TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
AVALIKU ÕIGUSE OSAKOND

Piret Schasmin

PRIVAATSUSÕIGUSE PIIRAMISE ÕIGUSLIK RAAMISTIK EUROOPA INIMÕIGUSTE KOHTU NING EUROOPA KOHTU LAHENDITE ALUSEL

Magistritöö

Juhendaja:
PhD Carri Ginter

Tallinn
2016

SISUKORD

SISSEJUHATUS

Infotehnoloogia kiire areng ning vajadus võidelda terrorismiga on toonud kaasa olukorra, kus inimeste eraellu tungitakse rohkem kui kunagi varem.[1] Olemasolev tehnoloogia võimaldab nii erasektori ettevõtetel kui ka riigil koguda, säilitada ja analüüsida suurtes kogustes personaalset informatsiooni väga paljude üksikisikute kohta. Võib tunduda, et see on viinud ühiskonna täiesti uue reaalsuseni, kus on muutunud privaatsuse tähtsus kui ka privaatsuse tähendus. Endine Sun Microsystems juht Scott McNealy ütles juba ligi 15 aastat tagasi, et „teil ei ole nagunii mittemingisugust privaatsust … saage üle sellest“ (inglise keeles „*You have zero privacy anyway … get over it*“).[2] Facebooki looja Mark Zuckerberg[3] on seevastu selgitanud, et privaatsus kui sotsiaalne norm on arenenud ja muutunud, sest inimesed ei hooli enam privaatsusest.

Kogu maailma vapustanud 9/11, terroriaktid Madridis 2004. aastal ja Londonis 2005. aastal andsid tõuke riikide valitsustele kasutada järjest enam olemasolevaid tehnoloogilisi vahendeid terroristide tabamiseks. Madridi ja Londoni terroriaktid andsid Euroopa Liidu tasemel tõuke elektroonilise side andmete kogumise ja säilitamise regulatsiooni kehtestamiseks.[4] Selle regulatsiooni alusel anti 2013. aastal ainuüksi Ühendkuningriikides välja 514 608 luba kommunikatsiooniandmete väljastamiseks, millele lisandusid 42 293 suuliselt tehtud päringut eriti kiireloomulisteks juhtumiteks.[5]

Oluline roll jälgimisprobleemi olemasolu tunnustamisel ning privaatsusküsimustega tegelemiseks oli Edward Snowdeni paljastustel NSA ülisalajase jälgimisprogrammi PRISM kohta. PRISM programmi eesmärgiks oli koguda internetist suures hulgas isiklikke andmeid, näiteks interneti otsinguajaloo, e-kirjade sisu, failide edastamise ning *online* vestluste kohta,

[1] N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick. „An overview of emerging challenges in privacy law. in Emerging Challenges in Privacy Law. Comparative perspectives. Edited by N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick. Cambridge: University Press 2014, k 1-2.

[2] P. Sprenger. Sun On Privacy: 'Get Over It'. Wired Magazine. 26.01.1999. – http://archive.wired.com/politics/law/news/1999/01/17538 (27.03.2016)

[3] T. Bardley. Zuckerberg Comments Underscore Conflict Between Social Networking And Privacy. PCWorld. 11.01.2010. – http://www.pcworld.com/article/186651/zuckerberg_comments_underscore_conflict_between_social_networking_and_privacy.html (27.03.2016)

[4] Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. – http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52005PC0438&from=ET (16.04.2016), lk 2.

[5] 2013 Annual Report of the Interception of Communications Commissioner. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302597/InterceptionCommunicationsCommissionerPrint.pdf (27.04.2016), lk 22.

kasutades sealjuures mitmete suurettevõtete abi, nagu Facebook, Google, Apple, Microsoft ja teised suurettevõtted.[6] Snowdeni lekitatud andmed tõid ilmsiks ka samalaadse jälgimisprogrammi Tempora, mida kasutas andmete kogumiseks Ühendkuningriikide luureteenistus.[7] Need paljastused on tekitanud mitmeid diskussioone selle üle, kas jälgimisühiskond on tänapäeval paratamatu.[8] Ühiskonnas on riigi jälgimistegevuse osas paraku väga levinud seisukohaks, et kui sul ei ole midagi varjata, siis ei ole sul ka midagi karta, mistõttu alahinnatakse sageli inimeste õigust privaatsusele.[9] Teaduskirjanduses on seevastu vägagi selgelt toodud esile, et privaatsusõigusesse sekkumine või privaatsuse kadumine on lääne demokraatiatele väga suureks ohuks. „Indiviidi privaatsuse põhiaspektide kadumine võib fundamentaalselt muuta inimkäitumist ning suhtlemist, meie enda arusaama isiklikust vabadusest ning demokraatlike ühiskondade eetosest".[10] Seetõttu on põhjust tunda muret privaatsusõiguse säilimise üle.

Edward Snowdeni paljastustega kaasnenud reaktsioon, sealhulgas kodanike massilise jälgimise taunimine nii erinevate suurettevõtete kui ka riigijuhtide poolt[11], võis anda lootust, et riiklike julgeoleku huvide kõrval pööratakse suuremat tähelepanu ka inimeste privaatsuse austamisele. Ka Euroopa Kohtu poolt elektroonilise andmeside direktiivi 2006/24/EÜ[12] kehtetuks tunnistamine 2014. aastal[13] põhjusel, et direktiivis sätestatud kohustus koguda massiliselt isikute kohta meta-andmeid riivab ebaproportsionaalselt isikute privaatsust, andis märku sellest, et inimeste privaatsuse kui põhiõiguse tagamine on jätkuvalt ühiskonnas oluline. Samas näitavad viimase aasta sündmused, eelkõige 2015. a novembris toimunud terroriaktid Pariisis ning 2016. a märtsis toimunud terroriaktid Brüsselis, et Euroopa riikide valitsuste üheks suurimaks väljakutseks on jätkuvalt võitlus terrorismiga, mis seab järjest suurema surve üksikisikute privaatsusele.[14]

---

[6] G. Greenwald, E. MacAskill. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. – http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (09.04.2016).
[7] S. Stalla-Bourdillon, J. Phillips, M. D. Ryan. Privacy vs. Security. Springer London 2014. lk 4.
[8] Nt M. N. Richards. The Dangers of Surveillance. – Harvard Law Review, 2013.
[9] S. Stalla-Bourdillon, lk 72.
[10] K. Lachmayer, N. Witzleb. The challenge to privacy from ever increasing state surveillance: a comparative perspective. - UNSW Law Journal. 2014/37(2), lk 749.
[11] J. Vasagar. Germany 'not a surveillance state', says Angela Merkel. The Telegraph. 19.07.2013. – http://www.telegraph.co.uk/news/worldnews/europe/germany/10190946/Germany-not-a-surveillance-state-says-Angela-Merkel.html (09.04.2016).
[12] Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. – ELT L 105, 13.04.2006, lk 54–63.
[13] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs Ireland.*
[14] Vt P. Luts. Koort: Euroopa peab üle vaatama tabud andmekogumise osas. ERR. 22.03.2016. – http://uudised.err.ee/v/eesti/a145d905-c876-4f4c-bff1-ac99aecd8a65/koort-euroopa-peab-ule-vaatama-tabud-andmekogumise-osas (09.04.2016).

Eelnevast tulenevalt on ühiskonnas probleemiks see, et terrorismiohuga võitlemine nõuab riikide valitsustelt järjest rohkem ennetavate meetmete kasutamisele võtmist, mis tähendab aga seda, et valitsustel on järjest suurem vajadus jälgida ühiskonna liikmete tegevust. See tähendab aga seda, et üksikute terroristide tabamiseks soovitakse koguda ja säilitada andmeid valimatult kõigi isikute kohta, mistõttu on ka sekkumine privaatsusesse järjest suurem. Sõltumata sellest, et käesoleval hetkel ei ole Eesti territooriumil otsest ohtu terrorirünnakuteks, on see teema aktuaalne ka Eesti tasandil. Eesti riik on võtnud ning plaanib võtta kasutusele meetmeid, mis võimaldavad isikute massilist jälgimist ning mille üheks eesmärgiks on terrorismi ja muude kuritegude ennetamine.

