlused suunatud sellele, kas sideandmete (eeskätt liiklus- ja asukohaandmete) üldine ja vahet tegemata säilitamine siseriikliku õiguse alusel on igal juhul ebaproportsionaalne põhiõiguste harta artiklite 7 ja 8 riivamine.

Eelotsusetaotluste sarnase problemaatika tõttu liideti kohtuasjad Euroopa Kohtu presidendi 10.03.2016 määrusega üheks menetluseks. Nõnda, pärast kirjalikku menetlust ja 12.04.2016 toimunud istungit langetas Euroopa Kohtu suurkoda 21.12.2016 otsuse käesolevas asjas. Kohtuotsusega kehtestas kohus kriteeriumid, millele tuginedes on võimalik kontrollida liikmesriigi säilitamisnormide vastavus direktiivi 2002/58 artikli 15 lõikele 1 ning harta artiklites 7 ja 8 olevate põhiõiguste riivamise nõuetele, mis on omakorda kehtestatud harta artikli 52 lõikega 1. Selleks tuli kohtul tasakaalustada eraelu puutumatuse ja isikuandmete kaitse julgeoleku tagamise ja kuritegude tõkestamise suhtes. Kohus lahendas antud probleemi käsitledes eraldi sideandmete säilitamist ja kasutamist, nagu seda teeb ka autor läbivalt käesolevas töös.

Sideandmete säilitamise osas langetas kohus otsuse, et direktiivi 2002/58 artikli 15 lõikega 1 on vastuolus kõik liikmesriikide õigusnormid, mis näevad ette kohustuse kõikide abonentide ja registreeritud kasutajate liiklus- ja asukohaandmete üldise ning vahet tegemata säilitamise võitluseks kuritegevusega[40].

Kohus kordas üle, et kuigi direktiivi 2002/58 artikli 15 lõige 1 lubab liikmesriigil piirata üldreegli ehk artikliga 5 sätestatud sideandmete konfidentsiaalsuse säilitamise kohustuse, peab õiguste piiramine olema kooskõlas riigi julgeoleku kaitsmise eesmärgiga. Riigi julgeoleku kaitsmise eesmärk hõlmab aga endas julgeoleku ja avaliku korra tagamist, riigikaitset, küberkaitset ning kuritegude menetlemist[41]. Antud direktiivi artikkel 15 kehtestab ka täpsemad nõuded sideandmete konfidentsiaalsuse piiramisele – taoline riive peab olema vajalik, otstarbekas ja proportsionaalne riigi julgeoleku kaitsmise eesmärgi saavutamiseks ning see peab toimuma üksnes piiratud aja jooksul[42].

[38] Inimõiguste ja põhivabaduste kaitse konventsioon - RT II 2010, 14, 54.
[39] EKo C-203/15 ja C-698/15, *Tele2 Sverige AB*, p 52.
[40] *Ibid*, p 112.
[41] *Ibid*, p 88-90.
[42] *Ibid*, p 95.

Vaidlusalused üldise säilitamise normid hõlmavad kõiki kehtetus direktiivis 2006/24 käsitletud andmeliike[43]. Tuginedes varasemale seisukohale *Digital Rights Ireland et al* asjas kordas kohus üle seda, et sideandmed kogumis võimaldavad teha täpseid järeldusi isikute eraelu kohta, mis omakorda toob kaasa eriti raske põhiõiguste harta artiklis 7 ja 8 sätestatud õiguste riive[44]. Antud riive on kohtu hinnangul niivõrd raske, et kohus pidas põhjendatuks lubada liiklus- ja asukohaandmete säilitamist üksnes võitluseks raske kuritegevusega[45] - selline käsitlus tuleneb ka kehtetu direktiivi 2006/24 artikli 1 lõikest 1. Kohus leidis, et eelnevalt käsitletud põhiõiguste riive erilise raskuste tõttu ei ole raskete kuritegude tõkestamise sõltuvus sideandmetest kui üldine vajaduse põhjendus piisav selleks, et liiklus- ja asukohaandmeid saaks säilitada üldiselt ning vahet tegemata[46]. Seega väljuvad üldist ning vahet tegemata säilitamist lubavad siseriiklikud normid rangelt vajaliku piiridest, mistõttu ei ole nad demokraatlikus ühiskonnas põhjendatud [47].

Otsusega andis Euroopa Kohus mõista, et sideandmeid võib säilitada sihistatult võitluseks raske kuritegevusega juhul, kui andmete säilitamine on andmete liigi, sidevahendite, abonentide ning säilitamise kestuse osas piiratud rangelt vajalikuga[48]. Kohus ei sisustanud millisel moel võiks sihistamine täpselt toimuda, kuid tõi välja mitmed kriteeriumid millele sihistatud säilitamine peab vastama. Esiteks peab see tagama mõjutatud isikutele garantiid, mis võimaldavad kaitsta nende isikuandmeid kuritarvitamise eest[49]. Teiseks võivad sihistatud säilitamise kriteeriumid varieeruda konkreetse meetme kontekstis, kuid andmete säilitamine peab igal juhul rajanema objektiivsetel kriteeriumitel, mis loovad seose säilitatavate andmete ja taotletava eesmärgi vahel ehk võimaldavad piirata tõhusalt meetme ulatust ehk puudutatud isikute ringi. Sellisteks viisideks saaks olla isiku või geograafilise asukoha põhine sihistatud säilitamine[50]. Eeltooduga sisustas Euroopa Kohus meetmed, mis võimaldavad tagada sideandmete säilitamise mõõdukuse riivatavate põhiõiguste suhtes.

Lisaks pidas kohus lubatavaks säilitada sideandmed piiratud ulatuses ärilistel eesmärkidel. Nimelt selgitas kohus, et direktiivi 2002/58 artikli 6 kohaselt on lubatud liiklusandmete

[43] *Ibid*, p 97.
[44] *Ibid*, p 98-100.
[45] *Ibid*, p 102.
[46] *Ibid*, p 103.
[47] *Ibid*, p 107.
[48] *Ibid*, p 108-109.
[49] *Ibid*, p 109.
[50] *Ibid*, p 110-111.

töötlemine ja säilitamine ulatuses, mis on vajalik arvete koostamiseks, teenuste turustamiseks ning lisaväärtusteenuste osutamiseks[51].

Otsuse teises plokis asus kohus analüüsima sideandmete kasutamise regulatsiooni. Kohus langetas otsuse, et direktiivi 2002/58 artikli 15 lõikega 1 on vastuolus kõik liikmesriikide õigusnormid, mis võimaldavad ametiasutuste juurdepääsu sideteenusega seotud liiklusandmetele ja asukohaandmetele ning mis:

- ei piira juurdepääsu sideandmetele kriminaalmenetlustes üksnes võitluseks raske kuritegevusega,
- ei nõua kohtulikku või sõltumatu haldusasutuse eelnevat kontrolli enne andmetele juurdepääsu ja
- ei nõua, et sideandmeid säilitataks EL territooriumil[52].

Kuna liiklus- ja asukohaandmete raskest riivest tuleneva raske kuritegevusega võitlemise kriteeriumist rääkis kohus säilitamise regulatsiooni plokis, ei peatutud sellel pikemalt. Küll aga selgitas kohus täpsemalt sideandmetele ligipääsu puudutavaid aspekte. Esiteks sõnas kohus viitega eelmises plokis öeldule, et sideandmetele juurdepääsu võimaldamisel tuleb tagada, et juurdepääs sideandmetele jääb üksnes vajaliku piiridesse[53]. See seab omakorda liikmesriikidele kohustuse kehtestada konkreetsed materiaal- ja menetlusõiguslikud tingimused, mille korral on õigustatud riigiasutuste ligipääs säilitatavatele sideandmetele[54].

Nende tingimuste järgimise kontrollikohustus peab Euroopa Kohtu hinnangul lasuma liikmesriigi kohtusüsteemil või sõltumatul haldusasutusel. Selleks peab juurdepääsu sooviv asutus esitama põhjendatud taotluse kohtule või sõltumatule haldusasutusele. Taotletav eesmärk peaks olema suunatud ennekõike kuriteo ennetamisele, avastamisele või menetlemisele[55]. Liikmesriikidele seati ka kohustus kontrollida kas sideandmete kasutamisega kaasnev isikuandmete töötlemine tagab põhiõiguste harta artikli 8 lõikega 3 kehtestatud miinimumkaitse. Miinimumkaitse nõue peab võimaldama, et riivatud isikutel on õigus esitada liikmesriigi järelevalveasutusele taotlus neid puudutavate andmete kaitseks[56].

[51] *Ibid*, p 86.
[52] *Ibid*, p 125.
[53] *Ibid*, p 116.
[54] *Ibid*, p 118.
[55] *Ibid*, p 120.
[56] *Ibid*, p 123.

### 1.4. Sideandmete säilitamise viisid, mis on kooskõlas Euroopa Liidu õigusega

*Tele2 Sverige et al* otsuse tõlgendamiseks oli vaja luua selgust selles, kuidas peab toimuma sideandmete sihistatud kogumine. Selleks oli vaja tuvastada Euroopa Kohtu poolt aktsepteeritavad sihistatud kogumise täpsemad kriteeriumid. Samuti ei loonud *Tele2 Sverige et al* otsus selgust selles osas kas liiklus- ja asukohaandmete üldise ning vahet tegemata säilitamise keeld laieneb vaieldamatult ka riigi julgeoleku kaitsmise eesmärgile. Lisaks jäi ebaselgeks mismoodi peaks toimuma identifitseerimisandmete (mis ei ole liiklus- ja asukohaandmete osaks) säilitamine. Nendele küsimustele vastas Euroopa Kohus 06.10.2020 otsusega *La Quadrature du Net et al* asjas[57].

Antud kohtuasja ajendiks olid kolm eraldiseisvat vaidlust, millest kaks leidsid aset Prantsuse Vabariigis ning üks Belgia Kuningriigis. Esiteks olid Prantsuse isikuandmete kaitse eest võitlevad ühendused palunud riigi kõrgeimalt halduskohtult tühistada riiklikud dekreedid, mis võeti vastu prantsuse sisejulgeoleku seadustiku luuretegevust puudetavate normide rakendamiseks. Sisejulgeoleku seadustik seadis sideettevõtjatele kohustuse rakendada oma võrkudes automatiseeritud andmetöötlust selleks, et julgeolekuasutuse taotlusel oleks võimalik tuvastada sidevõrgus sellised sideühendused, millest võis ilmneda terrorismi oht. Liikmesriigi kohus tuvastas, et sisejulgeoleku seadustikuga sätestatud säilitamiskohustus ning julgeolekuasutustele antud õigus pääseda ligi nendele andmetele kuulub direktiivi 2002/58 kohaldamisalasse[58]. Vaidluse lahendamiseks esitas siseriiklik kohus Euroopa Kohtule eelotsusetaotluse, milles palus selgitada kas sideandmete üldine ja vahet tegemata säilitamine võitluseks suure ja püsiva ohuga riigi julgeolekule (nt terrorism) on lubatav direktiivi 2002/58 artikli 15 lõike 1 kontekstis. Samuti paluti kohtul selgitada kas EL õigus lubab kindlaksmääratud isikute kohta liiklus- ja asukohaandmete kogumist reaalajas juhul, kui sideettevõtjale ei panda konkreetset andmete säilitamise kohustust[59].

Teine vaidlus tekkis samuti Prantsuse isikuandmete kaitse eest võitlevate ühenduste ning riigi. Vaidluse põhjuseks oli asjaolu, et peaminister ignoreeris ühenduste taotlust tunnistada kehtetuks siseriiklikud internetiteenuse identifitseerimisandmete laussäilitamist lubavad õigusnormid, mis ei ole ühenduste hinnangul kooskõlas EL õigusega. Samuti paluti käesolevas vaidluses kõigi sideandmete üldist ning vahet tegemata säilitamist lubavad õigusnormid[60].

[57] EKo C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net et al*, ECLI:EU:C:2020:791.
[58] *Ibid*, p 56-61.
[59] *Ibid*, p 68.
[60] *Ibid*, p 69-72.

Vaidluses tugineti ka Euroopa Kohtu varasemale seisukohale *Tele2 Sverige et al* asjas, kuid mäletatavasti ei puudutanud see identifitseerimisandmeid. Seega esitas siseriiklik kohus eelotsusetaotluse, milles muuhulgas palus selgitada kas EL õigusega on vastuolus identifitseerimisandmete ennetav üldine ning vahet tegemata säilitamine[61].

Kolmas vaidlus leidis aset Belgia Kuningriigis, kus mitmed isikud esitasid riigi konstitutsioonikohtule kaebused, milles väideti, et siseriiklikud sideandmete säilitamisnormid ei järgi EL õigusest tulenevaid nõudeid, mida käsitleti nii *Digital Rights Ireland et al* kui ka *Tele2 Sverige et al* asjades. Siseriiklik kohus tuvastas, et säilitamisnormide eesmärgiks on lisaks võitluseks kuritegevusega ka riigi julgeoleku ning avaliku korra tagamine.[62]. Belgia konstitutsioonikohus esitas Euroopa Kohtule eelotsuse taotluse, milles palus hinnata kas EL õigusega on vastuolus ka liiklus- ja asukohaandmete üldine ning vahet tegemata säilitamine riigi julgeoleku ja avaliku korra tagamise ning riigi- ja küberkaitse eesmärkidel. Sarnane küsimus esitati ka riigile pandud alaealiste seksuaalse kuritarvitamisega võitlemise kohustuse kontekstis[63].

Käesolevad vaidlused liideti Euroopa Kohtu presidendi otsusega ühiseks menetluseks ning 06.10.2020 langetas Euroopa Kohus otsuse käesolevas liidetud kohtuasjas. Otsusega andis Euroopa Kohus juhised tõlgendamaks direktiivi 2002/58/EÜ artikli 15 lõiget 1 õiguspäraselt.

Esiteks leidis kohus, et direktiivi 2002/58 artikli 15 lõikega 1 on vastuolus kõik seadusandlikud meetmed, mis näevad ette liiklus- ja asukohaandmete üldise ning vahet tegemata säilitamise sõltumata sellest mis direktiivi artikli 15 lõikes 1 nimetatud eesmärgil (avaliku korra tagamine, riigi- ja küberkaitse tagamine või kuritegude menetlemine), välja arvatud riigi julgeoleku tagamiseks, seda tehakse[64]. Kuigi kohus jättis oma otsusest välja otsesõnalise keelu säilitada liiklus- ja asukohaandmeid üldiselt riigi julgeoleku tagamiseks, seadis kohus sellisele säilitamisele väga ranged tingimused. Kohus selgitas, et riigi julgeoleku tagamine või kaitsmine on kõige tähtsam eesmärk direktiivi 2002/58 artikli 15 lõikes 1 nimetatud eesmärkidest. See omakorda õigustab intensiivsemat põhiõiguste riivet riigi julgeoleku tagamise eesmärgil, kuid ka selle eesmärgi täitmiseks tuleb kohtu hinnangul järgida põhiõiguste harta artikli 52 lõikest 1 tulenevaid nõudeid[65].

[61] *Ibid*, p 73.
[62] *Ibid*, p 74-75.
[63] *Ibid*, p 79.
[64] *Ibid*, p 168.
[65] *Ibid*, p 136.

Otsusega anti konkreetne selgitus tingimuste kohta, millele peab vastama sideandmete üldine ning vahet tegemata säilitamine riigi julgeoleku tagamiseks sellisel moel, et see järgiks harta artikli 52 lõikest 1 tulenevaid nõudeid. Selleks peab sideandmete üldise ning vahet tegemata säilitamise kohustus:

- kestma sellise piiratud aja vältel, mis on vältimatult vajalik ning mitte olema süstemaatiline ja
- tuginema konkreetsetele asjaoludele, mis võimaldavad järeldada, et liikmesriik seisab silmitsi tema julgeolekut ähvardava tõelise ja vahetu või ettearvatava suure ohuga, mis ohustab riigi põhifunktsioone ja põhihuve (põhiseaduslikku korda)
- olema tõhusalt kontrollitav kohtu või sõltumatu haldusasutuse poolt[66]

Teiseks leidis Euroopa Kohus, et lisaks võitlusele kuritegevusega ei saa liiklus- ja asukohaandmete üldine ja vahet tegemata säilitamine olla lubatav ka avaliku korra tagamiseks[67]. Kohus sõnastas oma otsuses ka aktsepteeritavad liiklus- ja asukohaandmete säilitamise viisid. Nimelt selgitas kohus, et sideandmete säilitamisega kaasnev raske riive võib olla õigustatud siis, kui see on toimunud eesmärgipäraselt[68]. Eesmärgipärasus seisneb käesoleval juhul selles, et säilitamine piiratakse andmetega, mis „*kuuluvad kindlasse ajavahemikku ja/või kindlasse geograafilisse piirkonda ja/või puudutavad teatavaid isikuid, kes võivad olla mingil viisil seotud raske kuriteoga, ega isikutega, kelle andmete säilitamine võib muul põhjusel raskete kuritegude vastu võitlemisele kaasa aidata*“[69]. Järelikult on EL õigusega kooskõlas sellised säilitamisnormid, mis seavad kohustuse liiklus- ja asukohaandmete ennetavaks säilitamiseks juhul, kui see on sihistatud konkreetse andmete liigi, sidevahendi või andmesubjektiga ning on piiratud ajaliselt vältimatult vajalikuga[70]. Antud käsitlus ühtib Euroopa Kohtu varasema seisukohaga *Tele2 Sverige et al* asjas.

Kohus tõi välja mõned näited aktsepteeritavast sihistatud säilitamisest. Isikupõhine sihistus võib olla õigustatud isikute suhtes, kes, tuginedes käimasolevas menetluses kogutud andmetele, kujutavad endast ohtu avalikule korrale (seos kuritegevusega) või riigi julgeolekule[71]. Lubatud on ka geograafiline ehk asukohapõhine sihistus – seda juhul, kui liikmesriik tuvastab, et ühes või mitmes piirkonnas esineb kõrgendatud oht raskete kuritegude ettevalmistamiseks või

[66] *Ibid*, p 137-139.
[67] *Ibid*, p 143.
[68] *Ibid*, p 146.
[69] *Ibid*, p 144.
[70] *Ibid*, p 147.
[71] *Ibid*, p 149.

toimepanemiseks. Sellisteks kohtadeks võivad olla kas piirkonnad kus on suur raskete kuritegude arv või mis on eriti haavatavad raskele kuritegevusele (pidevalt külastatavad avalikud ruumid või transpordisõlmed)[72].

Kolmandaks pidas kohus lubatuks üldise ning vahet tegemata side algatanud IP-aadressi identifitseerimisandmete säilitamise juhul, kui seda tehakse võitluseks raske kuritegevusega ning vältimatult vajaliku säilitamistähtaja jooksul[73]. Muude identifitseerimisandmete puhul pole nende säilitamise korral tegemist raske riivega, eriti olukorras kus nende andmetega ei avaldu sideseansside toimumise faktid ja asjaolud[74]. Seega on Euroopa Kohtu hinnangul EL õigusega kooskõlas seadusandlikud meetmed, mis näevad ette identifitseerimisandmete üldise ning vahet tegemata säilitamise võitluseks kuritegevusega[75] või mis näevad ette side lähtepunktile omistatud IP-aadresside üldise ja vahet tegemata säilitamise võitluseks raske kuritegevusega vältimatult vajaliku säilitamistähtaja jooksul.

Euroopa Kohus sätestas veel ühe aktsepteeritava meetme liiklus- ja asukohaandmete säilitamiseks. Selleks on liiklus- ja asukohaandmete nn kiirsäilitamine võitluseks raskete kuritegudega. Nimelt tõi kohus näitena välja olukorrad, kus andmeid on vaja säilitada kauem kui eelnevalt käsitletud meetmete aluseks olevad asjaolud seda võimaldavad[76]. Selleks võib liikmesriik näha ette võimaluse anda kohtulikult kontrollitavale asutusele õigus kohustada sideettevõtjat säilitama kiirkorras liiklus- ja asukohaandmeid kindlaksmääratud ajaks[77]. Seejuures peab kiirsäilitamine olema piiritletud vältimatult vajalikuga ning täitma kas riikliku julgeoleku kaitsmise või raske kuritegevuse vastu võitlemise eesmärki[78].