Esimene meede neist on elektroonilise andmeside andmete säilitamine. Kuigi juba 2014. aastal tunnistati Euroopa Kohtu poolt kehtetuks elektroonilise andmeside direktiiv, on Eesti endiselt nende riikide hulgas, kus kaks aastat pärast Euroopa Kohtu otsust kehtivad need riigisisesed sätted, mis võtavad üle kehtetuks tunnistatud direktiivi ning mis ei vasta Euroopa Kohtu otsuse alusel proportsionaalsuse põhimõttele.[15] Sellele probleemile on viidanud U. Lõhmus 2015. aastal ilmunud Juridica artiklis[16], milles õhutas ühtlasi arutelu selle üle, kui kaugele võib riik kodanike jälgimisega minna ning kas Eesti olustik nõuab vähemat tähelepanu isiku eraelu puutumatuse õigusele kui teistes Euroopa Liidu liikmesriikides.

Elektroonilise andeside meta-andmete säilitamine ei ole ainuke meede, mille puhul tekib küsimus inimeste privaatsusest. 2016. aasta 1. jaanuaril jõustusid riigipiiri seaduse muudatused[17], millega peavad kõik lennuettevõtjad edastama andmed Politsei- ja Piirivalveametile Eestisse saabuvate ja Eestist lahkuvate lennureisijate broneeringuinfo kohta ning neid andmeid hakatakse säilitama Politsei- ja Piirivalveameti hallatavas broneeringuinfo andmekogus. Lisaks sellele on Siseministeeriumil plaanis hakata automaatselt koguma informatsiooni ka kõigi hotellikülastajate kohta.[18] Liiklusohutuse tagamiseks on juba mitmeid aastaid kaalutud lõigu keskmise kiiruse mõõtmisel põhinevaid automaatseid järelevalvesüsteeme. Sellise järelevalvesüsteemi puhul fikseeritakse vastavate andurite abil

[15] U. Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. – Juridica 2015/X, lk 735.
[16] *Ibid*, lk 741.
[17] RT I, 31.12.2015, 27.
[18] Politsei hakkab ilmselt saama reaalajas kõigi hotellikülastajate andmeid. ERR. – http://uudised.err.ee/v/f1e44719-8eeb-4dc6-9972-6df87419c230/politsei-hakkab-ilmselt-saama-reaalajas-koigi-hotellikulastajate-andmeid (09.04.2016)

kõikide sõidukite sisenemisaeg teelõigule ja väljumisaeg teelõigult ning tuvastatakse kaamerate abil automaatselt kõikide sõidukite registreerimisnumbrid.[19]

Need on mõned näited, kus julgeoleku või avaliku korra kaitseks Eesti riik kogub või plaanib koguda isikuandmeid automaatselt paljude isikute kohta, sõltumata sellest, kas seda isikut kahtlustatakse mõne karistatava teo toimepanemises või mitte. Kuivõrd nende meetmetega on võimalik koguda andmeid meie kõigi kohta, tekib küsimus, kas selline massiline inimeste privaatsusesse tungimine on ikka hädavajalik.

Eelnevast tulenevalt on käesoleva töö eesmärgiks välja selgitada, milline on privaatsusõiguse piiramise õiguslik raamistik ning milliseid aspekte tuleks riigipoolse jälgimise meetmete kehtestamisel arvesse võtta. Teisisõnu soovitakse käesoleva tööga välja selgitada, kuidas peaks toimuma riigipoolse jälgimistegevuse kui privaatsusõiguse riive proportsionaalsuse hindamine, et saavutada tasakaalu privaatsusõiguse ja julgeoleku huvide vahel. Töö autor püstitab töös kaks hüpoteesi. Esiteks, inimeste privaatsusesse sekkumine selliste meetmetega, mis lubavad automaatselt paljude isikute kohta andmete kogumist, on lubatud üksnes väga rangetel ning erandlikel tingimustel. Teiseks, Eestis toimuv elektroonilise side andmete lauskogumine väljub lubatud julgeoleku eesmärkide raamidest, mis ei vasta Euroopa Kohtu ja Euroopa Inimõiguste Kohtu rangetele ning erandlikele tingimustele. Lähtuvalt töö eesmärgist ja hüpoteesist püstitatakse järgmised üürimisküsimused:

1) Milline tähendus on privaatsusel ning milliseid tagajärgi võib tuua kaasa liigne privaatsusesse sekkumine?
2) Millistel juhtudel on privaatsusõigusesse sekkumine lubatud?
3) Kuidas on Euroopa Kohus ja Euroopa Inimõiguste Kohus hinnanud jälgimise kui privaatsusõiguse riive proportsionaalsust?
4) Kuidas vastab Eesti elektroonilise side andmete regulatsioon Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktika tingimustele?

Käesolevas magistritöös kasutatakse töös püstitatud küsimustele vastamiseks analüütilist ja võrdlevat meetodit. Magistritöö peamisteks allikateks on võõrkeelsed teaduslikud allikad ning Euroopa Inimõiguste Kohtu ja Euroopa Kohtu lahendid. Lisaks on kasutatud ka eestikeelset õiguskirjandust, Riigikohtu praktikat, erinevaid õigusanalüüse ning õigusakte. Privaatsusõiguse teemal on kirjutatud pigem vähe ning siiani Eestis kirjutatud teadustööd ei ole käsitlenud

[19] Keskmise kiiruse mõõtmisel põhineva automaatse liiklusjärelevalve kasutamise uuring. 2013. – http://www.mnt.ee/public/ASSC_lopparuanne_v_final.pdf (09.04.2016)

põhjalikumalt privaatsusõiguse teemat riigi jälgimise ning julgeoleku vaatenurgast.[20] Privaatsusõigusega seotud tööd on keskendunud pigem eraelu puutumatusele üldiselt[21] või kitsamalt isikuandmete kaitsele[22] või töötaja privaatsusõigusele[23].

Käesolev magistritöö koosneb kolmest peatükist. Esimeses peatükis analüüsitakse privaatsusõiguse kujunemist, privaatsusõiguse sisu ja selle erinevaid elemente. Sealjuures käsitletakse privaatsusõiguse olulisust ning milliseid ohte sisaldab inimeste privaatsusesse sekkumine ja riigipoolne jälgimistegevus. Töö teises peatükis tutvustatakse peamiseid põhjuseid, millal on eraellu sekkumine põhjendatud ning millistel tingimustel on see lubatud. Suuremat tähelepanu pööratakse sellele, kuidas on Euroopa Kohus ja Euroopa Inimõiguste Kohus hinnanud riikliku jälgimise ja andmete kogumise kui privaatsusõiguse riivete proportsionaalsust. Selles peatükis tuuakse esile, milliseid teste on kohtud kasutanud ning millistest kaalutlustest lähtuvalt on kohtud üht või teist riivet õigustatuks pidanud. Töö kolmandas osas analüüsitakse Eestis kehtiva elektroonilise side andmete säilitamise ja kasutamise regulatsiooni vastavust Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikale.

Magistritöös esitatud tulemused saab võtta aluseks olemasolevate regulatsioonide täiendamiseks ning uute regulatsioonide väljatöötamiseks, mis puudutavad inimeste jälgimist ning isikute kohta andmete kogumist ja jagamist riigiasutustega.

[20] Erinevates uurimistöödes on käsitletud jälitustoiminguid kriminaalmenetluse vaatenurgast, kuid käesoleva töö temaatika on laiem kui kitsalt jälitustoimingute lubatavus kriminaalmenetluses.

[21] K. Lõhmus-Ein. Eraelu ja selle elementide õiguslik kaitsmine. Magistritöö. Tartu: Tartu Ülikool 2004.

[22] M. Küngas. Traditsiooniliste õiguskaitsevahendite rakendatavus isikuandmete kaitse õiguse tagamisel infoühiskonnas ja nende võimalikest arengutest. Magistritöö. Tallinn: Tartu Ülikool 2015. S. Sillaots. Isikuandmete kaitse regulatsiooni ühtlustamine isikuandmete kaitse üldmääruse eelnõus ja selle mõju Eestile. Magistritöö. Tartu: Tartu Ülikool 2014. R. Oorn. Infoühiskond ja selle erinevad aspektid riigihalduses ja andmekaitses. Magistritöö. Tartu: Tartu Ülikool 2007. E. Tikk. Informatsioonilise enesemääratlemise rahvusvahelis-õiguslik raamistik, sisustamine Eesti õiguses ja selle praktilisest kohaldamisest veebikeskkonnas. Magistritöö. Tartu: Tartu Ülikool 2004.