Lisaks eeltoodule langetas kohus seisukoha andmete automatiseeritud töötluse ning reaalajas kogumise kohta. Esiteks leidis kohus, et sideandmete automatiseeritud analüüsi kasutamine võib olla lubatud üksnes tõsise julgeoleku korral. Teiseks selgitas kohus, et liiklus- ja asukohaandmete kogumine võitluseks julgeolekuohtudega on lubatud üksnes kohtu või haldusasutuse loal ning seda vaid terrorismiga seotud isikute suhtes[79].

[72] *Ibid*, p 150.
[73] *Ibid*, p 154-156.
[74] *Ibid*, p 157.
[75] *Ibid*, p 159.
[76] *Ibid*, p 160-161.
[77] *Ibid*, p 163.
[78] *Ibid*, p 164.
[79] *Ibid*, p 192.

### 1.5. Sideandmete säilitamise ja kasutamise siseriikliku regulatsiooni õiguspärasus Eestis

Euroopa Kohtu eelkäsitletud otsuste järel tekkis põhjendatud küsimus, kas Eesti siseriiklik sideandmete säilitamise regulatsioon on vastavuses EL õigusega. Ei ole vaidlust selles, et hetkel kehtivas sõnastuses näeb ESS § 111[1] ette kõigi sideandmete, sealhulgas ka liiklus- ja asukohaandmete üldise ning vahet tegemata säilitamise. Selline õigusnorm on aga, tulenevalt Euroopa Kohtu seisukohast *Tele2 Sverige et al* otsuses, vastuolus direktiivi 2002/58 artikli 15 lõikega 1 ning riivab ebaproportsionaalselt põhiõiguste harta artiklites 7 ja 8 sätestatud õigusi. Küll aga ei jõutud Eesti õigusloomes mingite muudatusteni, mis taolist olukorda muudaks.

Kuivõrd ESS § 111[1] ei täitnud eelselgitatud Euroopa Kohtu otsustega seatud kriteeriumid lubatavaks juurdepääsuks sideandmetele, oli igati ootuspärane, et Euroopa Kohtu otsuste järel muutub sideandmete kasutamine Eesti süüteomenetlustes võimatuks. Eesti õiguspraktikasse jõudis eelnimetatud probleem õigepea pärast *Tele2 Sverige et al* otsust, kui Riigikohtus vaidlustati kriminaalasjas 1-16-6179 Tartu Ringkonnakohtu langetatud 17.11.2017 otsus (mis järgnes Viru Maakohtu 06.04.2017 otsusele).

Kassatsioonimenetluses vaidlustas süüdistatava kaitsja muuhulgas seda, et nii maa- kui ringkonnakohus tuginesid sideettevõtjalt saadud andmete protokollidele kui lubatavatele tõenditele. Kaitsja selgitas, et tulenevalt Euroopa Kohtu otsusest *Tele2 Sverige et al* asjas on nii sideandmete säilitamise kohustamine ESS § 111[1] alusel kui ka nende sideandmete kasutamine varguse, arvutikelmuse ning õigusemõistmise mõjutamise tõendamiseks lubamatu[80]. Kuivõrd ESS § 111[1] ning KrMS § 90[1] kuuluvad EL õiguse kohaldamisalasse, otsustas Riigikohus taotleda Euroopa Kohtult eelotsust mitmes menetlust puudutavas küsimuses.

Eelotsuse sisu mõistmiseks on oluline välja tuua ka Euroopa Kohtu suurkoja 02.10.2018 otsus *Ministerio Fiscal et al* asjas C-207/16[81], mida käsitleti ka Riigikohtu eelotsusetaotluse aluseks olevas kohtumääruses. Kokkuvõtvalt asus Euroopa Kohus selles otsuses seisukohale, et direktiiv 2002/58/EÜ kohaldub kriminaalmenetluse raames tehtavatele sideandmete päringutele[82] ning et direktiivi artikli 15 lg 1 esimese lause sõnastus ei piira kuritegude vastu võitlemise eesmärki üksnes raskete kuritegudega, vaid peab silmas kuritegusid üldiselt. Nimelt tähendab see, et väiksemat riivet kaasa toov juurdepääs sideandmetele võib olla põhjendatud

[80] RKKKm 1-16-6179, p 9.
[81] EKo C-207/16, *Ministerio Fiscal et al,* ECLI:EU:C:2018:788.
[82] RKKKm 1-16-6179, 12.11.2018 p 18.

ka üldiselt kuritegude vastu võitlemise eesmärgiga – selliseks väikseks riiveks on näiteks juurdepääs varastatud mobiiltelefonis avatud SIM-kaartide omanike ees- ja perekonnanimele ning aadressile[83].

Riigikohus otsustas taotleda Euroopa Kohtult eelotsust, milles küsis kas *Ministerio Fiscal* otsuse valguses kujutab juurdepääs kahtlustatava mobiiltelefoni sideseansside asukoha- ning ajaandmetele endast alati niivõrd rasket riivet, et juurdepääs sellistele andmetele on põhjendatud üksnes võitluseks raskete kuritegudega[84]. Lisaks küsiti Euroopa Kohtult, kas *Ministerio Fiscal* otsuses käsitletud proportsionaalsuse põhimõte tähendab, et mida raskem on menetletav kuritegu, seda enamatele andmetele on riigiasutuste juurdepääs õigustatud[85]. Samuti küsis Riigikohus ka seda, kas *Tele2 Sverige et al* otsuses käsitletud ning sideandmetele ligipääsu kontrolliva „sõltumatu haldusasutuse" funktsiooni võiks täita ka prokuratuur[86].

Euroopa Kohus vastas oma eelotsusega Riigikohtu esitatud küsimustele[87]. Otsuses rõhutati, et isegi piiratud hulk liiklus- ja asukohaandmeid võivad anda üsna täpset teavet abonendi eraelu kohta[88]. Euroopa Kohus kritiseeris sel korral ka konkreetselt Eesti õigust ning seda ESS § $111^1$ võtmes – kohus tuletas ESS § $111^1$ kontekstis meelde, et liiklus- ja asukohaandmete laussäilitamine on vastuolus direktiiviga 2002/58/EÜ, täpsemalt selle artikli 15 lõikega 1[89]. Oma eelotsuses selgitas kohus, et tõhususe põhimõtte kohaselt peaks liikmesriigi kriminaalkohus jätma arvesse võtmata teabe ja tõendid, mis on saadud liiklus- ja asukohaandmete laussäilitamise teel[90]. Lisaks eeltoodule selgitas kohus, et prokuratuuri ei saa käsitleda sõltumatu haldusasutusena sideandmetele ligipääsu otsustamisel, kuna prokuratuuri ülesanneteks on juhtida kohtueelset menetlust ja esindada riikliku süüdistust kriminaalasjades[91].

Tuginedes Euroopa Kohtu otsusele langetas Riigikohtu kriminaalkolleegium 18.06.2021 otsuse antud kriminaalasjas. Kolleegium toonitas, et vaatamata ESS § $111^1$ lg 2 ja tollel ajaperioodil kehtinud KrMS § $90^1$ vastuolule EL-i õigusega ei too see automaatselt kaasa sideandmete

[83] *Ibid*, p 21.
[84] *Ibid*, p 22.
[85] *Ibid*, p 24.
[86] *Ibid*, p 25.
[87] EKo C-746/18, Prokuratuur, ECLI:EU:C:2021:152.
[88] *Ibid*, p 40.
[89] *Ibid*, p 41-43.
[90] *Ibid*, p 44.
[91] *Ibid*, p 55-57.

protokollide kui tõendi lubamatuks tunnistamist[92]. Kohus asus hindama nende protokollide lubatavust Eesti õiguse ja kohtupraktika kontekstis. Kolleegium möönis, et sideandmete päringutega prokuratuuri loal rikuti eraelu puutumatust, õigust isikuandmete kaitsele ning sõna- ja teabevabadus, mida kehtestavad direktiivi 2002/58/EÜ artikli 15 lõige 1, samuti põhiõiguste harta artiklid 7, 8 ja 11. See omakorda kujutas endast eraelu puutumatuse riivet õigusliku aluseta[93]. Kohus analüüsis ka sideettevõtjalt saadud protokollide kui tõendi lubatavust. Kolleegium leidis, et vaidlusaluses kriminaalasjas ei põhjendanud sideandmete kogumise vältimatut vajalikkust. Seeläbi on sideandmetele juurde pääsemisega rikutud sideandmete üldise ja vahet tegemata säilitamise keeldu ning riivatud ülemääraselt süüdistatava õigust eraelu puutumatusele. Seega on oluliselt rikutud sideandmete kasutamise vältimatu vajalikkuse kriteeriumi nõudeid, mis omakorda teeb sideandmete protokollid lubamatuks tõendiks[94].

Viimaks otsustas kohus ühtlustada õiguspraktikat ning selgitas miks ei tohiks enne seadusemuudatust teha Eestis sideandmete päringuid[95]. Riigikohus kinnitab ESS § $111^1$ lg 2 ja KrMS § $90^1$ lg 2 vastuolu EL-i õigusega ning möönab vajadust tekitada Eesti õiguskorda sideandmete säilitamise õiguslik alus, mis oleks õiguspärane direktiivi 2002/58/EÜ artikkel 15 lg 1 kontekstis[96]. Riigikohtu hinnangul ilmnes arusaam sellest alates 07.10.2020, so pärast Euroopa Kohtu otsust liidetud kohtuasjas *La Quadrature du Net et al*[97]. Kriminaalkollegium selgitas, et selle otsusega kinnitati liiklus- ja asukohaandmete üldise ja vahet tegemata laussäilitamise vastuolu direktiivi 2002/58/EÜ artikli 15 lõikega 1 ning seda sõltumata juurdepääsule (ehk kasutamise poolele) seatud tingimustest[98]. Tulenevalt eeltoodust peab Riigikohus tahtliku ja olulise (ning lubamatu) eraelu puutumatuse riivena sideandmete väljanõudmisi asjades, kus laussäilitatud sideandmete kasutamiseks anti luba alates 07.10.2020 ehk pärast eelnimetatud Euroopa Kohtu otsust. Seejuures ei laiene see kasutaja identifitseerimistunnustega seotud andmete päringule KrMS § $90^1$ lg 1 alusel[99].

Vaatamata tekkinud olukorrale jätkasid uurimisasutused ning prokuratuur püüdlusi kasutamaks sideandmeid kriminaalmenetlustes. Esiteks täiendati kehtivat kasutamise regulatsiooni. Selleks kehtestati KrMS §-is $90^1$ alates 01.01.2022 tingimus, et ligipääs liiklus- ja asukohaandmetele on lubatud üksnes prokuratuuri taotlusel ja eeluurimiskohtuniku loal. Pärast KrMS § $90^1$

[92] *Ibid*, p 51-53.
[93] *Ibid*, p 55.
[94] *Ibid*, p 74-76.
[95] *Ibid*, p 104.
[96] *Ibid*, p 105.
[97] EKo C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net et al*, ECLI:EU:C:2020:791.
[98] RKKKo 1-16-6179, p 106.
[99] *Ibid*.

kooskõlla viimist Euroopa Kohtu praktikaga asus prokuratuur taotlema kohtutelt luba sideandmete väljanõudmiseks ning proovis esitada sideandmeid tõendina kohtus. Samas lähtub ka sideandmete kasutamise sätte uus redaktsioon ESS §-st 111[1], mis ei ole töö koostamise seisuga jätkuvalt kooskõlas Euroopa Kohtu praktikaga.

Sellisele ebamäärasele sideandmete kasutamisele pani punkti siseriiklik kohtusüsteem. Tartu Ringkonnakohus tegi 13.05.2024 määruse kriminaalasjas 1-24-1694[100], milles väljendatud seisukohtade järel loobus prokuratuur täielikult sideandmete väljanõudmisest edaspidistes kriminaalmenetlustes. Antud määruse vaidluseseme keskmes olid teostatud jälitustoiminguid, kuid kaitsjad olid tugevalt kritiseerinud sideandmete kasutamist antud kriminaalasjas. Nimelt ilmnes, et Tartu Maakohus hindas jälitustoimingu loa andmisel põhjendatud kuriteokahtlust tuginedes muuhulgas 25.10.2022 sideettevõtjalt saadud andmete protokollile[101]. Kaitsjad kritiseerisid seda, et kuigi prokuratuur järgis kriminaalmenetluse seadustikust tulenevaid nõudeid (eeskätt sideandmete väljanõudmise normi) ning kohus rahuldas väljanõudmise, saadi selle toiminguga kätte need andmed, mida sideettevõtja säilitas Euroopa Kohtu praktikaga vastuolus oleva ESS § 111[1] alusel[102].

Kohus, meenutades eelselgitatud Euroopa Kohtu ning Riigikohtu praktikat, asus seisukohale, et ESS § 111[1] pole jätkuvalt viidud kooskõlla EL õigusega. Kohus nõustus kaitsjate seisukohaga, et saadud sideandmeid säilitas sideettevõtja üldise säilitamiskohustuse alusel, mitte mõnel muul (nt ärilisel) alusel. Kuna laussäilitamine on vastuolus direktiivi 2002/58/EÜ artikli 15 lõikega 1, leidis kohus, et sideandmete säilitamine on toimunud õigusvastaselt ning prokuratuuril ja kohtul tulnuks jätta ESS § 111[1] kohaldamata. Seega poleks jälitusloa andud maakohus tohtinud tugineda loa andmisel sideettevõtjalt saadud andmetele[103]. Ajendatuna Euroopa Kohtu praktikast on Riigikohtu otsuse järel tekkinud olukord, kus alates 07.10.2020 ei ole Eestis võimalik nõuda kriminaal- ja väärteomenetlustes välja sideandmeid. See omakorda loob vajaduse siseriikliku sideandmete säilitamise (sh kogumise) ning kasutamise (väljanõudmise) regulatsiooni ülevaatamiseks. Et mõista paremini milline peaks olema Eesti sideandmete regulatsioon on asjakohane tutvuda nende liikmesriikide õigusega, kes on juba võtnud kasutusele eelnimetatud kriteeriumitele vastavad regulatsioonid.

[100] TrtRnKm 1-24-1694 13.05.2024. Kohtumäärus on tehtud autorile kättesaadavaks Tartu Ringkonnakohtu 24.03.2025 vastusega autori teabenõudele. Autorile on kättesaadavaks tehtud üksnes sideandmetega seotud juriidilist küsimust puudutav osa ehk määruse punktid 33-38.
[101] *Ibid*, p 33.
[102] *Ibid*, p 33-34.
[103] *Ibid*, p 37.

# 2. EUROOPA LIIDU LIIKMESRIIKIDE LAHENDUSED SIDEANDMETE TÕENDINA KASUTAMISEKS

## 2.1. Sideandmete sihistatud säilitamine Euroopa Liidu liikmesriikides

13.11.2024 avaldasid EJCN ning Euroopa Liidu Kriminaalõigusalase Koostöö Amet (Eurojust) uuringuraporti „*The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*“[104]. Raport käsitleb EL liikmesriikide lahendusi seoses Euroopa Kohtu praktikast tulenevate probleemidega sideandmete kasutamisel tõendina süüteomenetluses ning põhineb sarnasel uuringul, mida Eurojust viis läbi 2017. aastal[105]. Analüüsimetoodika nägi ette küsimustiku edastamist 27-le liikmesriigile. Küsimustik keskendus liikmesriikide kehtivale ning kavandatavale õigusraamistikule, mis käsitleb nii sideandmete säilitamist kui ka nende kasutamist kriminaalmenetlustes. Uuringu esimene osa annab ülevaate Euroopa Kohtu senisest praktikast vaidlusaluses küsimuses[106].

Raportis jõuti järeldusele, et avaldamise seisuga ei reguleeri umbes poolte liikmesriikide siseriiklik õigus sideandmete sihistatud säilitamist, vaid kasutusel on üldiste ning vahet tegemata säilitamisi kehtestavad raamistikud. Küll aga on paljudes riikides käimas töö selleks, et arendada uus ning EL õigusega kooskõlas olev sideandmete regulatsioon. Samas on teine pool liikmesriikidest võtnud kasutusele erinevad meetmed sihistatud säilitamiseks[107]. Sellise otsuse aluseks on Euroopa Kohtu praktikaga väljakujunenud liiklus- ja asukohaandmete üldise ning vahet tegemata säilitamise keeld ning kohtuotsustes väljatoodud lubatavad (sihistatud) viisid sideandmete kogumiseks ja säilitamiseks.

Liikmesriigid lähenesid sideandmete säilitamise sihistatuks muutmisele erinevalt. Osa liikmesriike piirab oma sideandmete säilitamisi konkreetsete piirkondadega, kehtestades erinevad kriteeriumid allutatavate piirkondade määramiseks. Mõned riigid kehtestasid regulatsiooni, mis võimaldab rakendada sideandmete säilitamist sihistatult konkreetsete isikute suhtes. Lisaks on paljudes riikides ette nähtud võimalus käivitada üldine sideandmete säilitamine riiki tõsiselt ohustava ning päriselt olemasoleva ja ettenähtava julgeolekuohu korral.

[104] Eurojust, European Judicial Cybercrime Network (EJCN). The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU. Veebis: https://www.eurojust.europa.eu/publication/effect-court-justice-european-union-case-law-national-data-retention-regimes-judicial-cooperation (14.04.2025).
[105] *Ibid*, lk 3.
[106] *Ibid*, lk 4-6.
[107] *Ibid*, lk 8.

Seejuures ei ole osad sihistatud säilitamiskordi kehtestanud liikmesriigid tühistanud varasemalt kehtinud üldiseid säilitamiskohustusi. Samas võib Euroopa Kohtu ning siseriiklike kohtute otsuste mõjul olla veendunud, et sellisel alusel säilitatud liiklus- ja asukohaandmeid reaalselt kasutada ei saa.

### 2.2. Sideandmete asukohapõhine kogumine ja säilitamine Belgia Kuningriigis

Mitme liikmesriigi, näiteks Belgia Kuningriigi õiguskord lubab piiritleda sideandmete säilitamist konkreetsete asukohtadega[108]. Eurojusti ja EJCN analüüsis tuuakse välja 2022. aasta augustist kehtiv Belgia Kuningriigi elektroonilise side seaduse[109] (edaspidi ka: *Loi relative aux communications électroniques*) artikkel 126/3, mis lubab sideandmete säilitamist asukohapõhiselt võitluseks raske kuritegevusega või ohtudega riigi julgeolekule. Analüüsis leiti kokkuvõtvalt, et sideandmed võib säilitada asukohapõhiselt järgnevatel alustel:

1. Sideandmete säilitamine 6, 9 või 12 kuu jooksul piirkondades, kus raske kuritegevuse (ohu-)tase ületab mõõdikuga sätestatud piiri.
2. Sideandmete säilitamine 12 kuu jooksul piirkondades, kus esineb suur ohutase riigi julgeolekule (3 palli neljast vastavalt riiklikule ohuhinnangule).
3. Sideandmete säilitamine 12 kuu jooksul piirkondades, mis on eriti haavatavad raske kuritegevuse ja riigi julgeoleku kontekstis (näiteks lennujaamad, sadamad, riigiasutuste hooned jne)[110].

Esimese aluse valguses kehtestati 07.02.2025 ministri dekreet, mis kehtestas piirkonnad, kus sideettevõtjad on kohustatud säilitama elektroonilise side seansside käigus tekkivad sideandmed[111]. Nõnda kehtestasid Belgia Kuningriigi sise- ning justiitsminister määruse artikliga 1 kohustuse säilitada sideandmed ühe aasta jooksul Belgia 11 juriidilises ringkonnas ning artikliga 2 üheksa-kuulise säilitamiskohustuse Eupeni juriidilises ringkonnas.