[23] M. Peeterson. Töötaja privaatsusõigus ja selle piiramine töösuhetes. Magistritöö. Tallinn: Tartu Ülikool 2012.

1. PRIVAATSUSÕIGUSE ÕIGUSLIK RAAMISTIK

1.1. Privaatsusõiguse kujunemine

Privaatsuse tunnustamine ühiskonnas leidis aset oluliselt varem, kui toimus selle tunnustamine ja kaitsmine õigushüvena.[24] Juba varasemalt kaitsesid erinevad normid isikute kodu, asju, samuti isiku puutumatust[25] ning seda kaitsti eelkõige füüsiliste tõkete, samuti moraalsete väärtushinnangutega.[26] Õigushüvena kerkis see esile eelkõige demokraatia arenguga, kui hakati tunnistama indiviidi õiguseid ja vabadusi.[27] Privaatsusõigus kaitses algselt üksnes teatud aspekte nagu kodu puutumatust, sõnumisaladust ning keha puutumatust.[28]

Esimesena tunnustati privaatsusõigust USAs 19. sajandi lõpus, kui advokaadid Warren ja Brandeis kirjutasid õigusest olla üksi jäetud (inglise keeles „*right to be left alone"*) seoses ajakirjanduse tungimisega isikute eraellu.[29] Kuigi USA on mõjutanud üldiselt põhiõiguste arengut Euroopas, on privaatsusõigus arenenud Euroopas siiski suhteliselt autonoomselt.[30] Privaatsusõiguse kujunemine toimus võrreldes teiste põhiõiguste arenguga mõneti erinevalt. Rahvusvaheliselt tunnustatud inimõiguste areng on tavaliselt saanud alguse esmalt riikide tasandil ning seejärel on need tunnustatuse saanud rahvusvahelisel tasandil.[31] Privaatsusõiguse areng toimus sellele vastupidiselt, sest kõige pealt tunnustati privaatsusõigust inimõigusena rahvusvahelisel tasandil ning alles seejärel tunnustati privaatsusõigust põhiseaduse tasandil laiemalt ka erinevates riikides.[32]

Tõuke privaatsusõiguse ning ka teiste inimõiguste reglementeerimiseks rahvusvahelisel tasandil tõid kaasa II maailmasõja sündmused.[33] Privaatsusõiguse kujunemisel mängis II maailmasõja sündmustest enim rolli see, et genotsiidi läbiviimiseks kasutati suuri andmeregistreid, mis tõi esile selle, milliseid tulemusi võib kaasa tuua avalikkuse tungimine inimese privaatsfääri.[34] Sellest tulenevalt sisustati privaatsusõigus kui inimõigus esimesena

[24] M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011, lk 13.
[25] J. Holvast. History of Privacy. Springer Berlin Heidelberg 2008, lk 13.
[26] M. Männiko, lk 13.
[27] M. Männikp, lk 13.
[28] J. Holvast, lk 15. O. Diggelmann and M. N. Cleis. How the Right to Privacy Became a Human Right. – Human Rights Law Review, 2014/14. Lk 441.
[29] D. Warren, L. Brandeis. The right to privacy. – Harvard Law Review, 1890/1891/4, 193.
[30] S. Stalla-Bourdillon, lk 6.
[31] O. Diggelmann, M. N. Cleis, lk 442.
[32] *Ibid*, lk 441.
[33] M. Männiko, lk 15.
[34] J. C. Buitelaar. Privacy: Back to the Roots. − German Law Journal 2012/13, No 3, lk 174.

inimõiguste ülddeklaratsioonis (*Universal Declaration of Human Rights*) 1948. aastal. Inimõiguste ülddeklaratsiooni artikkel 12[35] sätestas privaatsusõiguse järgmiselt:

> „*Kellegi isiklikku ja perekonnaellu ei või meelevaldselt vahele segada, kellegi korteripuutumatust, kirjavahetuse saladust või au ja reputatsiooni ei tohi meelevaldselt määrida. Igal inimesel on õigus seaduse kaitsele selliste vahelesegamiste ja rikkumiste eest.*“

Aja jooksul on vastu võetud ka rida teisi rahvusvahelisi instrumente, mis annavad võrreldes Inimõiguste deklaratsiooniga privaatsusõigusele väga sarnase kaitse. 1950. aastal võeti vastu Euroopa inimõiguste ja põhivabaduste kaitse konventsioon (EIÕK)[36], mis jõustus 1953. aastal. Selle artikkel 8 sätestab õiguse privaatsusele järgmiselt:

> „*1. Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu ja kodu ning sõnumite saladust.*
> *2. Ametivõimud ei sekku selle õiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks.*“.

Võrreldes inimõiguste ülddeklaratsiooni ja Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni sõnastust, sh inglisekeelset sõnastust, siis nende sisu on võrdlemisi sarnane. Terminoloogilisest küljest vaadatuna kasutatakse inimõiguste ülddeklaratsioonis terminit „privaatsus“ (inglise keeles *privacy*)[37] ning Euroopa inimõiguste ja põhivabaduste kaitse konventsioonis terminit „eraelu“ (inglise keeles *private life*)[38], mida kasutatakse ka käesolevas töös sünonüümidena.[39]

---

[35] Inimõiguste ülddeklaratsioon. Eestikeelne tõlge. – http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/est.pdf (16.04.2016)
[36] Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.
[37] Inimõiguste ülddeklaratsiooni artikkel 12: *No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks*.
[38] EIÕK artikkel 8: *Everyone has the right to respect for his private and family life, his home and his correspondence*.
[39] Privaatsust ning eraelu on sünonüümidena käsitletud ka Eesti Vabariigi põhiseaduse komm väljaandes (R. Maruste. PõhiS § 18/14 – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012).

1966. aastal võttis ÜRO peaassamblee vastu Kodaniku- ja poliitiliste õiguste rahvusvaheline pakti (ICCPR), mis sätestas samuti õiguse privaatsusele. Selle artikkel 17 sõnastus on peaaegu identne inimõiguste deklaratsiooni artikliga 12.[40]

Isiku eraelu kaitsega on otseselt seotud ka 1981. aastal Euroopa Nõukogu poolt vastu võetud isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni (nr 108).[41] Selle konventsiooni eesmärgiks on tagada isiku eraelu kaitse olukorras, kus toimub isikuandmete automatiseeritud töötlemine.[42] Tegemist on ühe esimese ning olulisema aktiga, mis keskendub eraldi isikuandmete kaitsele. Sealjuures näeb see konventsioon ette õiguskaitsevahendid, kui isiku taotlust tema kohta käivate andmete kinnituse, edastamise, parandamise või kustutamise kohta ei ole rahuldatud.[43]

Privaatsusõiguse sisustamisel on olnud väga oluline roll Euroopa Inimõiguste Kohtul (EIK), kes on EIÕK artiklit 8 tõlgendanud dünaamiliselt ning andnud privaatsusõigusele aja jooksul tähenduse, mida sellel algselt ei olnud.[44] EIÕK on olnud seega elav instrument.[45] Kuigi privaatsusõigust tunnustati inimõigusena juba 20. sajandi keskpaigas, toimus selle võidukäik 20. sajandi lõpus ning seda seoses informatsioonitehnoloogia ning elektroonilise meedia arenguga.[46] Ka Euroopa Inimõiguste Kohus on võtnud arvesse tehnoloogilisi arenguid ning sisustanud privaatsusõigust sellest lähtuvalt. Seda, kuidas EIK on EIK artiklit 8 sisustanud, tutvustatakse käesoleva peatüki punktis 1.3. Järgnevalt tutvustatakse, kuidas on privaatsusõigus reguleeritud Euroopa Liidu ning Eesti õiguses.

1.2. Privaatsusõigus Euroopa Liidu ning Eesti õiguses

Kuigi Euroopa Liit ei ole EIÕK-ga õiguslikult seotud, on Euroopa Kohus võtnud EIÕK sätteid eeskujuks EL õiguse põhiprintsiipide kujundamisel, mis on tingitud eelkõige sellest, et kõik EL

[40] Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (mitteametlik tõlge). – https://www.riigiteataja.ee/akt/23982 (27.03.2016).
[41] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3. – https://www.riigiteataja.ee/akt/78300 (14.04.2016)
[42] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni preambula ja artikkel 1.
[43] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni artikkel 8.
[44] L. Wildhaber, O. Diggelmann. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica I/2007. M. Männiko, lk 18.
[45] G. Letsas. The ECHR as a living instrument: its meaning and legitimacy. In Constituting Europe. The European Court of Human Rights in a National, European and Global Context. Edited by A. Follesdal, B. Peters, G. Ulfstein Cambridge University Press: Cambridge. 2013, lk 109-111.
[46] O. Diggelmann, M. N. Cleis, lk 442.

liikmesriigid on ratifitseerinud EIÕK. [47] Inimõigused on Euroopa Liidu aluslepingute osaks olnud alates aastast 2009, kui Euroopa Liidu põhiõiguste harta[48] (mis kuulutati välja juba 2000. aastal) muutus õiguslikult siduvaks kõikide liikmesriikide suhtes. Harta artikkel 7 sätestab privaatsuse kaitse järgmiselt:

> „*Igaühel on õigus sellele, et austataks tema era- ja perekonnaelu, kodu ja edastatavate sõnumite saladust*."

Lisaks artiklile 7 sätestatakse harta artiklis 8 eraldi õigus isikuandmete kaitsele:

> *„1. Igaühel on õigus oma isikuandmete kaitsele.*
>
> *2. Selliseid andmeid tuleb töödelda asjakohaselt ning kindlaksmääratud eesmärkidel ja asjaomase isiku nõusolekul või muul seaduses ettenähtud õiguslikul alusel. Igaühel on õigus tutvuda tema kohta kogutud andmetega ja nõuda nende parandamist.*
>
> *3. Nende sätete täitmist kontrollib sõltumatu asutus."*

Sõltumata Euroopa Liidu põhiõiguste harta olemasolust, on EIÕK siiski jätkuvalt inimõiguste kaitse aluseks Euroopa Liidus, mis tagab nö miinimum standardi kõigi õiguste jaoks.[49] Euroopa Liidu põhiõiguste harta artikkel 52 lg 3 sätestab muuhulgas, et „Hartas sisalduvate selliste õiguste tähendus ja ulatus, mis vastavad Euroopa inimõiguste ja põhivabaduse kaitse konventsiooniga tagatud õigustele, on samad, mis neile nimetatud konventsiooniga ette on nähtud. See säte ei takista liidu õiguses ulatuslikuma kaitse kehtestamist.". See säte ei ole oluline mitte üksnes inimõiguste tõlgendamise jaoks, vaid see määrab ka Euroopa Kohtu ning Euroopa Inimõiguste kohtu pädevuse.[50]

Eesti põhiseaduses on privaatsusõigus, nagu see on sätestatud EIÕK-s, kaitstud erinevates paragrahvides sätestatud õigustega.[51] Seega ei leia põhiseadusest eraelu kaitse kohta samasugust sõnastust, nagu see on sätestatud EIÕK-s või inimõiguste ülddeklaratsioonis. Perekonna- ja eraelu puutumatust kaitseb põhiseaduse § 26, au ja head nime kaitseb § 18, kodu puutumatust kaitseb § 33 ning sõnumite saladust kaitseb § 43. Perekonna- ja eraelu teatud

[47] U. Fink. Protection of privacy in the EU, individual rights and legal instruments. in Emerging Challenges in Privacy Law. Comparative perspectives. Edited by N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick. Lk 75.

[48] Euroopa Liidu põhiõiguste harta. – ELT C 326, 26.10.2012. – http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A12012P%2FTXT (09.04.2016)

[49] U. Fink, lk 75.

[50] *Ibid.* lk 75-76.

[51] K. Jaanimägi. PõhiS § 26/3 – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012.

küljed võivad kuuluda ka PS §-des 27 ja 42 (võimuorganite keeld koguda andmeid isiku veendumuste kohta), samuti § 44 lõikes 2 (informatsiooni andmine isiku tegevuse kohta) sõnastatud põhiõiguste kaitsealasse.[52] PS § 26 näol on tegemist üldsättega, mida tuleb kohaldada juhul, kui kaitsmist vajav erasfääri kuuluv hüve ei ole põhiseaduses kaitstud mõne erisättega.[53]

Lisaks eelnevatele on Eesti põhiseaduses olemas veelgi üldisem säte, mis võib rolli mängida eraelu kaitsmisel.[54] Selleks sätteks on PS § 19, mis tagab üldise vabaduspõhiõiguse. Üldine vabaduspõhiõigus (üldine isiksuspõhiõigus) kaitseb üldist enesemääramise- ja enesekujutamise õigust, mis kuulub EIÕK-s selle artikli 8 eraelu puutumatuse kaitsealasse.[55] Üldise isikuõiguse kaitseesemeks on üksnes säärased isiksuse vaba eneseteostuse kui inimväärikuse väljenduse tingimused, mida teised, eelnevalt nimetatud põhiõigused ei kaitse.[56]

Lähtuvalt Eesti Vabariigi põhiseadusest ning väljakujunenud kohtupraktikast, tuleb põhiõiguste tõlgendamisel lähtuda nii Euroopa inimõiguste konventsioonist kui ka Euroopa Liidu põhiõiguste hartast.[57] Järgnevalt tutvustaksegi seda, kuidas on privaatsusõigust sisustatud, milles on oluline roll Euroopa inimõiguste konventsioonil ning Euroopa Inimõiguste Kohtul.

1.3. Privaatsusõiguse tähendus ja selle elemendid

Privaatsusõigusele ei ole ühtset kindlat definitsiooni, vaatamata mitmetele püüdlustele seda formuleerida.[58] 19. sajandi lõpus määratlesid USA advokaadid Warren ja Brandeis privaatsuse kui õiguse olla üksi jäetud (inglise keeles „*right to be left alone*“).[59] See on aga üksnes üks tahk privaatsusest.[60] Üldisemalt võib privaatsuseks pidada isiku eraelulist sfääri, milles isikul on õigus otsustada, kas ja kui palju ta oma eraelu teiste inimeste, avalikkuse ja/või riigiga jagab.[61] Eraelu ehk privaatsust on sisustatud selliselt, see on igaühe õigus enesemääratlemisele ning

[52] *Ibid.*
[53] *Ibid.*
[54] *Ibid* § 26/4.
[55] *Ibid.*
[56] R. Alexy. Põhiõigused Eesti põhiseaduses. – Juridica eriväljaanne 2001, lk 50.
[57] M. Ernits. PõhiS II peatükk, sissejuhatus/1.3, 1.4. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012.
[58] O. Diggelmann, M. N. Cleis, k 442. U. Fink, lk 77.
[59] D. Warren, L. Brandeis, lk 193.
[60] U. Fink lk 77.
[61] M. Männiko, lk 18.

õigus elada oma soovide ja tahtmiste kohaselt minimaalse välise sekkumisega.[62] Sealjuures on märgitud, et see õigus hõlmab lisaks õigust kontrollida enda kohta käiva informatsiooni liikumist iseenda ja avaliku võimu vahel ning olla efektiivselt kaitstud eraellu põhjendamatute sekkumiste eest.[63]

Kuigi eraelu või privaatsust seostatakse sageli inimese intiimse sfääriga, on see tegelikkuses oluliselt laiem.[64] EIK on leidnud, et „Oleks ilmselt liialt kitsendav siduda eraelu mõiste „sisemise ringiga", milles isik võib elada oma elu, nagu ta soovib, ja välistada sealt täielikult välismaailm, mida sisemine ring ei hõlma. Eraelu austamine peab sisaldama ka teatud määral õigust luua ja arendada sidemeid teiste inimestega."[65] Seega hõlmab eraelu suhteid teiste inimestega, mis ei piirdu üksnes suhetega kõige lähedasemate isikutega.