Antud õiguslikku lahendusse võiks Euroopa Kohtu praktikat arvestades suhtuda kriitiliselt. Võttes arvesse, et kokku on Belgia Kuningriigis 12 juriidilist ringkonda, kehtestasid ministrid selle dekreediga üleriigilise kohustuse sideandmete säilitamiseks. Sisuliselt on taoline õigusakt

[108] Eurojust, EJCN, lk 8-9.
[109] *Loi relative aux communications électroniques – Moniteur belge, 20.06.2005. Numéro: 2005011238*.
[110] Eurojust, EJCN, lk 9.
[111] *Arrêté ministériel portant exécution de l'article 126/3, § 1, de la loi du 13 juin 2005 relative aux communications électroniques en vue de l'adoption de la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que la durée de conservation. Moniteur belge – 17.03.2025. Numéro: 2025001599.*

pealtnäha vastuolus Euroopa Kohtu seisukohaga *Tele2 Sverige et al* otsuses, mis keelas ära üldise ning vahet tegemata liiklus- ja asukohaandmete säilitamise.

Samas räägib sellise kriitika vastu riigi poolt kehtestatud range seadusandlus elektroonilise side andmete säilitamise kohta. Nimelt aitab ministrite niivõrd ranget dekreeti tõlgendada *Loi relative aux communications électroniques* artikkel 126/3, mis sätestab väga täpsed kriteeriumid, millal võib sideandmete säilitamine konkreetses piirkonnas muutuda lubatavaks. Kõnealuse artikli paragrahv 1 lubab säilitada sideandmed:

- juriidilistes ringkondades, kus säilitamise otsusele eelneva kolme aasta jooksul registreeriti aastas keskmiselt kolm või enam nn jälituse kataloogikuritegu 1000 elaniku kohta.
- ülejäänud (so esimesse loetellu mittekuuluva) juriidiliste ringkondade politseipiirkondades, kus säilitamise otsusele eelneva kolme aasta jooksul registreeriti aastas keskmiselt kolm või enam nn jälituse kataloogikuritegu 1000 elaniku kohta.

Käesolev artikkel ei jäta diskretsiooniõigust sideandmete säilitamise tähtaja kohta, vaid tähtajad on mõõdikupõhiselt paika pandud. Näiteks on juriidiliste ringkondade lõikes lubatud säilitada sideandmeid 6, 9 või 12 kuud vastavalt sellele, kas ringkonnas registreeriti säilitamise otsusele eelneva kolme aasta jooksul aastas keskmiselt 3-4, 5-6 või 7 ja enam nn jälituse kataloogikuritegu 1000 elaniku kohta. Sarnane süsteem kehtib ka politseipiirkondade kohta. Seaduse originaaltekst viitab kuritegude kataloogile, mis on loetletud Belgia Kuningriigi kriminaalprotsessi koodeksi (edaspidi ka: *Code d'instruction criminelle*) artikli $90^{1}$ paragrahvides 2-$4^{112}$. Need sätted on oma sõnastuse poolest võrreldavad KrMS § $126^{2}$ lõikes 2 oleva kuritegude loeteluga. Viimane kehtestab kuriteod, mille uurimisel on jälitustoimingute teostamine võimalik. Autor nimetab need lihtsustatult (jälituse) kataloogikuritegudeks.

Õigus kehtestada sideandmete kohustuslik säilitamine järgides eelkirjeldatud raamistikku on riigi sise- ning justiitsministritel ühiselt. Iga-aastaselt peavad ministrid määrama juriidilised ringkonnad ja politseipiirkonnad kus andmed säilitatakse ning kehtestama ka eeltoodu alusel 6-, 9- või 12-kuulise säilitamistähtaja. Kõrvutades *Loi relative aux communications électroniques* ning selle alusel kehtestatud ministrite dekreeti võib järeldada, et Belgia seadusandja ja täidesaatva võimu hinnangul on riigis niivõrd suur raske kuritegevuse tase et see õigustab sideandmete säilitamist kogu riigi territooriumil. Ministri dekreet rajaneb statistikal,

[112] *Code d'instruction criminelle. Livre Premier (Art. 8 à 136ter). Moniteur belge - 27 novembre 1808. Numéro: 1808111701*.

et 11 juriidilises ringkonnas 12-st pandi toime 7 või enam jälituse kataloogikuritegu 1000 elaniku kohta ning ühes ringkonnas 5-6 jälituse kataloogikuritegu 1000 elaniku kohta.

Teise *Loi relative aux communications électroniques* artiklist 126/3 tuleva alusena saab Belgia Kuningriigis säilitada sideandmeid riigi julgeoleku tagamiseks. Artikli 126/3 paragrahv 2 lubab säilitada sideandmed nendes geograafilistes piirkondades, kus Belgia Kuningriigi Ohuanalüüsi Koordineerimisüksuse (CUTA) ohuhinnangu alusel esineb suur ohutase riigi julgeolekule, täpsemalt vähemalt 3 palli 4 palli skaalal. Käesoleval juhul kehtestatakse elektroonilise side seaduse artikli 126/3 paragrahvi 2 alusel kuninglik dekreet mis loetleb, tuginedes CUTA ohuhinnangule, need suure ohutasemega piirkonnad.

CUTA on 2006. aastal asutatud Belgia Kuningriigi iseseisev riiklik analüüsiasutus, mis sünteesib koostööpartnerite kohustuslikus korras edastatavat (luure-)teavet. CUTA koostööpartnerite hulka kuulub suur hulk asutusi, teiste hulgas politsei, luureasutused, rahapesu andmebüroo ning teised õiguskaitseasutused[113]. Sellest tulenevalt võib väita, et CUTA valdusesse liigub kogu Belgia Kuningriigi poolt sünteesitav teave riiki ohustavate julgeolekuohtude kohta. Samuti on CUTA iseseisev asutus, mis omakorda suurendab asutuse ohuhinnangute neutraalsust, läbipaistvust ning usaldusväärsust[114].

CUTA toob välja, et taolised ohuhinnangud viiakse läbi konkreetse ürituse, riigi poolt kaitstava isiku, riiki ohustava isiku/grupeeringu suhtes või partnerasutuse taotlusel. Ohuhinnangud kehtestavad olukorrale ohutaseme skaalal 1-4 ning ohutaseme tuvastamine rajaneb rangelt kehtestatud metoodikal[115]. Vaatamata eeltoodud CUTA analüüside usaldusväärsust toetavatele argumentidele on CUTA avaldanud vaid ühe avaliku ohuhinnangu, seda 2023. aastal ning puutuvalt kogu Belgia Kuningriigi geograafilisse territooriumi. CUTA kehtestas 16.10.2023 ohuhinnanguga üleriigilise ohutaseme 3 – selline kõrge üleriigiline ohutase on põhjendatud CUTA ligi 40-leheküljelise raportiga[116].

Raportis selgitatakse, et ohutase tõsteti 2 pallilt 3 pallile seoses Brüsselis aset leidnud terrorirünnakuga Rootsi Kuningriigi jalgpallimeeskonna toetajatele. Kuigi CUTA kinnitab, et tegemist on isoleeritud intsidendiga, täheldab asutus järsku koostööpartnerite poolt edastatavate

[113] CUTA. Who we are. Veebis: https://cuta.belgium.be/who-we-are/ (14.04.2025).
[114] *Ibid*.
[115] CUTA. What do we do? Veebis: https://cuta.belgium.be/what-do-we-do/ (14.04.2025).
[116] CUTA. Annual report 2023. Veebis: https://cuta.belgium.be/wp-content/uploads/2024/09/Annual-report_2023.pdf (14.04.2025).

ohuolukorrateadete tõusu. 3-pallilist ohutaset põhjendab CUTA ka raske geopoliitilise kontekstiga, mida iseloomustab koraanide põletamine Rootsis, Iisraeli - Gaza konflikt ning üleüldine ekstremismi ja radikaliseerumise tõus. Selle hinnangu alusel ning tuginedes eelkirjeldatud õiguslikule alusele langetati 16.11.2023 kuninglik dekreet[117], mis kohustab säilitada kõik Belgia territooriumil tekkivad sideandmed 12 kuud selle hetkeni, kuni CUTA vähendab üleriiklikku ohutaset vähemalt 2 pallini.

Sarnaselt eelnevalt käsitletud kuritegude statistika alusel kehtestatud dekreediga on tegu järjekordse dekreediga, kus õiguslik raamistik võimaldab sideandmete üldist säilitamist kogu riigi territooriumil. Sellele vaatamata on CUTA ohuhinnangu ning selle alusel kehtestatud dekreedi näol tegemist pealtnäha põhjaliku kaalutlusotsusega. CUTA hinnangus esitatud seisukohti toetatakse üle terve Euroopa. Euroopa Liidu Õiguskaitsekoostöö Amet (Europol) avaldas 2024. aastal aruande terrorismi olukorra ja suundumuste kohta Euroopa Liidus (TE-SAT)[118]. Selles raportis esitas Europol liiduülese olukorraülevaate terrorismi arengute ning suundumuste kohta, kuid raport rajaneb liikmesriikide endi esitatud andmetel. Europoli hinnangul oli 2023. aastal terrorismioht üsna tõsine – aasta jooksul toimus seitsmes liikmesriigis 120 terrorirünnakut, millest 98 olid lõpule viidud[119]. Märkimisväärne on ka see, et TE-SAT täheldab sotsiaalmeedia ja otspunktkrüpteeritavate sõnumirakenduste väärkasutust terroristlike narratiivide levitamiseks ning rünnakute planeerimiseks[120].

*Loi relative aux communications électroniques* artikli 126/3 paragrahv 3 lubab säilitada sideandmed piirkondades, mis on eriti haavatavad julgeolekuohtudele ning rasketele kuritegudele. Nendeks piirkondadeks on paragrahvide 3-5 alusel:

- transpordisõlmed, täpsemalt sadamad, sadamaterminalid ning sadama turvatsoonid, suured rongijaamad (reguleeritud eraldi seadusega), metroojaamad, lennujaamad, tollilaod ja -terminalid;
- kriitilise taristu objektid, täpsemalt radiatsioonikaitsega tegelevad asutused, ohtlike ainetega seotud hädaolukordade lahendamise asutused, operatiivraadiosidet tagavad objektid, põhimaanteed, haiglad ja muud kriitilise taristu objektid, mida määratakse dekreediga;

[117] *Arrêté royal portant exécution de l'article 126/3, § 2, de la loi du 13 juin 2005 relative aux communications électroniques en vue de la confirmation du niveau de menace sur l'ensemble du territoire. Moniteur belge – 17.11.2023. Numéro: 2023047298*.
[118] Europol. European Union Terrorism Situation and Trend Report 2024. Veebis: https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf (14.04.2025).
[119] *Ibid*, lk 5.
[120] *Ibid*, lk 6.

- riigikaitse vaatest tähtsust omavad objektid, täpsemalt riigi- ning munitsipaalvalitsuse põhilised hooned (seaduses täpne loetelu), põhiseaduslikud institutsioonid, kaitse- või julgeolekuvaldkonna teadusasutused, politsei- ja julgeolekuasutuse objektid, sõjaväeobjektid, EL, NATO jm rahvusvaheliste organisatsioonide hooned, vanglad ja piirivööndi alad;
- relvakauplused või -töökojad ja lasketiirud;
- teised eriti haavatavad objektid, mida määratakse dekreediga.

Antud juhul kehtestab eelnimetatud asutuste ümber oleva sideandmete säilitamisala perimeetri Belgia Kuningriigi Kuningas. Asutuste täpne nimekiri on salajane ning asjaomastel isikutel on kohustus hoida seda nimekirja saladuses.

Eelkirjeldatud alustel peab sideettevõtja säilitama *Loi relative aux communications électroniques* artikli 126/2 paragrahvis 2 loetletud andmed. Nende andmete loetelu on sarnane Eesti ESS § $111^1$ lõigetes 1-3 loetletud andmetele. Juhul, kui seadusega pole teisiti ette nähtud, kehtestab *Loi relative aux communications électroniques* artikkel 126/1 andmete säilitamise üldiseks tähtajaks 12 kuud.

Kõigi kolme säilitamise õigusliku aluse puhul paistab silma, et sideandmete säilitamisele allutatud piirkonnad ja objektide ümbrused kehtestab Belgias täidesaatva võimu organ. Kontroll selle protseduuri üle on kehtestatud *Loi relative aux communications électroniques* artikli 126/1 paragrahviga 5. Selle kohaselt peab andmete säilitamise korraldust andev minister kuulama iga-aastaselt ära riikliku julgeoleku koordinatsioonikomiteedi ning andmekaitse eest vastutavate asutuste arvamuse. Seejärel peab täidesaatva võimu organ koostama olemasolevate andmete ning arvamuste alusel rapordi Belgia parlamendile. Rapordi ning parlamendile ülevaate andmise eesmärk on tuvastada, kas säilitamise alla kuuluvad piirkonnad vastavad *Loi relative aux communications électroniques* artikli 126/3 kriteeriumitele.

### 2.3. Sideandmete isiku- ja asukohapõhine kogumine ja säilitamine Taani Kuningriigis

Sarnaselt Belgia Kuningriigile on sideandmete asukohapõhine kogumine võimalik ka Taani Kuningriigis. Lisaks asukohapõhisele kogumisele on Taanis kehtestatud õigusnormid, mis võimaldavad koguda sihistatult ka konkreetsete üksikisikute sideandmeid. Uus sideandmete säilitamise regulatsioon tekkis pärast aastal 2022 läbi viidud reformi[121].

[121] Eurojust, EJCN, lk 9.

Sideandmete säilitamist reguleerib Taani Kuningriigi õigusemõistmise seadus[122] (edaspidi ka: *Retsplejeloven*), mis peab raskete kuritegudena (alloleva regulatsiooni valguses) eeskätt kõiki vähemalt 3-aastast vangistust ette nägevaid kuritegusid. Samuti peetakse rasketeks kuritegudeks Taani kriminaalkoodeksis[123] (edaspidi ka: *Straffeloven*) loetletud tahtlikult toime pandud riigivastaseid kuritegusid, rööve, ähvardamisi, samuti põgenemiste, kohustuste vältimistega või lapspornograafiaga seotud kuritegusid. Lisaks eeltoodule on rasketeks kuritegudeks ka *Straffeloven* paragrahvis 81 a loetletud kuriteod (isikuvastased kuriteod, avaliku korra vastased kuriteod, rasked varavastased kuriteod).

*Retsplejeloven* paragrahvi 786 b lõike 1 alusel võib politsei anda sideettevõtjale korralduse koguda ja säilitada sideandmeid sihistatult isiku suhtes:

1. 3 aasta kestel, kui isik on süüdi mõistetud raske kuriteo toimepanemises;
2. 5 aasta kestel, kui isik on süüdi mõistetud kuriteos mis näeb karistusena ette vähemalt 6-aastase vangistuse;
3. 10 aasta kestel, kui isik on süüdi mõistetud kuriteos mis näeb karistusena ette vähemalt 8-aastase vangistuse.

Antud säilitamise tähtaeg hakkab sama paragrahvi lõike 2 alusel kulgema sellest hetkest, kui isik kannab ära vangistuse või isik vabastatakse tingimisi ning allutatakse käitumiskontrollile. Tõlgendades eelkirjeldatud sätte sisu võib eeldada, et sellise sihistatud sideandmete säilitamise eesmärk on hoida ära retsidiivsust või vähemalt tagada korduvkurjategija suhtes läbiviidava uurimise parem tõhusus. Kuigi antud meede võib olla efektiivne, kahtleb autor kas taoline lahendus sobiks Eesti ühiskonda, arvestades kriminaal- ning korrektsioonipoliitilisi hoiakuid.

*Retsplejeloven* paragrahvi 786 b lõike 3 alusel võib politsei anda sideettevõtjale korralduse sideandmete kogumiseks 1 aasta jooksul ning nende edaspidiseks säilitamiseks 1 aasta jooksul:

1. seadme suhtes, mille suhtes rakendatakse seadmepõhiselt kohtu loal pealtkuulamist või kõnelogide salvestamist;
2. isikute suhtes, kes omavad või on omanud eelnevas punktis kirjeldatud seadet või kelle suhtes rakendatakse isikupõhiselt kohtu loal pealtkuulamist või kõnelogide salvestamist;
3. seadme suhtes, mille omanik on andnud loa sideandmete kogumiseks ja säilitamiseks.

[122] *Retsplejeloven - Lovtidende A, LBK nr 1160 af 05/11/2024*.
[123] *Straffeloven – Lovtidende A, LBK no. 1145 af 05/11/2024*.

Sellise sihistatud säilitamise eesmärk on tagada kohtu loal toimuva jälitustoimingu (pealtkuulamine või kõnelogide salvestamine *Retsplejeloven* paragrahvi 780 lõike 1 punkti 1 või 3 alusel) tarbeks vajalike andmete kättesaadavus. Punkti 3 alusel teostatavat säilitamist võib tõhusalt kasutada protseduurides, kus on vajalik uurida isiku tausta (nt julgeolekukontroll)

Taanis on reguleeritud ka sideandmete asukohapõhine sihistatud säilitamine. Olgu mainitud, et allolevad regulatsioonid ei kohaldu lauatelefonidele ning interneti-telefoni teenustele.
*Retsplejeloven* paragrahvi 786 c lõike 1 alusel võib politsei anda sideettevõtjale korralduse sideandmete kogumiseks ning säilitamiseks 1 aasta jooksul sellistes piirkondades suurusega kuni 3km$^2$, kus:

1. registreeritud raskete kuritegude arv on 1.5 korda suurem kui riigis keskmiselt;
2. elanikena on registreeritud 1.5 korda rohkem raskete kuritegude toimepanemise eest süüdimõistetuid kui riigis keskmiselt.[124]

*Retsplejeloven* paragrahvi 786 c lõike 2 alusel lubatakse sideandmete säilitamine 1 aasta jooksul geograafilistes piirkondades, kus asuvad riigi julgeoleku vaatest suure tähtsusega hooned, täpsemalt kuninglikud hooned, peaministri residents, saatkonnad, militaarobjektid, politseiasutuste hooned, piiripunktid, vanglad, infrastruktuuriobjektid (sillad, tunnelid ja praamisadamad, põhimaanteed) ja transpordisõlmed (lennujaamad, praamisadamad, bussiterminalid, rongiterminalid).

Need asukohapõhised kogumisviisid on sarnased Belgia regulatsioonidele, kuid erisusena paistab silma see, et Taanis määratakse kogumisele allutatavad piirkonnad palju väiksema pindala täpsusega ning ühe piirkonna valiku kriteeriumiga tuuakse välja piirkonnas elavaid süüdimõistetuid. Isikupõhise kogumise kriteeriumina peab Taani seadusandja põhjendatuks koguda sideandmeid isikute kohta, kes on enda toimepandud tegude eest juba vanglakaristuse ära kandnud. Sarnaselt Belgia õiguskorrale näeb ka *Retsplejeloven* ette sideandmete ajutist säilitamist. Seejuures kehtib riigis ka üldine ja vahet pidamata interneti-teenusega seotud omistatud identiteediandmete säilitamise kord, mis on reguleeritud *Retsplejeloven* paragrahviga 786 f - Euroopa Kohus lubas taoliste andmete säilitamist *La Quadrature du Net et al* otsusega**.**

[124] Üleriigilise keskmise kuritegude või süüdimõistetute arvu all peetakse aastast keskmist arvu viimase kolme aasta lõikes.

Sideandmete kasutamine kriminaalmenetluses on reguleeritud *Retsplejeloven* paragrahvidega 804 a, 805 ning 806. Nende kohaselt toimub sideandmete väljastamine politsei taotlusel ning kohtu loal, kui sideandmete väljastamisega kaasnev riive on proportsionaalne sideandmete kasutamise vajadusele kriminaalasjas. Kohtumäärus peab sisaldama kohtu põhistusi toimingu proportsionaalsuse osas. Edasilükkamatul juhul on võimalik nõuda välja sideandmed politsei enda korraldusel, kuid sellisel juhul peab kohus otsustama korraldusele järgneva 24 tunni jooksul selle toimingu lubatavuse.

### 2.4. Sideandmete ajutine kiirsäilitamine võitluseks kuritegevusega ja julgeolekuohtudega

Eurojusti ja EJCN raportis leiti, et paljude liikmesriikide õigus võimaldab käivitada ajutine sideandmete kiirsäilitamine konkreetse menetluse raames. Raportis on välja toodud 13 riiki, millest kõige enim paistavad silma varasemalt käsitletud Belgia ning Taani. Samuti näeb mitme liikmesriigi õigus võimaluse käivitada üleriigiline sideandmete säilitamine riiki ohustava tõsise julgeolekuohu korral. Täpsemalt tuuakse raportis välja Prantsusmaa, Iirimaa, Portugali ning juba varasemalt käsitletud Belgia ja Taani õiguskorrad[125].

Esiteks paistab nende riikide puhul silma andmete erakorralise säilitamise regulatsioon, mis on ette nähtud Belgia Kuningriigis. Antud protseduur on õiguslikult lahus eespool analüüsitud Belgias kehtivast sihistatud säilitamise regulatsioonist. *Code d'instruction criminelle* artikli $39^5$ kohaselt võib prokuratuur anda korralduse sideettevõtjale sideandmete säilitamiseks. Korralduse võib anda üksnes juhul, kui kriminaalasjas ilmneb põhjendatud kuriteokahtlus sellise kuriteo toimepanemises, mille eest on karistusena ette nähtud vähemalt üheaastane vangistus. Korraldus peab olema antud kirjaliku põhistatud määrusena, kuid edasilükkamatul juhul võib esialgse korralduse anda suuliselt ning seejärel põhistada seda määrusega. Korralduse kehtivus on kuni kaks kuud ning selle aja jooksul kogutud andmeid peab sideettevõtja säilitama kuni 6 kuud.

Ajutise säilitamise regulatsioon kuritegude tõkestamiseks on ette nähtud ka Taani Kuningriigis. *Retsplejeloven* paragrahv 786 d lõige 1 näeb ette võimaluse kohustada sideettevõtteid säilitama sideandmeid isikute, seadmete või konkreetsete piirkondade kohta juhul, kui esineb põhjendatud alus arvata, et see on seotud raskete kuritegude toimepanemisega. Asukohapõhine ajutine säilitamine ei ole lubatud lauatelefonide ning interneti-telefoni teenuse suhtes. Ajutine kogumise käivitamine on sama paragrahvi lõike 2 alusel lubatud üksnes kohtumäärusega.

[125] Eurojust, EJCN, lk 8-11.

Andmete kogumise kestus peab olema võimalikult väike ning ei saa olla pikem kui 6 kuud, mida omakorda saab pikendada 6 kuu kaupa. Sätte sõnastusest ei selgu kes on käesoleval juhul taotluse esitajaks, kuid koosmõjus teiste säilitamist puudutavate sätetega võib asuda seisukohale, et ka sel juhul on protsessi algatajaks politsei.

Belgia, Taani ja ka teiste eespool nimetatud riikide sideandmete ajutise säilitamise (*quick-freeze*) regulatsioon võimaldab uurimisasutusel ja prokuratuuril tagada konkreetses kriminaalasjas raskete kuritegude tõendamiseks vajaminevate sideandmete säilimine nende edaspidiseks kasutamiseks tõendina. Oma olemuselt on tegu äärmiselt sihistatud säilitamismeetmega, mille aktiveerimine on usaldatud kohtulikult kontrollitavatele asutustele ehk prokuratuurile ja politseile. Autor eeldab, et antud protseduuri õiguspärasust hinnatakse hiljem ka kohtumenetluses. Selliselt säilitatud andmeid saab tõhusalt kasutada raske kuritegevuse vastu, tõendamaks laia ampluaad tõendamisväärtusega asjaolusid.

Lisaks eelnimetatule näevad liikmesriigid ette ka ajutise säilitamise käivitamise üleriigiliselt või konkreetses piirkonnas riiki ohustava tõsise ning objektiivselt hinnatava julgeolekuohu korral. Belgias reguleerib antud protseduuri varasemalt käsitletud *Loi relative aux communications électroniques* artikli 126/3 teine alus, mis lubab sideandmete üldist säilitamist CUTA ohuhinnangu alusel. Taanis on see protseduur reguleeritud *Retsplejeloven* paragrahviga 786 e. Selle kohaselt võib justiitsminister, kuulates ära äri- ning tööstusministri ettepaneku, seada kuni 1-aastase kohustuse üldiseks ning vahet tegemata sideandmete säilitamiseks juhul, kui esinevad piisavalt kaalukad asjaolud mis viitavad sellele, et Taani Kuningriiki ohustab reaalne hetkel või tulevikus aset leidev julgeolekuoht.

Nagu eespool kirjeldatud, langetab Taanis ja Belgias julgeolekualase säilitamise otsuse minister ehk täidesaatva võimu esindaja. Iiri Vabariigis langetab aga selle otsuse kohus. Iirimaa sideandmete säilitamise seaduse *Communications (Retention of Data) Act 2011*[126] paragrahv 3A lõike 1 kohaselt esitab valdkonna eest vastutav minister riigi kõrgeima kohtu esimehe määratud kohtunikule või kohtunikele taotluse sideandmete üleriigiliseks säilitamiseks 12 kuu jooksul juhul, kui ministri hinnangul esineb tõsine ning reaalne olemasolev või tulevikus aset leidev oht riigi julgeolekule. Taotluse esitamise eel peab minister hindama julgeolekuohtu, arvestades sideandmete säilitamise reaalset vajalikkust ning proportsionaalsust. Taotlus peab olema esitatud personaalselt ministri poolt, rajanema kohtus vande all üleantaval teabel ning

[126] *Communications (Retention of Data) Act 2011 – Number 3 of 2011. Revised Act, Updated to 1 August 2023.*

sisaldama ka aega, mille kestel kehtib sideettevõtjatele kohustus koguda sideandmeid (ning säilitada nad edaspidi 12 kuu jooksul).

Sideandmete säilitamine julgeolekuohu korral on pigem äärmuslik meede, mille õigustamine eeldab reaalselt hinnatavat ja tajutavat, mitte hüpoteetilist julgeolekuohtu. Ülal käsitletud liikmesriikides on ette nähtud põhjalikud mehhanismid ja mõõdikud selliste ohtude hindamiseks. Autori hinnangul on need igati põhjendatud meetmed, mis on aga relevantsemad julgeolekuasutuste töös, mitte kriminaalmenetlustes. Kuivõrd need meetmed jäävad väljaspoole käesoleva töö temaatikat, jätab autor esitamata regulatiivsed ettepanekud, mis rajanevad eelkirjeldatud julgeolekualase säilitamisraamistikul. Samas möönab autor nende võimalikku kasu julgeolekuasutustele pandud ülesannete täitmisel.

### 2.5. Sideandmete säilitamise piiramine andmeliikide kaupa

Üheks viisiks tagada sideandmete õiguspärane säilitamine on säilitatavate andmete piiramine üksnes nende liikidega, mille puhul on Euroopa Kohus pidanud lubatavaks üldist ning vahet tegemata säilitamist. Tulenevalt Euroopa Kohtu otsusest *La Quadrature du Net et al* kaasuses on nendeks andmeteks sideühenduse lähteabonendile omistatud IP-aadressid ning sidevahendite kasutajate identiteediandmed[127].
Seda teed on EJCN ning Eurojusti rapordi andmetel astunud Portugali Vabariik[128]. Sideandmete kasutamist kriminaalmenetluses reguleerib Portugalis direktiivi 2006/24/EÜ ülevõtmisega kehtestatud seadus 32/2008[129]. Euroopa Kohtu praktika mõjul on seda seadust märkimisväärselt muudetud 02.05.2024 jõustunud seadusega 28/2024,[130] mis reformis oluliselt riigis kehtivaid sideandmetega seotud seadusi. Seaduse 32/2008 artiklit 6 muudeti selliselt, et sideettevõtja on kohustatud säilitama sideseansiga seotud baasandmeid, andmeid sideteenuse kasutaja identiteedi kohta ning side lähtepunktile omistatud IP-aadresside kohta. Muude andmete säilitamine on sama artikli alusel lubatud üksnes ajutise kiirsäilitamise korra järgi võitluseks raske kuritegevusega. Ajutise säilitamise kord sarnaneb eelnevalt kirjeldatud teiste liikmesriikide kordadele ning Portugalis eeldab ajutine kiirsäilitamine kohtu luba.

Seaduse 32/2008 artikli 9 lg 1 kohaselt võib eelnimetatud sideandmeid väljastada kasutamiseks kriminaalmenetluses üksnes prokuratuuri taotlusel ning eeluurimismagistraadi ehk kohtuniku

[127] EKo C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net et al*, p 168.
[128] Eurojust, EJCN, lk 10.
[129] *Lei n.º 32/2008, de 17 de julho, Diário da República n.º 137/2008, Série I de 2008-07-17, páginas 4454 – 4458*.
[130] *Lei n.º 18/2024, de 5 de fevereiro. Diário da República n.º 25/2024, Série I de 2024-02-05, páginas 9 – 22*.

loal juhul, kui need andmed on olulise tähtsusega tõe väljaselgitamiseks või kui tõendite kogumine muul viisil takistaks oluliselt raskete kuritegude uurimist, tuvastamist ja menetlemist. Järelikult on Portugali Vabariigis kohaldatud kohtulikku kontrolli sideandmete väljastamisel, samuti on sõnastuses viiteid ka *ultima ratio* või selletaolise põhimõtte järgimisele.

Säilitatavate andmete liikide piiramise teed on läinud ka Rootsi Kuningriik[131]. Rootsi elektroonilise side seadus 2022:482[132] 9. peatüki paragrahv 19 kohustab sideettevõtjaid säilitama üldiselt ning vahet tegemata andmeid, mis on vajalikud sideseansi lähte- ja lõppabonendi, samuti seansi aja, kestuse ja liigi, kasutatud seadmete ning nende asukoha tuvastamiseks.

Kõigi eelkäsitletud liikmesriikide sideandmeid puudutav regulatsioon annab hea ülevaate sellest, kuidas rakendada praktikas Euroopa Kohtu poolt kehtestatud kriteeriume. Tuginedes Euroopa Kohtu kriteeriumitele ning liikmesriikide regulatsioonile on võimalik asuda kehtestama regulatiivsed ettepanekud Eesti sideandmete regulatsioonile, et tagada selle edaspidine kooskõla EL õigusega.

[131] Eurojust, EJCN, lk 10-11
[132] *Lag (2022:482) om elektronisk kommunikation - 2022-05-19, t.o.m. SFS 2024:895*.

# 3. REGULATIIVSED LAHENDUSED SIDEANDMETE KASUTAMISEKS LUBATAVA TÕENDINA EESTI SÜÜTEOMENETLUSTES

## 3.1. Sideandmete väljanõudmise regulatsioon kriminaal- ning väärteomenetlustes

Regulatiivsete lahenduste väljatoomist on edaspidist analüüsi arvestades mõistlik alustada sideandmete väljanõudmise regulatsioonist. Selleks tuleb hinnata viimati reformitud KrMS § $90^1$ vastavust EL õigusele. Väärteomenetluste puhul on reguleerivaks sätteks VTMS § $31^2$.

Analüüsides kehtivat KrMS § $90^1$ redaktsiooni tuleb tõdeda, et käesolev säte on viimase muudatusega viidud kooskõlla autori poolt varasemalt väljatoodud regulatiivsete kriteeriumitega. Esiteks on ligipääs liiklus- ja asukohaandmetele piiratud käesoleva paragrahvi lõikega 2 sellisel moel, et andmete väljanõudmine toimub pärast kohtulikku kontrolli ehk eeluurimiskohtuniku loal kohtueelses menetluses ja kohtu loal kohtumenetluses. Kohtulik kontroll on rakendatud ka edasilükkamatu ligipääsu puhul – prokuratuuri edasilükkamatu loa korral peab toimingut sama paragrahvi lõike 6 alusel kontrollima kohtus, esitades järgneva esimese tööpäeva jooksul kohtule põhjendatud taotluse päringu lubatavaks tunnistamiseks.

Kooskõla EL õigusega väljendub ka selles, et uues redaktsioonis on piiritletud need kuriteod, mille puhul on sideandmete väljanõudmine üldse mõeldav. Esiteks piiratakse kuritegude liike paragrahvi lõike 3 alusel varasemast õiguspraktikast tuttava KrMS § $126^2$ lg 2 loeteluga kuritegudest, mille puhul on lubatud jälitustoimingute tegemine. Tegemist on regulatiivse lahendusega, mille abil defineeritakse rasked kuriteod Euroopa Kohtu praktika mõistes. Samas on käesolevas sättes ette nähtud mõnevõrra laiem tõlgendus rasketest kuritegudest. Nimelt võimaldab paragrahvi lõige 3 esitada päring ka siis, kui kuritegu ei ole loetelus, kuid ligipääsu õigustab kuriteo raskus ja laad ning kui päringuga ei riivata põhjendamatult isikuõigusi. Selline tõlgendus võimaldab kohtul hinnata loeteluväliste kuritegude puhul kuriteo kuulumist raskete kuritegude (Euroopa Kohtu praktikaga) avatud loetellu juhtumipõhiselt. Sellega võidakse välistada olukordi, kus mõistetavalt raske kuriteo puhul on võimatu teha sideandmete päring seetõttu, et kuritegu pole jälituskataloogi loetelus.

Ligipääs sideandmetele väljaspool eelnimetatud tingimusi ning kohtulikku kontrolli on võimalik vaid KrMS § $90^1$ lg 1 alusel, kuid ka selline ligipääs on varasemalt väljatoodud kriteeriumite kontekstis aktsepteeritav. Nimelt on Euroopa Kohus selgitanud *Tele2 Sverige et*

*al* otsuses, et kohtulikku kontrolli nõuab ligipääs liiklus- ja asukohaandmetele ning selline ligipääs on lubatav ainult võitluseks raske kuritegevusega[133]. Samas pääseb menetleja omapoolse päringuga vaid side identifitseerimistunnustega seotud andmetele, mida on Euroopa Kohus lubanud säilitada lausa üldiselt ning vahet tegemata, piirdudes tingimata vajalikuga. Lisaks pääsetakse paragrahvi lõike 3 alusel üksnes nendele andmetele, mille väljanõudmine on vältimatult vajalik.

KrMS § 90[1] kui sideandmete väljanõudmise (kasutamise) ainus kitsaskoht peitub paragrahvi lõike 2 sõnastuses, täpsemalt selles kuidas säte defineerib mitteidentifitseerivaid andmeid. Selle normi kohaselt on kohtuliku kontrolliga lubatud väljanõudmise päring „*elektroonilise side seaduse § 111[1] lõigetes 2 ja 3 loetletud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi lõikes 1*." Sisuliselt tekitab sideandmete valimi piiramine ESS § 111[1] lg-te 2 ja 3 loeteluga olukorra, kus kaudselt tekitatakse ka viide säilitamise alusele – sellisel juhul lubab KrMS § 90[1] justkui kasutada üksnes laussäilitamise sätte alusel säilitatud sideandmeid, mis on aga EL õigusega vastuolus. Autor tutvus nii vana[134] kui ka uue[135] redaktsiooni sätete seletuskirjadega, kuid ei leidnud sealt teavet selle kohta, miks sooviti õigusloome protsessis siduda väljanõutavate sideandmete valim ESS § 111[1] lõigetega 2 ja 3.

Kuna alljärgnevalt teeb autor mitmed regulatiivsed ettepanekud sideandmete säilitamise normistikule, mida on õigusloome vaatest ilmselt mõistlik rakendada mitme eraldiseisva sättena, on autori hinnangul põhjendatud sõnastada KrMS § 90[1] lg 2 ümber selliselt, et alles jääb vaid viide elektroonilise side seadusele, täpsemalt selle alusel säilitatud andmetele, piiramata seejuures päritavate andmete loetelu konkreetse ESS sättega. Nõnda tuleb KrMS § 90[1] lg 3 sõnastada ümber selliselt, et uurimisasutus võib teha prokuratuuri taotlusel ja eeluurimiskohtuniku loal kohtueelses menetluses või kohtu loal kohtumenetluses päringu elektroonilise side ettevõtjale elektroonilise side seaduse alusel säilitatud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi lõikes 1. Sellise sõnastuse kasuks räägib ka asjaolu, et sideteenuste tehnoloogilise arengu korral ei teki ESS ajakohastamisel olukorda, kus mõni uus sideandmete liik jääb liiga konkreetse viite tõttu KrMS § 90[1] lg 2 loetelust välja. Samuti ei tekita autori pakutud üldisem sõnastus uurimisasutustele ja prokuratuurile võimalust riivata põhjendamatult eraelu puutumatust, kuna selline sõnastus eeldab jätkuvalt ESS-is sisalduvate

[133] EKo C-203/15 ja C-698/15, *Tele2 Sverige*, resolutsiooni p-d 1 ja 2.
[134] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 175 SE. Seletuskiri. Veebis: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0/ (14.04.2025).
[135] Kriminaalmenetluse seadustiku muutmise seadus 392 SE. Seletuskiri. Veebis: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/69f4f636-076c-487f-93c2-3827044cfb50/ (14.04.2025).

säilitamisnormide vastavust EL õigusele ning kohtulikku kontrolli iga väljanõudmise päringu korral.

Tulenevalt eeltoodust on autori esimeseks regulatiivseks ettepanekuks sõnastada KrMS § $90^1$ lg 3 ümber selliselt, et uurimisasutus võib teha prokuratuuri taotlusel ja eeluurimiskohtuniku loal kohtueelses menetluses või kohtu loal kohtumenetluses päringu elektroonilise side ettevõtjale elektroonilise side seaduse alusel säilitatud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi lõikes 1.

Järgmisena on otstarbekas analüüsida sätet, mis reguleerib sama toimingut väärteomenetlustes. Sätte struktuur on võrreldav kriminaalmenetluse seadustikus oleva normiga. Esimese lõikega on ette nähtud identifitseerimisandmete pärimine kohtuvälise menetleja päringuga, seejuures on välja toodud ka pädevate menetlejate loetelu. Antud andmetele ei kohaldu kohtuliku kontrolli kohustus ning tingimuslik ligipääs üksnes võitluseks raske kuritegevusega ja tõsiste julgeolekuohtudega. Neid andmeid lubas Euroopa Kohus otsusega *La Quadrature du Net et al* asjas säilitada üldiselt ja vahet tegemata ka avaliku korra (Euroopa Kohtu praktikas käsitletav mõistena „avalik julgeolek“) tagamiseks. Seetõttu on põhjendatud anda nii kriminaal- kui ka väärteomenetluses menetlejatele õigus pääseda ligi identifitseerimisandmetele oma päringuga.

Samas pole autori hinnangul vastavuses EL õigusega VTMS § $31^2$ lõige 2 ning seda mitmel põhjusel. Esiteks esineb selle sätte puhul sama probleem mis kriminaalmenetluse seadustikus oleva normi puhul. Kuigi säte lubab ainult üksikpäringut konkreetse sideseansi kohta ning sisaldab endas Euroopa Kohtu poolt väljatoodud kohtuliku kontrolli nõuet on sideandmete valim (ja kaudselt ka allikas) seotud ESS §-ga $111^1$ ehk EL õigusega vastuolus oleva laussäilitamise sättega. Ka antud sätte puhul teeb autor ettepaneku üldistada viide sideandmetele sarnaselt KrMS § $90^1$ lg 3 ettepanekuga, asendades konkreetne viide fraasiga „elektroonilises side seaduse alusel säilitatud andmete saamiseks“ ning seda samadel põhjustel mis said varasemalt välja toodud kriminaalmenetluse seadustiku sätte analüüsil.