Mida privaatsusõigus on konkreetsemalt endas sisaldab, eelnevatest määratlustest ei selgu. Selleks tuuakse järgnevalt välja privaatsuse erinevad elemendid, mis tulenevad EIK kohtupraktikast tõlgendades EIÕK artiklit 8, mis kaitseb nelja olulist valdkonda: eraelu, perekonnaelu, kodupuutumatust ning kirjavahetuse saladust. Enne nende elementide väljatoomist on oluline märkida, et õigus privaatsuse austamisele hõlmab endas nii negatiivset kui ka positiivset kohutust.[66] Negatiivne kohustus tähendab seda, et riigil on kohustus mitte sekkuda isiku eraellu, sest EIÕK on suunatud eelkõige riigivõimu (valitsuse, politsei ja teiste riigiorganite) tegevuse piiramiseks.[67] Positiivne kohustus tähendab aga seda, et riik peab omalt poolt tagama, et isiku eraelu oleks kaitstud teiste isikute sekkumise eest.[68]

Enne kui minna erinevate elementide juurde, on oluline välja tuua, et privaatsusõiguse sisustamisel esineb nö kaks omavahel võistlevat põhiideede gruppi: 1) privaatsus kui vabadus ühiskonnast – õigus olla üksi jäetud, enda ja ühiskonna vahele distantsi jätmine; 2) privaatsus kui väärikus – elementaarsete ühiskonna normide austamine, mis puudutavad nt intiimsuhteid, reputatsiooni jne.[69] Need ideede grupid selgitavad, miks privaatsus on inimestele oluline. Privaatsus on esiteks vabaduse garantiiks ning teiseks, see aitab tagada inimeste väärkust. Mõlemad on demokraatliku ning liberaalse ühiskonna alustaladeks. Privaatsuse tagamiseks on

[62] R. Maruste. Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse. Tallinn: Juura 2004, lk 429.
[63] *Ibid*.
[64] U. Fink, lk 77.
[65] EIKo 16.12.1992, 13710/88, *Niemietz vs Germany*, p 29.
[66] S. Stalla-Bourdillon, lk 12.
[67] U. Fink, lk 89.
[68] S. Stalla-Bourdillon, lk 12. EIKo 12.06.2003, 35968/97, *Van Kück vs Germany*, p 70.
[69] O. Diggelmann, M. N. Cleis, lk 442.

S. Stalla-Bourdillon, J. Phillips ja M. D. Ryani hinnangul kaks eeldust: õigus eraelu salajasusele ning õigus eraelu vabadusele.[70] Seega on vabadus ühtlasi privaatsuse eelduseks kui ka privaatsuse tulemuseks.

Järgnevalt käsitletakse privaatsusõiguse järgmiseid elemente: füüsiline ja vaimne terviklikkus, informatsiooni kogumine ja avalikustamine, elukeskkond, identiteet ning autonoomia.

1) Füüsiline ja vaimne terviklikkus

Õigus kehalisele ja vaimsele terviklikkusele hõlmab õigust olla kaitstud kehaliste rünnete ja paljastuste eest, samuti soovimatu jälgimise eest, tungimise eest koju ja töökohta ning enda kujutiste jagamise eest.[71] EIK on märkinud, et inimese keha moodustab ühe kõige intiimsema osa inimese eraelust.[72] Lisaks füüsiliste rünnakute eest kaitseb artikkel 8 isikuid riigivõimu eest ka alandamise eest selles osas, mis ei kuulu artikli 3 kaitsealasse.[73] Inimese terviklikkus hõlmab ka inimese eksisteerimise abstraktsemaid elemente, nagu eneseväärikus, autonoomsus, tunded, mõtted ja arusaam moraalsusest.[74] Füüsilist ja vaimset terviklikkust võivad riivata näiteks tahtevastane meditsiiniline läbivaatus või ravi[75], vereproovi võtmine[76], sundravile saatmine[77], lapsele ravi määramisel seadusliku esindaja huvidega arvestamata jätmine[78] ning isikute läbiotsimine või läbivaatus vanglates või kriminaalmenetluse raames[79]. Selles tulenevalt tuleb inimene läbi vaadata või läbiotsida viisil, mis tagab inimese inimväärikuse, nt inimest võib läbi otsida üksnes samast soost isik.[80] Isiku füüsilist intiimsust tuleks kaitsta ka alasti keha sunnitud näitamise eest.[81]

Lisaks nn negatiivsele kohustusele hoiduda isiku eraellu sekkumisest, on riigil ka positiivne kohustus kaitsta isikuid teiste isikute vägivalla eest.[82] Riigipoolseks rikkumiseks on loetud

[70] S. Stalla-Bourdillon, lk 8.
[71] N. A. Moreham. The right to respect for private life in the European convention on human rights: a re-examination. – European Human Rights Law Review. 2008/1, lk. 49.
[72] EIKo 22.07.2003, 24209/94, *Y.F. vs Turkey*, p 33.
[73] N. A. Moreham, lk. 50.
[74] U. Fink, lk 78.
[75] EIKo *Y.F. vs Turkey*, p 33.
[76] EIKo 13.12.1979, 8278/78, *X vs Austria*.
[77] EIKo 16.06.2005, 61603/00, *Storck vs Germany*.
[78] EIKo 09.03.2004, 61827/00, *Glass vs United Kingdom*.
[79] EIKo 26.09.2006, 12350/04 *Wainwright vs United Kingdom*. R. Maruste, lk 431.
[80] U. Fink, lk 78.
[81] U. Fink, lk 78.
[82] N. A. Moreham, lk. 50.

näiteks seda kui riik ei ole suutnud karistada isikuid nende tegude toimepanemise eest, mis on rikkunud isiku füüsilist või vaimset terviklikkust või puutumatust.[83]

Isiku füüsilise ja vaimse terviklikkuse kaitse alla käib ka personaalse ruumi kaitse, kus isik saab olla omaette ning segamatult.[84] Sellisteks kohtadeks on näiteks inimese kodu (elukoht), auto, hotellituba, veesõiduk, või muu taoline avalikust väljast äratuntavalt eraldatud ning isiklikuks kasutamiseks mõeldud ruum laiemas mõttes.[85] Inimese koduks olemine ei sõltu sealjuures omandiõigusest või kasutamise sagedusest.[86] Kaasuses Gillow vs United Kingdom[87] leidis EIK, et sõltumata sellest, et isik pole majas elanud 19 aastat, võib seda pidada isiku koduks, sest isik on alati soovinud sinna tagasi kolida ning isik on säilitanud teatud seose selle majaga. Sealjuures võib eraelu kaitsega olla tagatud ka isiku töökoht, sest professionaalne või äritegevus on osa eraelust,[88] ning eraelu kaitsega võib olla tagatud ka juriidilise isiku aadress ja asukoht.[89]

Isiku füüsilist ja vaimset terviklikkuse kaitse alla läheb ka õigus mitte olla jälgitud, sh pealt kuulatud ning visuaalselt jälgitud.[90] Privaatsusõiguse rikkumisena on käsitletud näiteks telefonikõnede pealtkuulamist[91], pealtkuulamisseadme kasutamist inimese kodus[92], vangikongis[93], töökohal[94] ning inimeste salajast filmimist ja fotografeerimist[95]. Kaitse visuaalse jälgimise eest ei piirdu üksnes isiku kodu või personaalse ruumiga, vaid see laieneb ka avalikesse kohtadesse, sest ka isiku käitumine avalikkuses võib minna eraelukaitse alla.[96] See, kas avalikus kohas tehtud pildile võiks laieneda eraelu kaitse, peaks sõltuma kolmest asjaolust; 1) kas pildi tegemine kujutab endast sissetungi inimese privaatsusesse; 2) kas pilt seostub isikliku asjaga või avaliku sündmusega; 3) kas pilt on tehtud piiratud otstarbeks või tehakse see kättesaadavaks avalikkusele.[97]

[83] Nt EIKo 26.03.1985, 8978/80, *X and Y vs Netherlands.* EIKo 04.12.2003, 39272/98, *MC vs Bulgaria*.
[84] R. Maruste, lk 433.
[85] *Ibid*.
[86] U. Fink, lk 86.
[87] EIKo 24.11.1986, 9063/80, *Gillow vs United Kingdom*.
[88] EIKo *Niemietz vs Germany*, p 30.
[89] EIKo 16.07.2002, 37971/97, *Societe Colas Est and others vs France*, p 41-42.
[90] N. A. Moreham, lk. 53.
[91] EIKo 06.09.1978, 5029/71, *Klass and Others vs Germany*, p 42.
[92] EIKo 27.10.2004, 39647/98 40461/98, *Lewis vs United Kingdom*, p 39.
[93] EIKo 05.11.2002, 48539/99, *Allan vs United Kingdom*, p 36.
[94] EIKo 25.03.1998, 23224/94, *Kopp vs Switzerland*, p 27
[95] R. Maruste, lk 433.
[96] EIKo 17.07.2003, 63737/00, *Perry vs United Kingdom*, EIKo 28.01.2003, 44647/98 *Peck vs United Kingdom*.
[97] N. A. Moreham, lk 55.

Lisaks eelnevale laieneb eraelu kaitse ka isikust tehtud salvestuste (nt fotode) levitamisele. EIK on märkinud, et isikul on õigus temast tehtud piltidele, mistõttu kuulub piltide avaldamine eraelu valdkonda.[98] Nt kohtuasjas Peck vs United Kingdom leidis EIK[99], et sõltumata sellest et isik viibib avalikus kohas, on isikul õiguspärane ootus privaatsusele, kui see isik ei ole avaliku elu tegelane ning ei viibi avalikus kohas avalikul üritusel osalemiseks. Seoses avaliku elu tegelastega on EIK-l tulnud kaasustes nagu Von Hannover vs Germany lahendada küsimusi, kuidas saavutada tasakaalu privaatsuse kaitse (art 8) ning ajakirjandusvabaduse (art 10) vahel.[100] Eelnev näitab kui mitmekesine on õigus kehalisele ja vaimsele terviklikkusele, hõlmates väga erinevaid aspekte. Käesoleva töö mõistes kõige olulisemaks on õigus mitte olla jälgitud, mis seostub ka privaatsusõiguse järgmise elemendiga – isikuandmete kogumise ning avalikustamisega.

2) Informatsiooni kogumine ja avalikustamine

Eraelu kaitsealasse kuulub isikuandmete kogumine ning nende andmete avalikustamine.[101] Privaatsusõiguse rikkumiseks on loetud näiteks kirjade ja päevikute lugemist[102], telefoni ja interneti kasutamise jälgimist,[103] samuti ka inimese küsitlemist identiteedi kindlaks tegemiseks ning isikuandmete registreerimist[104]. Privaatsuse kaitse laieneb sealhulgas sõrmejälgedele ja DNA-le, mille osas EIK võtnud seisukoha, et kui politsei säilitab neid andmeid oma registrites isikute kohta, keda pole süüdimõistetud, ei kaalu sellisel juhul avalikud huvid andmete säilitamiseks üles erahuvisid ning selline tegevus rikub isiku privaatsusõigust.[105] EIK on rõhutanud ka meditsiiniliste andmete konfidentsiaalsuse olulisust isikuandmetena, mis on ühelt poolt oluline nii privaatsustunde austamiseks, ning teiselt poolt vajalik meediku elukutse ja tervishoiusüsteemi vastu usalduse säilitamiseks.[106] Lisaks meditsiinilistele andmetele on kuuluvad eraelu kaitse alla ka andmed inimeste kulutuste kohta, mida maksuamet sageli inimestelt nõuab, samuti identifitseerimiseks vajaminevad andmed erinevate sotsiaalteenuste pakkumiseks.[107]

[98] EIKo 11.01.2005, 50774/99, *Sciacca vs Italy*.
[99] EIKo *Peck vs United Kingdom*.
[100] Vt EIKo 07.02.2012, 40660/08, *Von Hannover vs Germany* (nr.2).
[101] N. A. Moreham, lk. 62. R. Maruste, lk 435.
[102] EIKo 22.10.2002, 47114/99, *Taylor-Sabori vs United Kingdom*; EIKo 27.09.1999, 33985/96 33986/96, *Smith and Grady vs United Kingdom*.
[103] EIKo 03.04.2007, 62617/00, *Copland vs United Kingdom*, p 29.
[104] EIKo 31.01.1995, 15225/89, *Friedl vs Austria*, p 21.
[105] EIKo 04.12.2008, 30562/04 ja 30566/04, *S and Marper vs United Kingdom*. U. Fink, lk 80.
[106] EIKo 25.02.1997, 22009/93, *Z vs Finland*.
[107] U. Fink, lk 80.

Ühe suure valdkonnana on EIK käsitlenud oma lahendites julgeolekuteenistuste poolt andmete kogumist ning kogutud andmete säilitamist salajastes registrites. EIK[108] on pidanud privaatsusõigust rikkuvaks kaitsepolitsei või julgeolekuteenistuste poolt kogutud andmete säilitamist salajastes registrites ning selliste andmete kasutamist. Sealjuures võivad need andmed olla avalikult kättesaadavad ning ei pruugi olla väga isiklikud, tundlikud andmed, vaid need peavad seonduma identifitseeritud või identifitseeritava indiviidiga.[109] Kohus on samas lahendites Leander vs Sweden[110] ja S and Marper vs United Kingdom[111] tunnustanud, et andmete kogumine kui selline riikliku julgeoleku nimel on lubatav, kuid võimalike kuritarvituste jaoks peavad olema paigas sobivad ja tõhusad tagatised. Seoses julgeolekuteenistuse käsutuses olevate eelmise režiimiaegsete andmekogude säilitamise ja kasutamisega on EIK näinud seda eraelu riivena, kui isikul, kelle kohta selliseid andmeid säilitatakse, puudub võimalus neid andmeid ümber lükata.[112]

Lisaks eelnevale on riigil positiivne kohustus tagada, et registrites, andmekogudes, arvutites säilitatav informatsioon ei oleks kättesaadav isikutele, kellel ei ole seaduse alusel õigust neid töödelda[113] ning et need, kellel see õigus on, ei kasutaks seda informatsiooni eesmärkidel, mis ei ole kooskõlas Euroopa inimõiguste konventsiooniga.[114] Sealjuures peavad riigid tagama, et kodanikel oleks võimalik kindlaks teha, millised asutused ja ettevõtted nende isikuandmeid hoiavad, millise sisuga andmeid hoitakse ning mis eesmärgil seda tehakse.[115] Õigus saada isikuandmete säilitamise kohta infot, aitab tagada seda, et isikut puuduvad andmed on õiged ning et need ei ole kogutud ebaseaduslikul viisil.[116] Kui andmed on ebaõiged või need on saadud ebaseaduslikul teel, on isikul õigus nõuda andmete parandamist või kustutamist.[117] Kokkuvõtlikult kaitseb privaatsusõigus väga erinevaid isikuga seotud andmeid, sh näiteks avalikke andmeid ning sõrmejälgi ja DNA-s, piirates oluliselt riigi õigust neid andmeid säilitada ning koguda.

3) Inimese elukeskkond

[108] EIKo 26.03.1987, 9248/81, *Leander vs Sweden*.
[109] EIKo 04.05.2000, 28341/95, *Rotaru vs Romania*, p 42-44; EIKo 16.02.2000, 27798/95, *Amann vs Swtizerland*, p 80.
[110] EIKo *Leander vs Sweden.*
[111] EIKo *S and Marper vs United Kingdom*.
[112] EIKo *Rotaru vs Romania*.
[113] EIKo 17.07.2003, 25337/94, *Craxi vs Italy*, p 74-75.
[114] U. Fink, lk 80.
[115] *Ibid.*
[116] *Ibid*, lk 81.
[117] *Ibid*, lk 81. EIKo 18.10.2011, 16188/07, *Kheili vs Switzerland*.