Teise probleemina näeb autor seda, millistele andmetele sellise üksikpäringuga väärteomenetluses ligi saadakse. Nimelt on Euroopa Kohus piiranud ligipääsu paljudele kriitilistele andmetele (eeskätt liiklus- ja asukohaandmetele) üksnes võitluseks raske kuritegevusega või riigi julgeolekut ähvardava ohu tõrjumiseks. Autori hinnangul pole vaidlust selles, et Eesti õiguskorras olevad väärteod ei ole käsitletavad raskete kuritegudena ning samuti ei ole nendes sätestatud teod käsitletavad tõsise ohuna riigi julgeolekule. Seetõttu ei ole autori

hinnangul põhjendatud ligipääs liiklus- ja asukohaandmetele väärteomenetluses. Antud probleemi lahendaks see, kui kasutusele võetaks eelmises lõigus väljatoodud üldine viide elektroonilise side seadusele. See sõnastus oleks autori hinnangul efektiivne probleemi lahendamiseks, kuna sideandmete üksikpäring läbib kohtuliku kontrolli ning üksikpäring on sama paragrahvi lg 3 alusel lubatud üksnes siis, kui see on vältimatult vajalik väärteomenetluse eesmärgi saavutamiseks. See omakorda annab kohtule ülesande kõrvutada kohtuvälise menetleja esitatud taotluses päritavate sideandmete loetelu reaalse riivega, mida taoline päring teeb. Teiseks saab kohus hinnata seda, kas päritavate sideandmete säilitamise aluseks olev norm on kohalduv väärtegude kui kergema raskusastmega süütegude kontekstis. Kolmandaks saab kohus tuvastada ka päringu vältimatu vajalikkuse olemasolu.

Tuleb möönda, et taoliste regulatiivsete ettepanekutega süütemenetlusi reguleerivates seadustikes jaatatakse võimalus ärilistel eesmärkidel säilitatavate andmete kasutamiseks. Autori hinnangul on aga see aktsepteeritav lahendus. Nimelt ei ole äriliste andmete säilitamine vastuolus EL õigusega. Juhul, kui väljanõudmisega kriminaalmenetluses või üksikpäringuga väärteomenetluses järgitakse vältimatu vajaduse tingimust, ei ole selline päring õigusvastane. Võttes arvesse, et äriliste andmete säilitamine on õiguspärane, pääsetakse päringuga ligi õiguspäraselt säilitatud andmetele. Kuna sellisel juhul on nii säilitamise regulatsioon kui ka (ettepanekutega muudetud) päringute regulatsioon õiguspärane, ei esine autori hinnangul põhjust tunnistada ligipääs sellistele andmetele lubamatuks. Samas rõhutab autor, et juhul kui sideettevõtja säilitas ärilisel eesmärgil ka liiklus- ja asukohaandmeid, tohib sellistele andmetele pääseda ligi üksnes kohtu loal ning seda ainult rasket kuritegu uurivas kriminaalmenetluses. Ligipääs liiklus- ja asukohaandmetele väärteomenetluses pole võimalik ning ligipääsu sellistele andmetele saab tõkestada üksikpäringu taotlust läbivaatav kohus.

Tulenevalt eeltoodust annab autor sideandmete väljanõudmise (kasutamise) regulatsiooni kontekstis kaks ettepanekut. Esiteks teeb autor ettepaneku sõnastada KrMS § $90^1$ lg 3 ümber selliselt, et uurimisasutus võib teha prokuratuuri taotlusel ja eeluurimiskohtuniku loal kohtueelses menetluses või kohtu loal kohtumenetluses päringu elektroonilise side ettevõtjale elektroonilise side seaduse alusel säilitatud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi lõikes 1. Teiseks teeb autor ettepaneku sõnastada VTMS § $32^2$ lg 2 ls 1 ümber selliselt, et käesoleva paragrahvi lõikes 1 nimetatud asutus võib kohtu loal teha üksikpäringu elektroonilise side seaduse alusel säilitatud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi esimeses lõikes.

### 3.2. Sideandmete asukohapõhine säilitamine võitluseks raske kuritegevusega ja identifitseerimisandmete üldine ning vahet tegemata säilitamine

Kuna sideandmete kui tõendi lubatavus eeldab lisaks õiguspärasele kasutamise regulatsioonile ka säilitamise regulatsiooni, toob autor järgnevalt välja ettepanekud kehtestada erinevad viisid sideandmete säilitamiseks selliselt, et need ei oleks vastuolus EL õigusega. ESS § $111^1$ on võtmetähtsusega sideandmete defineerimisel ja säilitamise korra määramisel, aga selles sätestatud üldise ja sihistamata liiklus-ja asukohaandmete säilitamise kriteerium tuleks jätta sättest välja seoses vastuoluga EL õiguse suhtes.

Selleks teeb autor ettepaneku muuta ESS § $111^1$ lõiget 1, 2, 3 ja 4 selliselt, et teenuseosutaja on kohustatud säilitama andmeid üksnes käesolevas seaduses säilitatud juhtudel või kriminaalmenetluse seadustikus sätestatud tingimustel ajutise kiirsäilitamise korral (autor teeb allpool ettepaneku sellekohase paragrahvi lisamiseks kriminaalmenetluse seadustikku). Seeläbi ei nõua need normid enam üldist ning vahet tegemata liiklus- ja asukohaandmete säilitamist, vaid täidavad üksnes defineerivat, sõnastades konkreetsed andmeliigid mida tuleb säilitada seaduses sätestatud juhtudel ehk autori edaspidi antud ettepanekute alusel loodud uute normide alusel.

Samas tuleb tõdeda, et Euroopa Kohus lubas oma seisukohaga *La Quadrature du Net et al* asjas säilitada identifitseerimisandmeid üldiselt ja vahet tegemata. Sellest tulenevalt teeb autor ettepaneku täiendada elektroonilise side seadust õigusnormiga, mis kohustab sideettevõtjat säilitama identifitseerimistunnustega seotud andmeid lõppkasutaja tuvastamiseks ning lähteabonendile määratud IP-aadresside kohta. Võttes arvesse arvutitega seotud pettuste suurt kasvu on autori hinnangul põhjendatud säilitada kõiki lähteabonendile määratud IP-aadressite andmed. Jättes identifitseerimisandmete regulatsioon paindlikumaks, jääb reaalse vajaduse hindamine süüteomenetlustes kohtu hinnata. Nimelt on kehtiva õigusega lubatavad üksnes sideandmete päringud, mis on vältimatult vajalikud kriminaalmenetluse eesmärgi saavutamiseks. Kui kohtu hinnangul on päritavate sideandmete hulk ja liik liialt ebaproportsionaalsed saavutatava eesmärgi suhtes, saab kohus jätta sideandmete päringu taotluse rahuldamata.

Järgnevalt teeb autor ettepaneku kehtestada Eestis sihistatud sideandmete säilitamise normid. Kõrvutades Euroopa Kohtu praktikaga kehtestatud kriteeriume ning liikmesriikide juba kehtivaid lahendusi sihistatud säilitamiseks on põhjendatud võtta Eesti õiguskorras kasutusele normid, mis sihistavad sideandmete säilitamist asukohapõhiselt, vajadusel ka isikupõhiselt.

Varasemalt tuvastas autor, et Taani ning Belgia kuningriikide õigus lubab sideandmete sihistatud säilitamist geograafilistes piirkondades, milles on suur registreeritud raskete kuritegude arv. Sellise regulatiivse ettepaneku analüüsimiseks tuleb tuvastada optimaalne geograafilise piirkonna suurus ning mõõdik, mille alusel võib järeldada, et selles piirkonnas on suur registreeritud raskete kuritegude arv.

Esiteks tuleb panna paika geograafilise piirkonna suurus ning eraldusviis. Belgia Kuningriik, kasutab selleks juriidilisi ringkondi (riigis kokku 12) ning nendes olevaid politseipiirkondi. Töö kirjutamise seisuga on 12 ringkonnas 12-st selline registreeritud raskete kuritegude arv, et Belgia õiguse alusel on õigustatud sideandmete säilitamine kõigis neis ringkondades. 01.01.2024 seisuga on Belgias 11,76 miljonit elanikku[136] ning kõigi nendega seotud sideandmed kuuluvad töö kirjutamise seisuga säilitamisele geograafilise sihistuse alusel. See tähendab, et igas juriidilises ringkonnas elab aritmeetiliselt keskmiselt umbes 8,33% elanikkonnast ehk 1 miljon elanikku (jagades elanike arv kogu riigis ringkondade arvuga). Võttes arvesse Eesti elanike arvu, on üks juriidiline ringkond pealtnäha võrreldav terve Eesti territooriumiga. Kuivõrd üleriigiline säilitamisnorm tähendaks Euroopa Kohtu praktika kontekstis üldist ning vahet tegemata säilitamist, ei ole see lubatav. Eesti suurust arvestades oleks Belgia juriidilisi piirkondi põhjendatum võrrelda meie nelja maakohtu piirkonnaga (ühtib Politsei- ja Piirivalveameti prefektuuride regionaalse jaotusega):

Joonis 1. Eesti maakohtute tööpiirkonnad


Allikas: Eesti Kohtud.

[136] *StatBel. Total population in Belgium and the regions*, 2014-2024. Veebis: https://bestat.statbel.fgov.be/bestat/crosstable.xhtml?view=fc14c1ce-7361-4d42-a892-fce8e81a1b79 (14.04.2025).

Kõrvutades maakohtute tööpiirkondi Eesti elanike arvuga kohalike omavalitsuste kaupa[137], saab öelda, et Harju Maakohtu tööpiirkonnas elab 649 071 elanikku (47,37% elanikkonnast), Tartu Maakohtu tööpiirkonnas 320 073 elanikku (23,36% elanikkonnast), Viru Maakohtu tööpiirkonnas 186 354 elanikku (13,61% elanikkonnast) ning Pärnu Maakohtu tööpiirkonnas 214 853 elanikku (15,66% elanikkonnast). Vaadates kui suure protsendi elanikkonnast hõlmab iga maakohtu piirkond võib järeldada, et ka sel juhul on tegemist piirkondadega, mis on Belgia omast suuremad. Autori hinnangul on ka selline geograafiline kriteerium liialt ebaproportsionaalne säilitamisega kaasneva põhiõiguste riive suhtes.

Järgmised potentsiaalsed geograafilised kitsendused võiks olla seotud haldusjaotusega. Suurem kriteerium on maakonnad, mille elanike arv varieerub 9778 elanikust (Hiiumaa) 649 071 elanikuni (Harjumaa). Võttes arvesse riigi rahvastiku suurt koondumist Harjumaale ei ole proportsionaalne kasutada ka maakondade kriteeriumit. Väiksem haldusjaotluslik üksus on kohalik omavalitsus ehk vald või linn. Nende elanike arv varieerub 445 elanikust (Vormsi vald) 461 602 elanikuni (Tallinna linn). Taoline sihistamine on autori hinnangul aktsepteeritav juhul, kui täidetakse allpool kasutusele võetava mõõdikuga seatud kriteerium.

Teise viisina saab geograafilist kriteeriumit määratleda läbi pindala – sellise tee valis Taani Kuningriik. Varasemalt sai tuvastatud, et sideandmete säilitamist sihistatakse geograafiliselt läbi kuni 3-ruutkilomeetrilise pindalaga piirkondade. Võttes arvesse, et Taanis on elanikkonna keskmine asustustihedus 136 inimest ruutkilomeetri kohta[138], mõjutab 3 km$^2$ pindalaga alas sideandmete säilitamine keskmiselt 408 inimest. Eesti asustustihedusega 31,6 elanikku ruutkilomeetri kohta[139] tähendab see keskmiselt 95 elaniku ehk 4 korda väiksema hulga inimeste mõjutamist. Järelikult saaks Eestis Taani regulatsiooniga sarnast efekti saavutada siis, kui sideandmeid säilitataks 4 korda suuremal ehk kuni 12km$^2$ suurusel alal. Kuid ka sel juhul ei oleks mõjutatavate elanike arv tasakaalus. Vaadates viimase rahvaloenduse tulemusena tekkinud Eesti rahvastikutiheduse kaarti[140] võib kaardi pealt täheldada selliseid 12km$^2$ suuruseid alasid (umbes 3.5x3.5 ruutu kaardil), kus ei ela ühtegi elanikku. Samas on Tallinnas selliseid 12km$^2$ suuruseid alasid, kus elanike arv ulatub umbes 80 tuhande inimeseni. Siin saaks

[137] Eesti Linnade ja Valdade Liit. Elanike arv kohalike omavalitsuste kaupa. Veebis: https://www.elvl.ee/elanike-arv (14.04.2025).
[138] *Udenrigsministeriet*. Denmark and Ireland key statistics. Veebis: https://irland.um.dk/en/about-denmark/denmark-and-ireland (14.04.2025).
[139] Statistikaameti andmebaas. RV0291U: Rahvaarv, pindala ja asustustihedus, 1. jaanuar. Veebis: https://andmed.stat.ee/et/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV0291U/table/tableViewLayout2 (14.04.2025).
[140] Statistikaamet. Eesti rahva- ja eluruumide loendus 2021. Eesti rahvastikutihenduse interaktiivkaart. Veebis: https://storymaps.arcgis.com/stories/0c3f940a39454a5396432d666e79006e (14.04.2025).

tasakaalustavaks faktoriks olla näiteks tingimus, et Eesti suuremates linnades peab see ala olema väiksem.

Eeltoodust tulenevalt on pindalapõhise geograafilise sihistuse toomine Eesti õiguskorda autori hinnangul äärmiselt raskendatud riigi ebaühtlase asutustiheduse tõttu. Pindala, mis sobib ideaalselt maapiirkonnale toob suurema linna kontekstis kaasa sideandmete säilitamise kohaldamise palju suurema hulga rahvastiku suhtes. Etteruttavalt võib välja tuua ka selle, et pindalapõhise kriteeriumi puhul tekib omajagu raskusi ja koormust säilitamise alla paigutatava pindala valiku põhjendamiseks ning kuritegevuse statistika väljaselgitamiseks. Võttes arvesse, et Justiits- ja Digiministeerium avaldab iga-aastaselt kuritegevuse ülevaateid kus on ka registreeritud kuritegude arv maakondade lõikes[141], eeldab autor, et riigi valduses on ka andmed registreeritud kuritegude arvu kohta väiksemate haldusüksuste, nt valdade ja linnade lõikes. Seega on juba tagatud vähemalt esmane vajadus raskete kuritegude arvu hindamiseks kohaliku omavalitsuste lõikes. Kuna piirkondade määramine peab toimuma teatava regulaarsusega (nt kord aastas teiste liikmesriikide näitel), on igati optimaalsem kasutada juba olemasolevat statistikat, mis aga põhineb riiklikul haldusjaotusel. Nendel põhjustel ning lähtudes soovist vältida üleliigse halduskoormuse tekitamist teeb autor valiku haldusjaotuse põhiseks geograafiliseks sihistamiseks ning seda kohaliku omavalitsuse üksuste lõikes koos erisusega Tallinna linna osas.

Geograafilise asukoha põhilise sihistatud säilitamise teiseks eelduseks on objektiivne ning mittediskrimineeriv mõõdik. Kuna liiklus- ja asukohaandmete kasutamise vajadus tuleneb riigile pandud ülesandest võidelda raske kuritegevusega, on autori hinnangul igati aktsepteeritav tuua mõõdikuks raske kuritegevuse tase geograafilistest piirkondades. Justiits- ja Digiministeeriumi 2023. aasta kuritegevuse ülevaate lehel on võimalik analüüsifaili allalaadimise teel tutvuda registreeritud tervikstatistikaga viimase 10 aasta kohta[142].

Kõrvutades seda statistikat KrMS § $126^2$ lõikes 2 sätestatud jälituskataloogiga saab aimu sellest, kui palju registreeriti jälituskataloogi kuritegusid. Paraku ei ole võimalik tuua välja väga täpne arv, kuna jälituskataloogis on osad kuriteod välja toodud üksnes paragrahvi konkreetse lõike või punktina, aga avalik statistika on esitatud kõigi paragrahviga seotud kuritegude kohta. Lisades ühe statistilise näitajana ka kogu registreeritud kuritegude arvu ning arvutades välja

[141] Justiits- ja Digiministeerium. Kuritegevus Eestis 2023. Veebis: https://www.justdigi.ee/kuritegevus2023/ (14.04.2025).
[142] *Ibid*. Veebis: https://www.justdigi.ee/kuritegevus2023/excel/kuritegevuse_ulevaade.xlsx (14.04.2025).

kataloogikuritegude osakaal saab järeldada järgmist. 2023. aastal registreeriti 27 418 kuritegu, millest täielikult on jälituskataloogis 17 181 kuritegu – järelikult on raskete kuritegude osakaal 62,66%. See protsent tõuseks lisades juurde ka kuriteokoosseisud, mis on kantud jälituskataloogi vaid osaliselt.

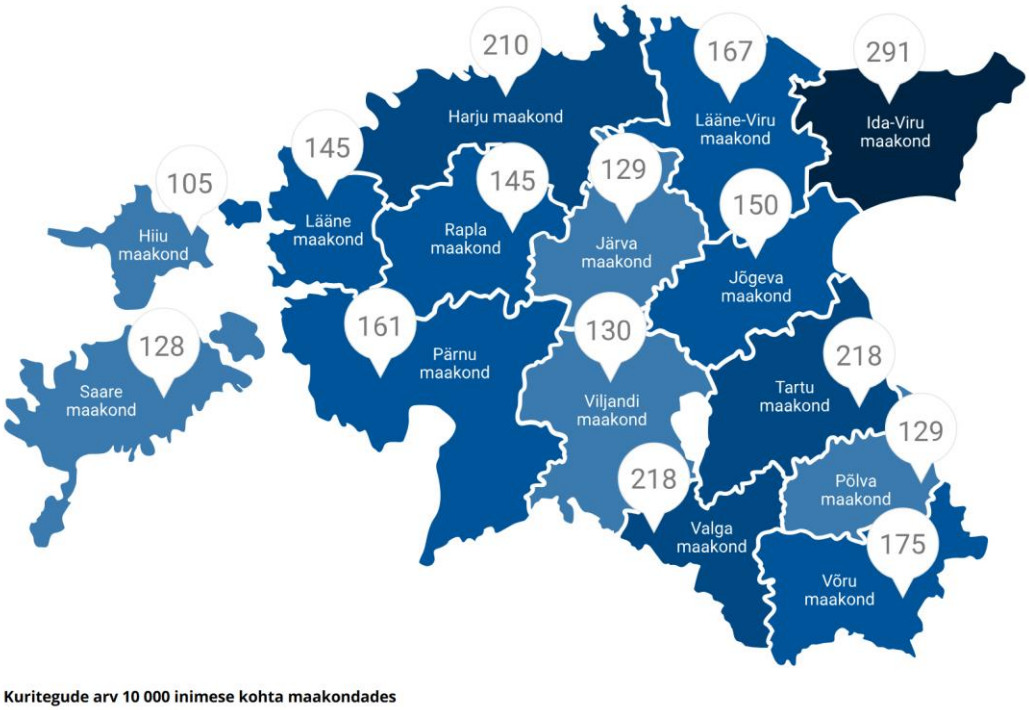
Eesti rahvaarv oli 2023. aastal 1 365 884[143] ning samal aastal registreeriti 17 181 täielikult jälituskataloogi kantud koosseisuga kuritegu, seega registreeriti selliseid kuritegusid 12,57 1000 elaniku kohta. Üleüldse pandi toime 27 418 kuritegu ehk 20 kuritegu 1000 inimese kohta. Kõrvutades seda numbrit Belgia ning Taani õiguses olevast nõudest, et säilitamine võib kõne alla tulla alates 3 raskest kuriteost 1000 elaniku kohta, tuleb analüüsida, kas 3 kataloogikuritegu 1000 elaniku kohta on asjakohane mõõdiku suurus Eesti kontekstis.

3 kataloogikuritegu 1000 inimese kohta tähendab, et, tuginedes linnade ja valdade rahvaarvule[144], näiteks Eesti väikseima valla puhul (Vormsi vald – 445 elanikku) õigustaks sideandmete säilitamist ümardatult täisarvuni 2 kuriteo registreerimine. Näiteks Tartu linnas oleks sel juhul nõutavaks registreeritud kuritegude arvuks 295, Rapla vallas aga 40. Nende asukohamaakondades oleks need numbrid vastavalt Läänemaal 62, Tartumaal 489 ning Raplamaal 102 rasket kuritegu. Selline mõõdiku suurus on autori hinnangul proportsionaalne tehtava riive suhtes. Autor möönab, et kehtestatava mõõdiku täpsem suurus võiks paremini selguda õigusloome protsessi ning poliitilise debati käigus.