Privaatsusõigus hõlmab ka õigust elada keskkonnas, mis on vaba keskkonnareostusest.[118] Kuigi see ei tundu esmapilgul sobituvat hästi eraelu huviga artikli 8 mõistes ning see ei ole otseselt ka konventsioonis kirjas, on kohus tunnustanud, et tõsine keskkonnareostus võib oluliselt mõjutada isiku heaolu ning võimalust nautida oma kodu, mõjutades negatiivselt isiku era- ning perekonnaelu.[119]

Privaatsusõiguse rikkumiseks on loetud näiteks olukorda, kus riik ei ole suutnud ära hoida ebaseadusliku jäätmejaama ehitamist[120], pole suutnud anda informatsiooni inimestele kohaliku keemiatööstuse ohtude kohta[121] või pole suutnud ära hoida lõbustusasutustest tulenevat mürareostust elamupiirkonnas[122]. Õigus puhtale keskkonnale pole nähtud siiski absoluutse õigusena, vaid kohus on näinud vajadust hinnata nii konkreetse indiviidi huvisid kui ka ühiskonna huvisid tervikuna.[123] Näiteks Hatton ja teised vs the United Kingdom kaasuses leidis EIK, et sõltumata sellest, et lennujaama tegevusest tulenev müra võib rikkuda nende õigust privaatsusele, on see rikkumine põhjendatav riigi majandusliku heaoluga.[124] See näitab, et privaatsusõigus hõlmab väga erinevaid aspekte ning sageli tuleb nende piiramist kaaluda lähtuvalt avalikest huvidest.

4) Identiteet

Isiku identiteet on sellistele unikaalsete tunnuste kogum, mille alusel eristub isik kõikidest teistest isikutest.[125] Sealjuures on see isiku enesemääratlus iseenda ja välismaailma jaoks, see on vabadus otsustada ja olla see, kes tahetakse olla.[126] Identiteeti kannavad edasi isiku nimi, etniline kuuluvus, sugu, isiku välimus ja muud füüsilised omadused, iseloom, käitumine, tunded, mõtlemine, seksuaalne määratlus, isiklik ruum, sotsiaalne võrgustik, elukäik, riietus jne.[127]

EIK on lahendanud palju kaasuseid, mis käsitlevad identiteediga seotud privaatsusõiguse rikkumisi, ning mis on laiendanud ning avardanud oluliselt EIÕK artikli 8 sisu. Näiteks

[118] N. A. Moreham, lk. 64. M. Männiko, lk 33.
[119] N. A. Moreham, lk. 64. EIKo 08.07.2003, 36022/97 *Hatton and others vs United Kingdom*. EIKo 09.02.1994, 16798/90, *Lopez Ostra vs Spain*.
[120] EIKo 09.02.1994, 16798/90, *Lopez Ostra vs Spain*.
[121] EIKo 19.02.1998, 14967/89, *Guerra vs Italy*, p 56-60.
[122] EIKo 16.11.2004, 4143/02, *Gomez vs Spain*, p 53-63.
[123] EIKo 08.07.2003, 36022/97, *Hatton ja teised vs United Kingdom*.
[124] *Ibid*.
[125] M. Männiko, lk 18.
[126] R. Maruste, lk 429.
[127] M. Männiko, lk 18. R. Maruste, lk 429.

kaasuses Odiere vs Prantsusmaa[128] oli EIK seisukohal, et isikul on õigus teada oma geneetilisi vanemaid, sest informatsioon vanemate kohta moodustab osa isiku identiteedist. [129] Identiteet on seega oluline isiku enesemääratlemise jaoks, mis on üks olulisemaid vabaduse väljendusi, nagu ka järgmine privaatsusõiguse element.

5) Autonoomia

Õigus arendada perekondlikke ja muid sotsiaalseid suhteid, õigus otsustada oma seksuaalsuhete üle, rakendada kontrolli oma tervise ning ravi üle, on osa indiviidi autonoomiast, mis kuulub privaatsusõiguse kaitse alla.[130] Indiviidi autonoomia on oluline seetõttu, et Euroopa inimõiguste konventsiooni tuumaks on inimväärikuse ja inimese vabaduse austamine[131] ning autonoomia põhimõte on nende väärtuste või garantiide aluseks.[132]

Nagu märgitud, kaitseb privaatsusõigus ühe aspektina näiteks isiku seksuaalset autonoomiat.[133] EIK on korduvalt kinnitanud, et privaatsus kaitseb kõiki seksuaalse tegevuse vorme, sh homoseksuaalsust, kui need ei riku isikute individuaalseid õiguseid.[134] Näiteks leidis EIK kaasuses Dudgeon vs United Kingdom[135], et ainuüksi sellise seaduse olemasolu, mille alusel on täiskasvanud meeste vabatahtlik seksuaaltegevus keelatud ning karistatav, on vastuolus õigusega privaatsusele. Kohtuasjas Christine Goodwin vs United Kingdom oli kohus seisukohal, et riikidel on kohustus tunnustada soovahetust, lubades teha sünnitunnistusel ja teistel ametlikel dokumentidel parandusi.[136]

Euroopa inimõiguste konventsiooni artikkel 8 kaitseb õigust perekonnaelule. See, kas suhe on käsitletav perekondliku suhtena, sõltub suhte iseloomust ning lähedaste isiklike seoste olemasolust.[137] EIK on oma praktikas pidevalt arendanud perekonna mõistet, võttes arvesse ühiskonnas toimuvaid sotsiaalseid ning õiguslikke muutuseid. Näiteks on EIK perekonnaelu tõlgendanud väga paindlikult ning võtnud arvesse moodsa perekonna elukorraldust, lahutuste

[128] EIKo 13.02.2003, 42326/98, *Odievre vs Prantsusmaa*.
[129] Privaatsusõiguse ja identiteediga seotud aspektide kohta vt lähemalt L. Wildhaber, O. Diggelmann. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica I/2007.
[130] N. A. Moreham, lk 71.
[131] EIKo 29.04.2002, 2346/02, *Pretty vs United Kingdom*, p 65.
[132] EIKo 11.07.2002, 28957/95, *Goodwin vs United Kingdom*, p 90.
[133] U. Fink, lk 78.
[134] *Ibid*.
[135] EIKo 22.10.1981, 7525/76, *Dudgeon vs United Kingdom*.
[136] EIKo 11.07.2002, 28957/95, *Christine Goodwin vs United Kingdom*.
[137] U. Fink, lk 85.

mõju ning meditsiinilisi võimalusi.[138] Kaasuses Johnston vs Ireland[139] oli EIK seisukohal, et mitteabielus olevate, aga üksteisega koos elavate lastega paaride elu käib samuti perekonnaelu kaitse alla. EIK[140] on leidnud, et eraelu ning perekonnaelu kaitse alla käivad lisaks ka samasooliste suhted. Õigus eraelule hõlmab samuti ema ja lapse suhet ning alates 2009. aastast tunnistas EIK, et õigus eraelule kaitseb ka abielus mitteoleva isa ning tema lapse vahelist suhet.[141]

Kuivõrd Euroopa inimõiguste konventsioon nö elav instrument, mida tuleb tõlgendada iga kord vastavalt uutele tingimustele[142], ei ole eelnevalt väljatoodu elemendid ja nende kirjeldus kindlasti ammendav ning lõplik. Sealjuures tuleks silmas pidada, et privaatsusõigus ei ole oma olemuses eesmärk ise, vaid see on vahend saavutamaks kõrgemat eesmärki, milleks on õigus inimväärikusele.[143] Samuti ei ole privaatsus absoluutne väärtus ning üks kõige keerulisem ülesanne probleemide lahendamisel ühiskonnas on teha otsus kahe võistleva väärtuse vahel.[144] Näiteks kerkib see küsimus olukorras, kus on tungiv vajadus kaitsta riigi julgeolekut ning põhiseaduslikku korda. Et mõista paremini selle otsuse tegemise keerukust, käsitletakse järgnevalt seda, miks on privaatsus oluline ning milliseid negatiivseid mõjusid võib kaasa olukord, kus riik jälgib oma kodanikke.