Alternatiivselt võiks Taani Kuningriigi näitel kehtestada kohustus säilitada sideandmeid nendes piirkondades, kus registreeriti 3 korda rohkem raskeid kuritegusid 1 000 inimese kohta kui riigis keskmiselt. 2023. aasta lõikes tähendaks see Eesti kontekstis piirkondi, kus pandi toime rohkem kui 37,71 rasket kuritegu 1 000 inimese kohta. Selgitamaks välja, kas Eestis on üldse selliseid piirkondi, tuleb saada andmed regiooniti toimepandud kuritegude arvu või suhtarvu kohta. Justiits- ja Digiministeerium on avaldanud järgnevad andmed registreeritud kuritegude arvu kohta 10 000 inimese kohta maakondades aastal 2023:

[143] Statistikaameti andmebaas. RV021.
[144] Eesti Linnade ja Valdade Liit.

Joonis 2. Kõigi registreeritud kuritegude arv 10 000 inimese kohta maakondades




Allikas: Justiits- ja Digiministeerium.

Kuna joonisel on toodud andmed 10 000 inimese kohta, tuleb analüüsitava mõõdikuga (1 000 inimese kohta) võrdlemiseks jagada joonisel esitatud arvud 10-ga. Selgub, et Eestis ei ole selliseid maakondi, kus registreeritud kuritegude arv 1 000 inimese kohta ületab Taani mudeli järgi arvutatud suhtarvu 37,71. Järelikult on põhjendatud oletada, et sellise mõõdikuga tuleks säilitamine kõne alla väid üksikutes kohaliku omavalitsuse üksustes.

Järelikult on otstarbekas kehtestada mõõdik Belgia mudeli alusel, tuues kõrvale ka autori valitud geograafiline kriteerium valdade ja linnade ehk kohaliku omavalitsuse üksuste näol. Autori hinnangul võiks, sarnaselt kõigile teistele, anda säilitamiskohustuse kehtestamise õiguse justiitsministrile oma määrusega. Samuti pole põhjust muuta ESS § $111^1$ lõikes 4 sätestatud üheaastast säilitamistähtaega, kuivõrd üldjuhul ei kesta aktiivne kohtueelne menetlus üle aasta ning see säilitamistähtaeg on ka võrdne teistes liikmesriikides kehtestatuga.

Tulenevalt eeltoodust teeb autor ettepaneku luua Eesti õiguskorda asukohapõhiselt sihistatud liiklus- ja asukohaandmete säilitamine. Selleks tuleb täiendada elektroonilise sätte seadust uue sättega, mis lubab kohustada sideettevõtjaid säilitama ESS § $111^1$ lõigetes 2 ja 3 loetletud liiklus- ja asukohaandmed, mis on tekkinud kohaliku omavalitsuse üksustes, kus registreeritud KrMS § $126^2$ lõikes 2 loetletud kuritegude arv selle piirkonna 1000 elaniku kohta on suurem

kui 3. Käesolevas sättes nimetatud piirkondade loetelu peaks autori ettepanekul kehtestama iga-aastaselt justiitsvaldkonna eest vastutav minister määrusega.

### 3.3. Sideandmete ajutine kiirsäilitamine kriminaalmenetluse raames

Autor soovib anda ka ettepaneku sideandmete ajutiseks kiirsäilitamiseks konkreetse kriminaalmenetluse raames. Selline regulatsioon võimaldaks uurimisasutustel ja prokuratuuril tagada olulist tõendiväärtust omavate sideandmete säilimine selleks, et neid saaks hiljem kasutada tõendina kriminaalmenetluses. See regulatsioon aitaks ka adresseerida neid geograafilisi paikkondi, mida eelmise ettepanekuga kirjeldatud asukohapõhise sihistatud säilitamise kord ei kataks liiga madala raske kuritegevuse tase tõttu. Autor ei tee sarnast ettepanekut väärteomenetluste kontekstis, kuna liiklus- ja asukohaandmete kasutamine ei ole selliste süütegudega võitlemiseks Euroopa Kohtu poolt lubatud. Tagamaks kiirsäilitamise piiritlemist vältimatult vajalikuga on otstarbekas kehtestada säilitamiskorraldusele 6-kuuline ajaline piirang, sarnaselt Taani Kuningriigis kehtestatud piirangule.

Tuginedes varasemalt käsitletud liikmesriikide ning eeskätt Belgia Kuningriigi regulatsioonile teeb autor ettepaneku luua kriminaalmenetluse seadustikku paragrahv, mis annab võimaluse teha sideettevõtjale korraldus säilitada kriminaalmenetluse tarbeks isiku, elektroonilise side seadme või paikkonnaga seotud sideandmed. Säilitatavate sideandmete valim võiks olla defineeritud läbi KrMS § $90^1$ lõike 2, kuna antud regulatsioon nimetab ammendavalt ära sideandmed viitega elektroonilise side seaduse vastavale normile. Korralduse kehtivuse aeg peaks olema piiritletud vältimatult vajalikuga, kuid see ei saa olla kauem kui 6 kuud.

Taolise regulatsiooni puhul on oluline kehtestada ka kitsendused KrMS § $90^1$ lg 2 näitel. Nimelt võiks sellise korralduse andmine olla lubatav üksnes siis, kui tegemist on käesoleva seadustiku § $126^2$ lõikes 2 nimetatud kuriteoga ning kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Loetelus nimetamata kuritegude korral võiks säilitamiskorraldus olla lubatud siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks ning seda õigustab kuriteo raskus ja laad ning kui päringuga ei riivata põhjendamatult isikuõigusi.

Ajutise kiirsäilitamise korralduse peaks andma prokuratuur oma määrusega, kuid säilitamisloaga ei tohi automaatselt kaasneda ka ligipääsuõigus nendele andmetele - seda mitmel põhjusel. Esiteks seetõttu, et Euroopa Kohtu hinnangul on kiirsäilitamise otsust pädev tegema kohtulikult kontrollitav asutus. Prokuratuur on selline asutus, kuna tema suhtes teostatakse järelevalvet läbi kriminaalasja sisulise menetlemise kohtus, kohtuliku

jälitustegevuse järelevalve ning samuti läbi prokuratuuri otsuste kohtusse kaevatavuse. Prokuratuur kohtulikult kontrollitava asutusena saaks käsitleda säilitamise määruses andmete säilitamise põhjenduse, säilitamisele kuuluvad andmed ning toiminguga tehtava riive vältimatut vajadust kriminaalmenetluse eesmärgi suhtes. Teiseks ei ole otstarbekas määrata sideandmete kiirsäilitamisele eraldi kohtulikku kontrolli, kuna see teostatakse igal juhul siis, kui prokuratuur asub taotlema sideandmete väljanõudmise päringu esitamist. Taotluse läbivaatamise raames saab kohus muuhulgas kontrollida seda, kas prokuratuuri poolt antud säilitamiskorraldus oli põhjendatud ning seadusega kooskõlas. Sellise regulatsiooni kasuks räägib ka asjaolu, et suurema riivega toimingute (näiteks varjatud jälgimiste) luba annab prokuratuur ning kohtueelses menetluses ei ole ette nähtud otsest kohtulikku kontrolli selle toimingu järele.

Tuginedes eeltoodule teeb autor ettepaneku luua kriminaalmenetluse seadustikku täiendav säte, mis annab võimaluse teha sideettevõtjale korraldus säilitada kriminaalmenetluse tarbeks isiku, elektroonilise side seadme või paikkonnaga seotud ESS § $111^1$ lõigetes 2 ja 3 nimetatud andmed kestvusega kuni 6 kuud alates korralduse andmisest. Sellise korralduse andmine peab olema lubatav üksnes siis, kui tegemist on käesoleva seadustiku § $126^2$ lõikes 2 nimetatud kuriteoga ning kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Loetelus nimetamata kuritegude korral võib säilitamiskorraldus olla lubatud siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks ning seda õigustab kuriteo raskus ja laad ning kui päringuga ei riivata põhjendamatult isikuõigusi. Korralduse sideandmete säilitamiseks peab andma prokuratuur oma määrusega ning ligipääs andmetele peab toimuma KrMS paragrahviga $90^1$ sätestatud alusel ja korras. Korralduses peavad olema märgitud andmed, mida korraldusega on lubatud koguda, andmete säilitamise põhjendus ning ajavahemik, mille kohta on andmeid lubatud koguda (korralduse kehtivuse aeg).

### 3.4. Sideandmete säilitamine riigi julgeoleku tagamiseks

Eesti julgeolekukeskkond on turbulentne. Välisluureameti hinnangul on Venemaa Föderatsiooni eesmärk domineerida sõjaliselt Läänemere regioonis. Venemaal läbiviidav relvajõudude reform mõjutab otseselt Eestit, kuna sellega on oodata Vene Föderatsiooni relvajõudude suuremat kohalolu ning suuremat alalist paiknemist Eesti piiri läheduses[145]. Ka Riigikogu poolt heaks kiidetud Eesti julgeolekupoliitika alustes tuuakse Eesti jaoks suurima julgeolekuohuna idanaabrit Venemaad, mööndakse ka eksistentsiaalset ohtu. Hetkel tajutav mittesõjaline oht seisneb Venemaa läbiviidavates hübriidrünnakutes, mille eesmärk on

[145] Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2024. Tallinn, 2024. Lk 15-18. Veebis: https://www.valisluureamet.ee/doc/raport/2024-et.pdf (23.04.2025).

kallutada siseriiklikud ning rahvusvahelised poliitilised ja ühiskondlikud hoiakud ning valikud Venemaale sobivas suunas[146]. Kaitsepolitseiamet fikseerib pidevalt Vene eriteenistuste aktiivset tegevust piiril. Näiteks kogub Venemaa Föderaalne Julgeolekuteenistus (FSB) koos enda koosseisu kuuluva Piirivalveteenistusega suures ulatuses andmeid Eesti-Vene piiri ületajate, nende meelsuse ning sugulaste kohta - välistatud ei ole ka nendega kaasas olevate sideseadmete kontroll[147].

Varasemalt analüüsitud liikmesriikidest on pea kõik näinud oma õiguskorras ette ka erakorralise võimaluse sideandmete üleriigilise laussäilitamise käivitamiseks juhul, kui esineb objektiivselt hinnatav tõsine riiki ohustav julgeolekuoht. Arvestades Euroopa ning konkreetselt Eesti praegust julgeolekupilti on autori hinnangul igati põhjendatud näha ette sarnane meede liiklus- ja asukohaandmete ka meie õiguskorras. Säilitamisotsuse vastuvõtmise kord võiks rajaneda teise Läänemere piirkonna riigi ehk Taani Kuningriigi eeskujul. Sisuliselt on sarnane säilitamisotsus juba Eesti õiguskorras ette nähtud ESS § $111^1$ lõikega 6, kuid tulenevalt eelnevalt läbiviidud analüüsist ning regulatiivsetest ettepanekutest ei tohi üldine säilitamine kohalduda automaatselt ka liiklus- ja asukohaandmetele. Seega teeb autor ettepaneku täiendada elektroonilise side seadust normiga, mis lubab käivitada ka liiklus- ja asukohaandmete säilitamine riigi julgeoleku huvides.

Sellise liiklus- ja asukohaandmete säilitamine peaks olema lubatav üksnes juhul, kui esineb reaalne ehk objektiivselt hinnatav ning tõsine Eesti Vabariiki ohustav julgeolekuoht, mis on saabunud või saabub lähitulevikus. Säilitamisotsuse võiks Taani ja Belgia eeskujul langetada täidesaatva võimu esindaja oma määrusega. Võttes arvesse, et tegemist on äärmiselt riivava ning kõigi Eesti elanikke hõlmava säilitamistoiminguga, peaks säilitamisotsuse langetama ESS § $111^1$ lg 6 näitel Vabariigi Valitsus. Otsuse kehtivus võiks sarnaselt teistele ESS normidele olla lubatud kuni 12 kuuks.

Tulenevalt eeltoodust teeb autor ettepaneku täiendada elektroonilise side seadust paragrahviga, mis annab Vabariigi Valitusele õiguse käivitada liiklus- ja asukohaandmete üldine ning vahet tegemata säilitamine kogu Eesti Vabariigi territooriumil kuni 12 kuuks juhul, kui esineb hinnatav ning tõsine Eesti Vabariiki ohustav julgeolekuoht, mis on saabunud või saabub lähitulevikus.

[146] Riigikogu 22.02.2023 otsus ”Eesti julgeolekupoliitika alused” heakskiitmine. RT III, 28.02.2023, 1. Lisa 1, lk 3.
[147] Tuul, M. Kaitsepolitsei aastaraamat 2024-2025. Tallinn, 2025. Lk 30. Veebis. https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf (23.04.2025).

Lisaks on mitmed liikmesriigid näinud ette sideandmete (sh liiklus- ja asukohaandmete) üldise ning vahet tegemata asukohapõhise säilitamise asukohtades, mis on riigi julgeoleku vaatest eriti haavatavad. Varasemalt sai tuvastatud, et nendeks on asukohad või kinnistud, kus asuvad põhiseaduslikud institutsioonid, täidesaatva võimu põhilised asutused (nt ministeeriumid) õiguskaitse- ning julgeolekuasutused, riigi põhilised transpordisõlmed, militaarobjektid ning riigipiir. Asukohtade üldist haavatavust möönab ka Eesti õigus. Nimelt on riigikaitseseaduse[148] §-ga 83 sätestatud riigikaitseobjekti definitsioon. RiKS § 83 lg 1 kohaselt on see ala, mille ründamise, hõivamise, kahjustamise või hävitamisega kaasneb oht riigi julgeolekule või kõrgendatud oht avalikule korrale. Kuigi objektile riigikaitseobjekti staatuse omistamisega seotud aktid ei ole avalikud ning tihtipeale riigisaladust sisaldatavad, on RiKS § 83 lg 1 sõnastusest igati põhjendatud järeldada, et põhiseaduslikud ja täidesaatva võimu institutsioonid, samuti õiguskaitse- ning julgeolekuasutuste kasutusel olevad asukohad kuuluvad RiKS § 83 lõike 2 alusel kehtestatud kategooriatesse. Autori hinnangul on, tuginedes nendele kategooriatele, igati põhjendatud kehtestada asukohapõhine laussäilitamine riigikaitseobjekti ning selle vahetus läheduses (nt kinnistut ümbritsevate teede) piires.

Lisaks riigikaitseobjektidele võib olla põhjendatud sideandmete üldine säilitamine riigi suurimates transpordisõlmedes, milleks on lennujaamad, põhilised sadamad, suuremad bussijaamad, rongijaamad ning hetkel ehitusjärgus olev Rail Baltica rahvusvaheline rongiterminal. Kaitsepolitseiamet toob transpordisõlmede kontekstis näiteks 2017. aastal aset leidnud lõhkeainetega seotud terroriintsidendid Londoni metroopeatuses ning Brüsseli rongijaamas[149]. Minimaalselt võiks taoline säilitusmeede olla piiratud riigi põhiliste rahvusvahelise transpordi sõlmedega, milleks on autori hinnangul Tallinna ja Tartu lennujaamad, Tallinna sadama reisi- ja kruiisiterminalid, Tallinna, Tartu ja Pärnu bussijaamad, Balti jaam ning tulevikus valmiv Rail Baltica reisiterminal. Oluliste transpordisõlmede täpsem valik võiks autori hinnangul selguda õigusloome protsessi ning poliitilise debati käigus.

Võttes arvesse turbulentset julgeolekuolukorda ning idanaabrist tulenevat ohtu oleks põhjendatud kaaluda ka kõigi sideandmete üldist asukohapõhist säilitamist Eesti riigipiiri vahetus läheduses. Eesti riigipiiri puhul põhjendab haavatavust see, et meie piir on suures osas käsitletav EL ja NATO välispiirina – teisel pool välispiiri asub Venemaa Föderatsioon, mille tegevuse ohtu Eesti julgeolekule on käsitletud eespool. Piiripõhine säilitusmeede võiks olla rakendatud vähemalt Eesti-Vene piiril ning seda vähemalt piirivööndi laiusel alal. Piirivööndi

[148] Riigikaitseseadus - RT I, 14.03.2023, 31.
[149] Tuul, M. lk 56.

mõiste tuleneb riigipiiri seadusest[150]. RiPS § $6^1$ kohaselt on piirivöönd kuni viie kilomeetri laiune piiriga külgnev maa-ala sisemaa poole, mis kehtestatakse riigipiiri valvamiseks ja kaitsmiseks ning piirirežiimi tagamiseks. Samas ei ole välistatud piiripõhise laussäilitamise kehtestamine ka suuremale maa-alale, kuid sellisel juhul peaks see olema põhjendatud objektiivselt hinnatava ohukriteeriumiga.

Tulenevalt eeltoodust teeb autor ettepaneku täiendada elektroonilise side seadust õigusnormiga, mis lubab liiklus- ja asukohaandmete üldist ning vahet tegemata säilitamist riigikaitseobjektide territooriumil ning nende vahetus läheduses, riigi olulisemates transpordisõlmedes ning piirivööndis riigipiiri seaduse mõistes. Riigi julgeoleku tagamiseks kehtestatud säilitamisnormide alusel säilitatud andmetest võib olla äärmiselt suur kasu avaliku korra ning julgeoleku vastaste kuritegude uurimisel. Täiendavalt on sellisest meetmest kasu ka julgeolekualaste ülesannete täitmisel. Nimelt pääseks nendel säilitamisalustel säilitatud andmetele põhjendatud vajaduse korral ligi ka julgeolekuasutuste seaduses[151] (JAS) nimetatud julgeolekuasutused.

Selleks on julgeolekuasutustele ette nähtud eraldiseisev sideandmete kasutamisnorm - õigus piirata isiku õigust eraelu puutumatusele läbi õiguse koguda andmeid elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha kohta JAS § 26 lg 3 p 4 alusel. JAS § 27 lg 3 alusel otsustab sideandmete kasutamise kuni kaheks kuuks julgeolekuasutuse juht või tema poolt volitatud ametnik. Seejuures eeldab toiming, tulenevalt JAS § 27 lõikest 4, selle läbiviimist kooskõlas ESS nõuetega.

Seega teeb autor kaks ettepanekut liiklus- ja asukohaandmete säilitamiseks riigi julgeoleku tagamise eesmärgil. Esiteks teeb autor ettepaneku täiendada elektroonilise side seadust paragrahviga, mis annab Vabariigi Valitusele õiguse käivitada liiklus- ja asukohaandmete üldine ning vahet tegemata säilitamine kogu Eesti Vabariigi territooriumil kuni 12 kuuks juhul, kui esineb hinnatav ning tõsine Eesti Vabariiki ohustav julgeolekuoht, mis on saabunud või saabub lähitulevikus. Teiseks teeb autor ettepaneku täiendada elektroonilise side seadust õigusnormiga, mis lubab liiklus- ja asukohaandmete üldist ning vahet tegemata asukohapõhist säilitamist riigikaitseobjektide territooriumil ning nende vahetus läheduses, riigi olulisemates transpordisõlmedes ning piirivööndis riigipiiri seaduse mõistes.

[150] Riigipiiri seadus - RT I, 07.06.2024, 13.
[151] Julgeolekuasutuste seadus - RT I, 14.03.2023, 25.

# KOKKUVÕTE

Sideandmed on sideteenuse osutamise käigus tekkinud andmed sideteenuse kasutamise üksikasjade kohta ning sidevõrgu kaudu edastatava sõnumi vormi, aja ja viisi kohta. Sideandmed jagunevad liigiti, vastavalt nendega kaasneva põhiõiguste riive raskusele, identifitseerimisandmeteks, liiklusandmeteks ning asukohaandmeteks. Identifitseerimisandmed võimaldavad tuvastada sideteenuste lõppkasutajate identiteet või lähteabonendile omistatud IP-aadress. Liiklusandmed võimaldavad tuvastada sideseansi toimumise või sideteenuse kasutamise fakt ning sellega seotud asjaolud, välja arvatud andmed edastatud sõnumi sisu kohta. Asukohaandmed võimaldavad tuvastada kus asus sidevahend sideteenuse osutamise, sideseansi kestuse või levi tugevuse tuvastamispäringu saatmise ajal.

Sideandmete lubatav kasutamine tõendina süüteomenetluses eeldab õiguspärast kahekomponendilist regulatsiooni. Siseriiklik õigus peab ette nägema õiguspärase ning nõuetele vastava sideandmete säilitamise regulatsiooni ja sideandmete kasutamise regulatsiooni. Esimene komponent hõlmab endas sideandmete kogumist sideettevõtja poolt ning nende edaspidist säilitamist, teine komponent hõlmab endas säilitatud sideandmete väljanõudmist sideettevõtjalt ning nende edaspidist kasutamist tõendina.

Sideandmete säilitamist kasutamiseks süüteomenetlustes reguleerib Eestis ESS § $111^1$. Antud õigusnorm sätestab sideettevõtjatele kohustuse säilitada üldiselt ning vahet tegemata kõiki sideandmeid seoses vajadusega kasutada neid andmeid põhjendatud korral süütegude menetlemiseks, julgeoleku tagamiseks ning spetsiifiliste haldus- ja tsiviilkohtumenetluste läbiviimiseks. Lisaks on sideettevõtjal õigus säilitada sideandmed ärilistel eesmärkidel ulatuses, mis on vajalik arvete koostamiseks, teenuste turustamiseks ning lisaväärtusteenuste osutamiseks.

Sideandmete kasutamist süüteomenetlustes näevad ette KrMS § $90^1$ ning VTMS § $31^2$. Kasutamise regulatsioon näeb kriminaalmenetluses menetlejale ning väärteomenetluses seadusesättes loetletud kohtuvälisele menetlejale õiguse teha iseseisvalt päring sideettevõtjale identifitseerimisandmete saamiseks. Kõikide teiste sideandmete puhul tuleb andmete väljanõudmise päringu jaoks saada kohtu luba prokuratuuri või kohtuvälise menetleja põhistatud taotluse alusel. Ligipääs on õigustatud üksnes juhul, kui see on vältimatult vajalik kriminaal- või väärteomenetluse eesmärgi saavutamiseks.

Euroopa Kohtu praktikast tulenevad mitmed kriteeriumid, millele peab vastama Eesti sideandmete säilitamise ja kasutamise regulatsioon. Põhilise kriteeriumina ei tohi siseriiklik regulatsioon, lähtuvalt Euroopa Kohtu otsustest *Digital Rights Ireland et al* ning *Tele2 Sverige et al* asjades, näha ette liiklus- ja asukohaandmete üldist ning vahet tegemata säilitamist. Küll aga on selline kohustus ette nähtud ESS §-iga 111[1], mistõttu on Eesti sideandmete säilitamise regulatsioon vastuolus EL õigusega. Euroopa Kohus selgitas, et sideandmed ning eriti liiklus- ja asukohaandmed kogumis võimaldavad teha väga täpseid järeldusi isikute eraelu kohta, näiteks isikute harjumuste, elukoha, harrastatavate tegevuste, sotsiaalsete tegevuste ja grupikuuluvuse kohta. See omakorda toob kaasa eriti raske Euroopa Liidu põhiõiguste harta artiklis 7 ja 8 sätestatud õiguste, ehk eraelu puutumatuse ning isikuandmete kaitse põhiõiguste, riive. Antud riive on niivõrd raske, et liiklus- ja asukohaandmete säilitamine saab olla lubatud üksnes võitluseks raske kuritegevusega või riigi julgeoleku kaitsmiseks.

Liiklus- ja asukohaandmete üldine ja vahet tegemata säilitamine on, lähtuvalt Euroopa Kohtu otsusest *La Quadrature du Net et al* asjas, lubatud vaid erandjuhul, kui see toimub ajutiselt riigi julgeoleku kaitse eesmärgil. Lisaks võib selline säilitamine toimuda alaliselt ning üldiselt riigi julgeoleku vaatest haavatavates asukohtades, nagu selleks on transpordisõlmed ning riikliku tähtsusega hooned. Samas võib, lähtuvalt Euroopa Kohtu otsustest asjades *Ministerio Fiscal et al* ning *La Quadrature du Net et al*, säilitada üldiselt ning vahet tegemata identifitseerimisandmed sidevahendi kasutaja isiku kohta ning tingimata vajalikud identifitseerimisandmed lähteabonendile määratud IP-aadresside kohta.

Üldise ning vahet tegemata säilitamise asemel võib siseriiklik regulatsioon, tulenevalt Euroopa Kohtu seisukohast *Tele2 Sverige et al* ning *La Quadrature du Net et al* asjades, näha ette liiklus- ja asukohaandmete sihistatud säilitamist võitlemiseks raske kuritegevusega või riigi julgeolekuohtudega. Euroopa Kohus pidas *La Quadrature du Net et al* otsuses lubatavaks säilitada liiklus- ja asukohaandmed ajutiselt isiku- või asukohapõhiselt objektiivsete ja mittediskrimineerivate asjaolude alusel, näiteks pärast kohtu või sõltumatu haldusasutuse kontrolli isikute suhtes, kelle puhul on mõjuv põhjus kahtlustada, et nad on ühel või teisel viisil seotud terrorismiga. Samuti pidas Euroopa Kohus lubatavaks konkreetse isiku, sideallika või paikkonnaga seotud sideandmete ajutist kiirsäilitamist kohtulikult kontrollitava asutuse, näiteks prokuratuuri otsusega.

Sideandmete kasutamist ehk väljanõudmist pidas Euroopa Kohus oma otsusega *Tele2 Sverige et al* asjas lubatavaks üksnes pärast kohtu või sõltumatu haldusasutuse kontrolli – selliseks

asutuseks ei saa olla prokuratuur. Ligipääs sideandmetele peab olema piiritletud üksnes vältimatult vajalikuga ning ligi tohib pääseda üksnes sellistele sideandmetele, mida on kogutud ja säilitatud õiguspäraselt ning kooskõlas EL õigusega. Seejuures võib liiklus- ja asukohaandmetele ligi pääseda üksnes võitluseks raske kuritegevusega ja riigi julgeoleku kaitseks.

Töös analüüsitud Euroopa Kohtu otsuste järel asusid liikmesriigid uuendama enda sideandmete regulatsioone, et viia nad kooskõlla EL õigusega. Seda teed läks ka Eesti, täiendades enda sideandmete kriminaalmenetlustes kasutamise regulatsiooni – seejuures ei ole Eestis jätkuvalt muudetud sideandmete säilitamist puudutavat regulatsiooni, mis on oma üldise ning vahet tegemata säilitamiskohustuse tõttu vastuolus EL õigusega. Kui umbes poolte liikmesriikide õiguses on õiguse uuendamise protsess jätkuvalt pooleli, siis teistes riikides on kasutusele võetud erinevad sideandmete regulatsioonid. Nendest riikidest paistavad enim silma Belgia Kuningriik ja Taani Kuningriik, kellel on äärmiselt detailne ning mitmekesine sideandmete säilitamise regulatsioon. Osad liikmesriigid, nagu Rootsi ja Portugal, otsustasid piirata säilitatavate andmete liike nende liikidega, mille puhul on Euroopa Kohus pidanud lubatavaks üldist ning vahet tegemata säilitamist. Nendeks andmeteks on identifitseerimisandmed ehk andmed lähtepunktile omistatud IP-aadresside või sideseansi lõppkasutaja identiteedi kohta.

Belgia Kuningriik kehtestas enda õiguses sideandmete asukohapõhise sihistatud kogumise ja säilitamise regulatsiooni. Antud regulatsioon tugineb põhimõttele, et sideandmete säilitamine on lubatud sellistes piirkondades, kus registreeritakse kolm või enam rasket kuritegu 1000 elaniku kohta. Piirkondade suuris on piiritletud Belgia 12 juriidilise piirkonnaga, alternatiivselt nendes olevate politseipiirkondadega. Seega kehtestatakse säilitamisele allutatavad piirkonnad tuginedes statistilistele andmetele registreeritud kuritegude kohta. Belgia regulatsioon paneb paika ka säilitamistähtajad – sideandmeid peab säilitama 6-12 kuu jooksul sõltuvalt selles, mitu rasket kuritegu 1000 inimese kohta piirkonnas toime pandi. Säilitamise kohustuse kehtestavad riigi sise- ning justiitsminister iga-aastaselt, tuginedes eelkirjeldatud reeglitele. Samuti näeb Belgia siseriiklik õigus ette kohustuse säilitada sideandmed riigi julgeoleku tagamiseks piirkondades, mis on eriti haavatavad julgeolekuohtudele ning rasketele kuritegudele – nendeks on riigiasutuste hooned, transpordisõlmed, piirialad ning militaarobjektid.

Põhjaliku sideandmete säilitamise regulatsiooniga paistis silma ka Taani Kuningriik. Nende siseriiklik regulatsioon näeb ette võimaluse säilitada isikupõhiselt raske kuriteo toimepanemises süüdi mõistetud isiku poolt sideteenuse kasutamisega tekkivaid sideandmeid

3-10 aasta jooksul sõltuvalt temale karistusena mõistetud vangistuse pikkusest. Sarnaselt Belgiale kehtib ka Taanis sideandmete asukohapõhise sihistatud säilitamise regulatsioon. Küll aga läheneb Taani õigus objektiivsetele säilitamiskriteeriumitele teisiti. Nimelt on Taanis ette nähtud õigus kohustada sideettevõtjat säilitama 1 aasta jooksul sideandmeid kuni 3km$^2$ pindalaga piirkondades, kus registreeritud raskete kuritegude arv on 1.5 korda suurem kui riigis keskmiselt või kus elanikena on registreeritud 1.5 korda rohkem raskete kuritegude toimepanemise eest süüdimõistetuid kui riigis keskmiselt. Ka Taani õiguses on ette nähtud sideandmete säilitamine riigi julgeoleku vaatest suure haavatavusega objektide läheduses.

Kuna Euroopa Kohus pidas *La Quadrature du Net et al* otsusega lubatavaks ka sideandmete nn kiirsäilitamist konkreetse menetluse raames, kehtestasid mitmed liikmesriigid vastava siseriikliku regulatsiooni. Belgias annab kiirsäilitamise loa prokuratuur vähemalt 1-aastast vangistust ette nägeva kuriteo toimepanemise kahtluse korral, luba kehtib 2 kuud ning selle jooksul kogutud sideandmeid peab sideettevõtja säilitama 6 kuu kestel. Taani õigus näeb ette võimaluse kohustada sideettevõtteid koguma sideandmeid kuni 6 kuu kestel (pikendamise võimalusega) isikute, seadmete või konkreetsete piirkondade kohta juhul, kui esineb põhjendatud alus arvata, et see on seotud raskete kuritegude toimepanemisega.

Mitmed liikmesriigid, nagu Belgia, Taani ning Iirimaa, on näinud oma õiguses ette võimaluse käivitada üldine ning vahet tegemata sideandmete säilitamine üleriigiliselt või konkreetses piirkonnas riiki ohustava tõsise ning objektiivselt hinnatava julgeolekuohu korral, nagu seda on lubanud Euroopa Kohus *La Quadrature du Net et al* otsuses. Belgia õiguse kohaselt kehtestatakse sideandmete säilitamise kohustus piirkondades, kus riikliku rangelt kehtestatud metoodikale tugineval ohuhinnangul on tuvastatud eriti suur ohutase riigi julgeolekule - töö koostamise seisuga on esineb selline ohutase kogu riigi territooriumil. Taanis käivitab üldise säilitamise kestusega kuni 1 aasta justiitsminister, kui esinevad piisavalt kaalukad asjaolud mis viitavad sellele, et riiki ohustab reaalne hetkel või tulevikus aset leidev julgeolekuoht. Erinevalt Belgia ja Taani regulatsiooni langetab Iirimaal sellise otsuse kohus. Iiri õiguse kohaselt esitab valdkonna eest vastutav minister riigi kõrgeima kohtu esimehe määratud kohtunikule või kohtunikele taotluse sideandmete üleriigiliseks säilitamiseks 12 kuu jooksul juhul, kui ministri hinnangul esineb tõsine ning reaalne olemasolev või tulevikus aset leidev oht riigi julgeolekule.

Tuginedes Euroopa Kohtu kehtestatud sideandmete kogumise ja säilitamise lubatavuse kriteeriumitele ning liikmesriikide näidetele nende kriteeriumite praktilisel rakendamisel on võimalik koostada regulatiivsed ettepanekud kehtivale sideandmete säilitamist ja kasutamist

puudutavale regulatsioonile selleks, et viia see kooskõlla EL õigusega ning tagada seeläbi sideandmete kasutamise lubatava tõendina süüteomenetlustes.

Esiteks teeb autor ettepaneku sideandmete kasutamise regulatsiooni täiendamiseks, täpsemalt ettepaneku eemaldada menetlusseadustikes olev konkreetne viide ESS §-le $111^1$ üldise viitega elektroonilise side seadusele, et õiguslikult oleks võimalik nõuda välja need sideandmed, mida säilitatakse autori allpool käsitletud ettepanekute alusel. Selleks teeb autor ettepaneku sõnastada KrMS § $90^1$ lg 3 ümber selliselt, et uurimisasutus võib teha prokuratuuri taotlusel ja eeluurimiskohtuniku loal kohtueelses menetluses või kohtu loal kohtumenetluses päringu elektroonilise side ettevõtjale elektroonilise side seaduse alusel säilitatud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi lõikes 1. Samuti teeb autor ettepaneku sõnastada VTMS § $32^2$ lg 2 ls 1 ümber selliselt, et käesoleva paragrahvi lõikes 1 nimetatud asutus võib kohtu loal teha üksikpäringu elektroonilise side seaduse alusel säilitatud andmete kohta, mida ei ole nimetatud käesoleva paragrahvi esimeses lõikes. Seejuures jääb mõlema sätte puhul kehtima vältimatu vajalikkuse kriteerium.

Järgmisena teeb autor ettepaneku muuta ESS § $111^1$ lõikeid 1, 2, 3 ja 4 selliselt, et teenuseosutaja on kohustatud säilitama vastavas lõikes sätestatud andmeid käesolevas seaduses säilitatud juhtudel 1 aasta jooksul nende tekkimisest või ajutise kiirsäilitamise korral kriminaalmenetluse seadustikus sätestatud tingimustel. Seeläbi ei nõua need normid enam üldist ning vahet tegemata liiklus- ja asukohaandmete säilitamist, vaid täidavad üksnes defineerivat, sõnastades konkreetsed andmeliigid mida tuleb säilitada seaduses sätestatud juhtudel ehk autori edaspidi antud ettepanekute alusel loodud uute normide alusel.

Autor teeb ettepaneku luua Eesti õiguskorda asukohapõhiselt sihistatud liiklus- ja asukohaandmete säilitamine, võttes aluseks Taani ning Belgia kehtestatud mõõdikud ning autori läbiviidud analüüsi nende mõõdikute sobivuse kohta. Selle tulemusena tuleb autori ettepanekul täiendada elektroonilise sätte seadust uue sättega, mis lubab kohustada sideettevõtjaid säilitama ESS § $111^1$ lõigetes 2 ja 3 loetletud liiklus- ja asukohaandmed, mis on tekkinud kohaliku omavalitsuse üksustes, kus registreeritud KrMS § $126^2$ lõikes 2 loetletud kuritegude arv selle piirkonna 1000 elaniku kohta on suurem kui 3. Käesolevas sättes nimetatud piirkondade loetelu peaks autori ettepanekul kehtestama iga-aastaselt justiitsvaldkonna eest vastutav minister määrusega.

Autor annab ka ettepaneku sideandmete ajutiseks kiirsäilitamiseks konkreetse kriminaalmenetluse raames. Selleks teeb autor ettepaneku luua kriminaalmenetluse seadustikku täiendav säte, mis annab võimaluse teha sideettevõtjale korraldus säilitada kriminaalmenetluse tarbeks isiku, elektroonilise side seadme või paikkonnaga seotud ESS § $111^1$ lõigetes 2 ja 3 nimetatud andmed kestvusega kuni 6 kuud alates korralduse andmisest. Sellise korralduse andmine peab olema lubatav üksnes siis, kui tegemist on käesoleva seadustiku § $126^2$ lõikes 2 nimetatud kuriteoga ning kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Loetelus nimetamata kuritegude korral võib säilitamiskorraldus olla lubatud siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks ning seda õigustab kuriteo raskus ja laad ning kui päringuga ei riivata põhjendamatult isikuõigusi. Korralduse sideandmete säilitamiseks peab andma prokuratuur oma määrusega ning ligipääs andmetele peab toimuma KrMS paragrahviga $90^1$ sätestatud alusel ja korras. Korralduses peavad olema märgitud andmed, mida korraldusega on lubatud koguda, andmete säilitamise põhjendus ning korralduse kehtivuse aeg ehk aeg, mille kohta on andmeid lubatud koguda.

Arvestades Eesti julgeolekukeskkonna turbulentsust teeb autor viimaks ettepanekud kehtestada regulatsioonid sideandmete säilitamiseks riigi julgeoleku kaitse eesmärgil. Esiteks teeb autor ettepaneku täiendada elektroonilise side seadust paragrahviga, mis annab Vabariigi Valitusele õiguse käivitada liiklus- ja asukohaandmete üldine ning vahet tegemata säilitamine kogu Eesti Vabariigi territooriumil kuni 12 kuuks juhul, kui esineb hinnatav ning tõsine Eesti Vabariiki ohustav julgeolekuoht, mis on saabunud või saabub lähitulevikus. Kaitsmaks Eesti riikliku julgeoleku vaatest eriti haavatavaid objekte teeb autor ka ettepaneku täiendada elektroonilise side seadust õigusnormiga, mis lubab liiklus- ja asukohaandmete üldist ning vahet tegemata asukohapõhist säilitamist riigikaitseobjektide territooriumil ning nende vahetus läheduses, riigi olulisemates transpordisõlmedes ning piirivööndis riigipiiri seaduse mõistes.

Töös esitatud regulatiivsed ettepanekud võimaldavad viia Eesti sideandmete säilitamise ja kasutamise regulatsioon kooskõlla EL õigusega. Ettepanekute kasutusele võtmise korral võib muudatuste täpsem sõnastus selguda kõige efektiivsemalt õigusloome protsessi ning poliitilise debati käigus. Küll aga tagavad need ettepanekud, et sideandmete säilitamine ning kasutamine süüteomenetlustes on oma eesmärgist tulenevalt mõõdukas sellega kaasneva eraelu puutumatuse ning isikuandmete kaitse põhiõiguse suhtes. Selle tulemusena saab sideandmete kasutamine tõendina süüteomenetluses olla lubatav ning vastavuses EL õigusega.

# USAGE OF ELECTRONIC COMMUNICATIONS DATA AS PERMISSIBLE EVIDENCE IN OFFENCE PROCEEDINGS

Abstract

In today's digital society, it is impossible to imagine effective people-to-people communication without electronic communication and the means to do so. Unfortunately, as crime progresses with the time, electronic communications have also become an integral part of the criminals' toolbox. The more communication tools are used in everyday life, the more they leave traces - electronic communications data that can be invaluable evidence in offence investigations. Communications data enable investigative authorities to map the links between individuals, to identify the timeframes of communications and, in some cases, the locations of the parties involved. Consequently, it is important to allow the use of data obtained from the communication operator (hereinafter also referred to as "communications data") in criminal and misdemeanour proceedings (named together as offence proceedings).

Communications data is defined as data generated during the provision of a communications service, relating to details of the use of the service and the form, time and manner of the message transmitted. Communications data are classified into identification data, traffic data and location data, according to the severity of the interference with fundamental rights they involve. Identification data establish the identity of end-users, or the IP address assigned to the originating user. Traffic data identify the fact of the communication session or use of the service and the related circumstances, apart from the content of the message. Location data identify the location of the communication equipment during the provision of services, the duration of the session or the sending of a request for signal strength detection.

The admissible use of communications data as evidence in offence proceedings requires a legitimate two-part regulation. National law must provide for a lawful and appropriate regime for the retention of communications data and for the use of communications data. The first component covers the collection of the communications data by the telecommunications operator and their subsequent retention, whereas the second component covers the access to the retained communications data from the telecommunications operator and their subsequent use as evidence. However, at the time of writing, the use of communications data as admissible evidence in offence proceedings has become almost impossible. This is because the European Court of Justice (and later the Supreme Court) has ruled that it is unlawful to retain traffic and location data generally and indiscriminately, as provided for in Section $111^1$ of the Electronic Communications Act, and to use such data as admissible evidence in the context of Section $90^1$

of the Code of Criminal Procedure. This showed that the regulation on the retention of communications data is incompatible with EU law.

The main objective of this thesis is to identify whether and how should national law be amended to allow the admissible use of communications data as evidence in offence proceedings. To do so, it is necessary to analyse the current regulation of the retention and use of communications data and to identify the criteria that the regulation of communications data must meet to comply with EU law, including the case law of the European Court of Justice. As a result, it will be possible to identify the conditions under which the retention and use of communications data is permissible in the context of EU law. Since the Court of Justice judgments are not only applicable to Estonia, author will also identify how other European Union Member States have brought their regulation of communications data in line with EU law. As a result, it will ultimately be possible to fit the solutions of other countries into the context of Estonian law to provide real regulatory solutions to meet the main objective of the work. In doing so, these criteria must balance the interests of offence proceedings against the interference with fundamental rights that the retention and use of communications data entails.

Based on the above, the research questions of the thesis are as follows:

1. How is the collection, retention and use of communications data as evidence in offence proceedings regulated in the Republic of Estonia?
2. What criteria, based on the case law of the European Court of Justice and the Estonian courts, must be met by the regulation for the use of communications data as admissible evidence in offence proceedings?
3. How have other EU Member States changed their regulation of communications data in the light of the case law of the European Court of Justice?
4. What regulatory changes in Estonian law would allow the retention and use of communications data as admissible evidence in offence proceedings in accordance with EU law?

The study uses qualitative and comparative research methods. The qualitative method analyses the regulation of the retention and use of communications data and the applicable criteria under EU law. By comparing Member States' laws, the author identifies solutions to align communications data regulation with EU law and allow its use as admissible evidence. Firstly, the author discusses the regulation and analyses the criteria under Estonian and EU law for the lawful retention and use of communications data as evidence. In the second chapter, the author

analyses Member States' legislation to identify how they have aligned their regulation with EU law. In the third chapter, the author seeks regulatory solutions for the Estonian regulation to ensure compliance with EU law and effective use of communications data as evidence.

The use of communications data in the Republic of Estonia is governed by the Code of Criminal Procedure (KrMS) and the Code of Misdemeanour Procedure (VTMS), linked to the Electronic Communications Act (ESS), which regulates what constitutes communications data and its collection and storage. Use in criminal proceedings is provided for in Section $90^1$ of the KrMS and Section $31^2$ of the VTMS, granting the prosecutor and out-of-court proceedings officer the right to request identification data independently, while access to other communications data requires court authorisation based on a reasoned request. Access is justified only if indispensable for achieving the purpose of proceedings. Retention for use in offence proceedings is governed by Section $111^1$ of the ESS, imposing a general and undifferentiated obligation on communication operators to retain all communications data for prosecution, security purposes, and specific administrative and civil proceedings. Operators may also retain data for commercial purposes to the extent necessary for billing, marketing, and value-added services.

The case-law of the European Court of Justice sets several criteria that the Estonian regulation must meet. National regulation must not provide for general and indiscriminate retention of traffic and location data, as prohibited by the *Digital Rights Ireland et al* and *Tele2 Sverige et al* judgments. Section $111^1$ of the ESS imposes such an obligation, making Estonian regulation incompatible with EU law. The Court stressed that communications data allow precise conclusions about private life, causing serious violations of the rights to privacy and data protection under Articles 7 and 8 of the Charter of Fundamental Rights of the EU. Retention can only be authorised to combat serious crime or protect national security. General and indiscriminate retention is only exceptionally allowed if temporary, subject to judicial or independent review, and intended to safeguard national security. Permanent general retention is permitted only at vulnerable locations such as transport hubs and buildings of national importance. Following *Ministerio Fiscal et al* and *La Quadrature du Net et al*, general retention of identification data, including necessary IP address information, is permissible.

Instead of general retention, Member States may provide for targeted retention of traffic and location data to combat serious crime or national security threats, as outlined in *Tele2 Sverige et al* and *La Quadrature du Net et al*. The Court allows temporary retention on a personal or

location basis based on objective, non-discriminatory criteria, following judicial or independent administrative review of suspected individuals linked to terrorism. Quick-freezing of specific communications data by judicially supervised authorities, like a public prosecutor's office, is permitted. In *Tele2 Sverige et al*, the Court ruled that data use is only permissible after court or independent administrative review, excluding the public prosecutor's office. Access must be strictly necessary and limited to lawfully collected and retained communications data, and only for combating serious crime or protecting national security.

Following these judgments, Member States began updating their communications data regulations to align with EU law. While many states are still revising their laws, countries like Belgium and Denmark have introduced detailed and varied retention systems. Others, like Sweden and Portugal, have limited retention to identification data, for which general and indiscriminate retention is permissible under EU law.

The Kingdom of Belgium has introduced in its law a regulation on the location-based targeted collection and retention of communications data, based on the principle that retention is allowed in areas where three or more serious crimes per 1000 inhabitants are recorded, limited to the 12 judicial regions or the police districts within them. Retention periods are 6–12 months depending on crime levels, and the obligation is set annually by the Minister of the Interior and the Minister of Justice. Belgian law also provides for retention for national security purposes in vulnerable areas such as public authority buildings, transport hubs, border areas and military sites. The Kingdom of Denmark provides for retention of communications data generated by persons convicted of serious offences for between 3 and 10 years depending on the sentence. Like Belgium, Denmark has location-based targeted retention, allowing retention within areas up to 3km² where serious crimes or convictions are 1.5 times the national average, and near highly vulnerable sites.

Following the La Quadrature du Net et al judgment, several Member States introduced quick-freeze retention rules. In Belgium, quick-freeze is authorised by the prosecutor for suspected offences punishable by at least 1 year's imprisonment, valid for 2 months with data kept for 6 months. In Denmark, the quick-freeze can obligate companies to collect data for up to 6 months (extendable) if linked to serious offences. Several Member States, such as Belgium, Denmark and Ireland, allow general and indiscriminate retention in the event of a serious threat to national security: under Belgian law, based on a national threat assessment; in Denmark, triggered by

the Minister of Justice for up to 1 year; and in Ireland, by court decision upon ministerial request, for 1 year as well.

Drawing on the criteria established by the European Court of Justice and the practical approaches adopted by Member States, it is possible to formulate regulatory proposals to align the current framework for the retention and use of communications data with EU law, thereby ensuring its admissibility as evidence in offence proceedings. Firstly, the author proposes to improve the regulation of the use of communications data by removing the specific reference to Section $111^1$ of the ESS in the procedural codes, replacing it with a general reference to the ESS. This would allow retrieval of communications data retained under the amendments proposed below. It is therefore suggested to amend Section $90^1$ Subsection 3 of the KrMS and Section $31^2$ Subsection 2 of the VTMS, enabling the investigating authority, with judicial authorisation, to request all data retained under ESS (with specific limitations to misdemeanour procedure).

Secondly, the author proposes amending Section $111^1$ Subsections 1-4 of the ESS so that service providers would only retain data in cases provided for by ESS or based on rapid retention orders under the KrMS, thereby eliminating the general and indiscriminate retention of traffic and location data. Thirdly, the author suggests introducing location-based targeted retention of traffic and location data, modelled on Denmark and Belgium. Specifically, the ESS should be supplemented to require retention of data in local government areas where the number of serious offences, as listed in Section $126^2$ Subsection 2 of KrMS, exceeds three per 1000 inhabitants, with the list of such areas updated annually by the minister responsible for the field of justice.

Furthermore, the author proposes enabling temporary rapid retention of traffic and location data during specific criminal proceedings. A new provision in the KrMS should allow the prosecutor to order a communications operator to retain data for up to six months, either for serious offences listed in Section $126^2$ Subsection 2 of KrMS, or exceptionally for other offences where justified. The retention order must specify the scope, reasons, and duration, and access to the data must comply with Section $90^1$ of the KrMS.

Given Estonia's security challenges with a potential threat revolving from Russian Federation, the author proposes new regulations for the retention of communications data for national security purposes. Specifically, the author suggests amending the ESS to allow the Government

of the Republic the right to initiate the general and indiscriminate retention of traffic and location data throughout the territory of the Republic of Estonia for up to 12 months in the event of an assessable and serious threat to the security of the Republic of Estonia that has occurred or will occur in the near future. Additionally, the author proposes allowing location-based, indiscriminate data retention near national defence sites, major transport hubs, and border zones.

The regulatory proposals put forward in the thesis will enable the regulation of the retention and use of Estonian communications data to be brought in line with EU law. If the proposals are adopted, the precise wording of the amendments may best be clarified during the legislative process and the political debate. Nevertheless, these proposals will ensure that the retention and use of communications data in offence proceedings is proportionate to its purpose and to the fundamental right to privacy and the protection of personal data that it entails. As a result, the use of communications data as evidence in offence proceedings will be admissible and in line with EU law.

# KASUTATUD ALLIKAD JA LÜHENDID

Kasutatud kirjandus:


1. Antson, A. Elektroonilise side andmete säilitamise ja põhiõiguste tagamise vahekord kriminaalmenetluses. Magistritöö. Juhendajad R. Kiris ja J. Ginter. Tartu: Tartu Ülikool 2021.
2. CUTA. *Who we are*. Veebis: https://cuta.belgium.be/who-we-are/ (14.04.2025).
3. CUTA. *What do we do*? Veebis: https://cuta.belgium.be/what-do-we-do/ (14.04.2025).
4. CUTA. *Annual report 2023*. Veebis: https://cuta.belgium.be/wp-content/uploads/2024/09/Annual-report_2023.pdf (14.04.2025).
5. Eesti Kohtud. Maakohtute jaotus kaardil. Veebis: https://www.kohus.ee/eesti-kohtud/kohtususteem/maakohtud (14.04.2025)
6. Eesti Linnade ja Valdade Liit. Elanike arv kohalike omavalitsuste kaupa. Veebis: https://www.elvl.ee/elanike-arv (14.04.2025).
7. Eurojust, *European Judicial Cybercrime Network* (EJCN). *The effect of Court of Justice of the European Union case-law on national data retention regimes and judicial cooperation in the EU*. Veebis: https://www.eurojust.europa.eu/publication/effect-court-justice-european-union-case-law-national-data-retention-regimes-judicial-cooperation (14.04.2025).
8. Europol. *European Union Terrorism Situation and Trend Report 2024*. Veebis: https://www.europol.europa.eu/cms/sites/default/files/documents/TE-SAT%202024.pdf (14.04.2025).
9. Justiits- ja Digiministeerium. Kuritegevus Eestis 2023. Veebis: https://www.justdigi.ee/kuritegevus2023/ (14.04.2025).
10. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seadus 175 SE. Seletuskiri. Veebis: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/86dde8ff-c50e-48ba-a39e-a325fe15a3f0/ (14.04.2025).
11. Kriminaalmenetluse seadustiku muutmise seadus 392 SE. Seletuskiri. Veebis: https://www.riigikogu.ee/tegevus/eelnoud/eelnou/69f4f636-076c-487f-93c2-3827044cfb50/ (14.04.2025).
12. Nahkur-Tammiksaar, D.; Uku; H. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2021. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2021/kriminaalmenetluse-statistika (14.04.2025).

13. Nahkur-Tammiksaar, D.; Uku; H. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2022. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2022/kriminaalmenetluste-statistika (14.04.2025).
14. Nahkur-Tammiksaar, D.; Pern, T; Uku; H. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2023. Veebis: https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2023/kriminaalmenetluse-statistika (14.04.2025).
15. Nahkur-Tammiksaar, D.; Zautin, V. Kriminaalmenetluse statistika. Prokuratuuri aastaraamat 2024. https://aastaraamat.prokuratuur.ee/prokuratuuri-aastaraamat-2024/kriminaalmenetluse-statistika (14.04.2025).
16. Prokuratuur. Riigi peaprokuröri kõne refereering sotsiaalvõrgustikus Facebook. Veebis: https://www.facebook.com/prokuratuur.ee/posts/pfbid03zkbszfpVokmJ6LKVYK7dEh98yKJg5HtSgirjgdR5uw7YwgM2AfaQB2gkvZnjWFEl (14.04.2025).
17. StatBel. *Total population in Belgium and the regions*, 2014-2024. Veebis: https://bestat.statbel.fgov.be/bestat/crosstable.xhtml?view=fc14c1ce-7361-4d42-a892-fce8e81a1b79 (14.04.2025).
18. Statistikaamet. Eesti rahva- ja eluruumide loendus 2021. Eesti rahvastikutihenduse interaktiivkaart. Veebis: https://storymaps.arcgis.com/stories/0c3f940a39454a5396432d666e79006e (14.04.2025).
19. Statistikaameti andmebaas. IT20: Arvuti ja koduse internetiühendusega leibkonnad. Veebis: https://andmed.stat.ee/et/stat/majandus__infotehnoloogia__infotehnoloogia-leibkonnas/IT20 (01.02.2025).
20. Statistikaameti andmebaas. RV021: Rahvastik, 1. Jaanuar. Veebis: https://andmed.stat.ee/et/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV021 (01.02.2025).
21. Statistikaameti andmebaas. RV0291U: Rahvaarv, pindala ja asustustihedus, 1. jaanuar. Veebis: https://andmed.stat.ee/et/stat/rahvastik__rahvastikunaitajad-ja-koosseis__rahvaarv-ja-rahvastiku-koosseis/RV0291U/table/tableViewLayout2 (14.04.2025).
22. Statistikaameti andmebaas. SI35: Elektroonilise side kliendid ja liinid (2011-2016). Veebis: https://andmed.stat.ee/et/stat/Lepetatud_tabelid__Majandus.%20Arhiiv__Infotehnoloogia%20ja%20side.%20Arhiiv__side/SI35 (01.02.2025).

23. Tuul, M. Kaitsepolitsei aastaraamat 2024-2025. Tallinn, 2025. Veebis. https://kapo.ee/sites/default/files/content_page_attachments/aastaraamat-2024-2025_0.pdf (23.04.2025).
24. *Udenrigsministeriet*. *Denmark and Ireland key statistics*. Veebis: https://irland.um.dk/en/about-denmark/denmark-and-ireland (14.04.2025).
25. Vahter, T. Prokuratuur sai kohtus nii valusa kaotuse, et loobus kuritegude uurimisel sideandmete kasutamisest. Eesti Ekspress 08.10.2024. https://ekspress.delfi.ee/artikkel/120327337/prokuratuur-sai-kohtus-nii-valusa-kaotuse-et-loobus-kuritegude-uurimisel-sideandmete-kasutamisest (03.02.2025).
26. Välisluureamet. Eesti rahvusvahelises julgeolekukeskkonnas 2024. Tallinn, 2024. Veebis: https://www.valisluureamet.ee/doc/raport/2024-et.pdf (23.04.2025).

Kohtulahendid:

1. EKo C 293/12 ja C 594/12, *Digital Rights Ireland et al*, ECLI:EU:C:2014:238.
2. EKo C-203/15 ja C-698/15, *Tele2 Sverige AB et al*, ECLI:EU:C:2016:970.
3. EKo C-207/16, *Ministerio Fiscal et al*, ECLI:EU:C:2018:788.
4. EKo C-511/18, C-512/18 ja C-520/18, *La Quadrature du Net et al*, ECLI:EU:C:2020:791.
5. EKo C-746/18, Prokuratuur, ECLI:EU:C:2021:152.
6. RKKKm 3-1-1-51-14 koos riigikohtunike Saale Laose ja Eerik Kergandbergi eriarvamusega.
7. RKKKo 3-1-1-93-15.
8. RKKKm 1-16-6179.
9. RKÜKo 1-17-2359.
10. TrtRnKm 1-24-1694 13.05.2024.

Eesti ja Euroopa Liidu õigusaktid:

1. Elektroonilise side seadus (ESS) - RT I, 30.12.2024, 9.
2. Euroopa Liidu põhiõiguste harta, 2016/C 202/02.
3. Inimõiguste ja põhivabaduste kaitse konventsioon - RT II 2010, 14, 54.
4. Julgeolekuasutuste seadus (JAS) - RT I, 14.03.2023, 25.
5. Kriminaalmenetluse seadustik (KrMS) - RT I, 17.04.2025, 6.
6. Riigikaitseseadus (RiKS) - RT I, 14.03.2023, 31.
7. Riigikogu 22.02.2023 otsus ”Eesti julgeolekupoliitika alused” heakskiitmine. RT III, 28.02.2023, 1.

8. Riigipiiri seadus (RiPS) - RT I, 07.06.2024, 13.
9. Väärteomenetluse seadustik (VTMS) - RT I, 17.04.2025, 12.
10. 12.07.2002 Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) - EÜT L 201, 31.07.2002, p. 37–47.
11. 15.03.2006 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, 13.04.2006.

Välisriikide õigusaktid:

1. *Arrêté ministériel portant exécution de l'article 126/3, § 1, de la loi du 13 juin 2005 relative aux communications électroniques en vue de l'adoption de la liste des arrondissements judiciaires et des zones de police soumises à l'obligation de conservation ainsi que la durée de conservation. Moniteur belge – 17.03.2025. Numéro: 2025001599*.
2. *Arrêté royal portant exécution de l'article 126/3, § 2, de la loi du 13 juin 2005 relative aux communications électroniques en vue de la confirmation du niveau de menace sur l'ensemble du territoire. Moniteur belge – 17.11.2023. Numéro: 2023047298*.
3. *Code d'instruction criminelle. Livre Premier (Art. 8 à 136ter). Moniteur belge - 27 novembre 1808. Numéro: 1808111701*.
4. *Communications (Retention of Data) Act 2011 – Number 3 of 2011. Revised Act, Updated to 1 August 2023*.
5. *Lag (2022:482) om elektronisk kommunikation - 2022-05-19, t.o.m. SFS 2024:895*.
6. *Lei n.º 32/2008, de 17 de julho, Diário da República n.º 137/2008, Série I de 2008-07-17, páginas 4454 – 4458*.
7. *Lei n.º 18/2024, de 5 de fevereiro. Diário da República n.º 25/2024, Série I de 2024-02-05, páginas 9 – 22*.
8. *Loi relative aux communications électroniques – Moniteur belge, 20.06.2005. Numéro: 2005011238*.
9. *Retsplejeloven - Lovtidende A, LBK nr 1160 af 05/11/2024*.
10. *Straffeloven – Lovtidende A, LBK no. 1145 af 05/11/2024*.

Lühendid:

1. CUTA – Belgia Kuningriigi Ohuanalüüsi Koordineerimisüksus (ingl: *Coordination Unit for Threat Analysis*).
2. EJCN – Euroopa Küberkuritegevuse Justiitskoostöövõrgustik.
3. EKo – Euroopa Kohtu üldkogu otsus.
4. EL – Euroopa Liit.
5. Eurojust - Euroopa Liidu Kriminaalõigusalase Koostöö Amet.
6. Europol - Euroopa Liidu Õiguskaitsekoostöö Amet.
7. JT – jälitustoimingud.
8. IP – Interneti-protokoll.
9. NATO - Põhja-Atlandi Lepingu Organisatsioon (Atlandi Liit).
10. RKKKm – Riigikohtu kriminaalkolleegiumi määrus.
11. RKKKo – Riigikohtu kriminaalkolleegiumi otsus.
12. RKÜKo – Riigikohtu üldkogu otsus.
13. TrtRnKm – Tartu Ringkonnakohtu määrus.
14. UK - Suurbritannia ja Põhja-Iiri Ühendkuningriik.