1.4. Privaatsuse olulisus ja jälgimise negatiivsed mõjud

Enne kui minna privaatsuse olulisuse juurde, on oluline käsitleda seda, kelle huvisid privaatsusõigus teenib. Privaatsust seostatakse sageli isiku enda erahuviga, sest paljud teooriad on näinud privaatsust eelkõige indiviidi õigusena, mis tuleneb austusest isiku autonoomsuse, isikuks olemise vastu.[145] Näiteks Thomas Emersoni sõnul põhineb privaatsus individualismil ning privaatsusõigus on eelkõige õigus mitte osaleda kollektiivses elus.[146] Seda käsitlust võib

[138] U. Fink, lk 85.
[139] EIKo 18.12.1986, 9697/82, *Johnston vs Ireland*.
[140] EIKo 24.06.2010, 30141/04, *Schalk and Kopf vs Austria*.
[141] U. Fink, lk 85. EIKo 03.12.2009, 22028/04, *Zaunegger vs Germany*.
[142] U. Fink, lk 90-91.
[143] S. Stalla-Bourdillon, lk 13.
[144] W. H. Rehnquist. Is an expanded right of privacy consistent with fair and effective law enforcement? Or: Privacy, You´ve Come a Long Way Baby. – Kansas Law Review, 1974/23, lk 2.
[145] D. J. Solove. „I've Got Nothing to Hide" and Other Misunderstandings of Privacy. – San Diego Law Review. 2007/44. Lk 760.
[146] D. J. Solove 2007, lk 760.

siiski ekslikuks pidada. Nagu ka julgeolek ja turvalisus, on ka privaatsus samaaegselt nii isiklik huvi kui ka avalik huvi, mis teenivad nii üksikisikut ennast kui ka ühiskonna gruppe laiemalt.[147]

Seda eelkõige seetõttu, et üksikisikute privaatsuse kaitsmine toob kaasa positiivseid mõjusid ühiskonnale üldiselt.[148] D. J. Solove hinnangul on privaatsuse kaitsmisel sotsiaalne väärtus, sest ühiskonnas elamisele on iseloomulik konfliktide esinemine, mistõttu on ühiskonnas on hea elada üksnes siis, kui inimestel lubatakse elada ilma nende ellu sekkumata.[149] D. J. Solove hinnangul oleks „Ühiskond ilma privaatsuse kaitseta … lämmatav ja see ei oleks koht, kus enamus sooviks elada.“[150] Individuaalseid õiguseid kaitstes võib ühiskond saada kasu eelkõige seeläbi, et inimestele vabaduse andmisega võimaldatakse inimestel ennast realiseerida.[151] Sealjuures ei ole privaatsus üksnes piirang ühiskonnale, vaid läbi selle on võimalik tagada ühiskonnas käitumisreeglite järgimist ning tsiviliseeritust.[152] Teisisõnu vajab ühiskond privaatsust selleks, et tagada ühiskonnas korda.[153] Privaatsus ei tähenda indiviidi õiguste huvide eelistamist ühiskonna huvide ees, vaid see on sotsiaalne kontroll, mis tuleneb ühiskonna enda normidest ja väärtustest.[154] Teisisõnu, isegi kui privaatsus kaitseb indiviidi, teeb ta seda kogu ühiskonna toimimise nimel, mistõttu ei ole tegemist indiviidi ja ühiskonna õiguste või huvide vastandumisega.[155] Seega on privaatsusõigus nii üksikisiku huvides kui ühiskonna huvides laiemalt.

Tulles privaatsuse olulisuse juurde, tuleb märkida, et privaatsus on oluline mitmest perspektiivist lähtuvalt. Esiteks, filosoofilisest küljest on Euroopa riikides oluline inimväärikus ja inimese terviklikkus, samuti individuaalne autonoomia ja enesemääratlemine, mis toetavad üldiselt inimõiguste mõiste sisu ning olulisust.[156] Privaatsus aitab tagada inimese autonoomsust ja enesemääratlemist, näiteks otsuste tegemisel.[157] Ka psühholoogiliselt vajavad inimesed omaette ruumi, et hinnata oma ümbrust, samuti tegeleda nende tegevustega, mis avalikkuses valmistaksid neile piinlikkust.[158] Sageli on võimatu lõdvestuda ilma privaatsuseta.[159]

---

147 S. Stalla-Bourdillon, lk 65.
148 *Ibid*, lk 66.
149 D. J. Solove, lk 760.
150 *Ibid*, lk 762.
151 *Ibid*.
152 R. C. Post. The Social Foundations of Privacy: Community and Self in the Common Law Tort. – California Law Review. 1989/77, lk 959.
153 D. J. Solove, lk 763.
154 *Ibid*.
155 *Ibid*.
156 R. Clarke. What's 'Privacy? 2006. – http://www.rogerclarke.com/DV/Privacy.html (24.03.2016)
157 J. Griffin. The Human Right to Privacy. - San Diego Law Review. 2007/44, lk 700.
158 R. Clarke.
159 J. Griffin, lk 701.

Sotsioloogiliselt peavad inimesed saama vabalt käituda ning suhelda teistega ilma kartuseta, et neid jälgitakse.[160] Privaatsus võimaldab suhtluses teiste inimestega jääda ausaks.[161] Teisisõnu on privaatsus seotud vabadusega tegutseda, sest paljudel puudub julgus või enesekindlus tegutseda avalikkuse ees.[162]

Privaatsus on oluline ka majanduslikus mõttes, et inimesed saaks olla vabad, mis võimaldab neil olla innovaatilised.[163] Innovaatilistele inimestele on omane see, et nad kalduvad eksperimenteerides kõrvale üldistest normidest.[164] Kui need inimesed oleksid aga kogu aeg kellegi silme all, tunneksid need inimesed end ebamugavalt ning tõenäoliselt ei kalduks nii sageli tavapärasest kõrvale. Ka poliitiliselt peavad inimesed olema vabad mõtlema, argumenteerima ja käituma.[165] Poliitiline vabadus, sealhulgas mõttevabadus on eelduseks demokraatia toimimisele.

Üheks suurimaks ohuks inimese privaatsusele on jälgimine, seda nii riigi kui ka eraisikute/ettevõtete poolt. Inimeste jälgimine ei ole uus nähtus, kuid seoses tehnoloogia arengu ja julgeoleku olukorraga, on see muutumas järjest olulisemaks teemaks. Jälgimist võib defineerida kui fokusseeritud, süstemaatilist ja rutiinset tähelepanu personaalsetele üksikasjadele, mille eesmärgiks on mõjutamine, juhtimine kaitsmine või suunamine.[166] Kuigi jälgimisel võib olla palju eesmärke, on need seotud tavaliselt võimuga – sooviga mõjutada või kontrollida jälgitavat.[167]

Jälgimine võib toimuda erivormides, kuid käesoleva töö kontekstis võib tuua välja kaks olulist tüüpi: massijälgimine, mille käigus kogutakse valimatult informatsiooni kõigi kohta eesmärgiga kasutada seda tulevikus, ning eesmärgistatud jälgimine, mis puudutab üksnes loetud isikuid.[168] Nii massijälgimine kui ka eesmärgistatud jälgimine kujutavad endast eraellu sekkumist, kuid nende tõsisus sõltub sekkumise tüübist ehk millist informatsiooni kogutakse, säilitatakse ning võimalik et ka väärkasutatakse.[169] Massijälgimisega seoses on kasutusel ka termin „suurandmed“ (inglise keeles *Big Data*), millega kirjeldatakse massiivsete

[160] R. Clarke.
[161] J. Griffin., lk 701.
[162] *Ibid*, lk 701-702.
[163] R. Clarke.
[164] *Ibid.*
[165] *Ibid*
[166] D. Lyon. Surveillance Studies. Cambridge: Polity Press 2007, lk 14.
[167] *Ibid*, lk 14; N. M. Richards. The Dangers of Surveillance. – Harward Law Review 2013, lk 1937.
[168] S. Stalla-Bourdillon, lk 13-14.
[169] S. Stalla-Bourdillon, lk 15.

andmekogude loomist ja analüüsimist.[170] Suurandmed ei ole tähelepanuväärne mitte üksnes isikuandmete suure koguse tõttu, vaid seetõttu, et olulist teavet saadakse läbi erinevate seoste loomise, mis saadakse erinevatest valdkondadest ning allikatest.[171]

Sageli väidetakse, et inimeste jälgimisega ei kaasne privaatsuse probleemi, sest kui sul pole midagi varjata, siis pole sul ka midagi karta.[172] See põhineb valel eeldusel, et privaatsuse mõte on varjata halbu asju.[173] Igal isikul on õigus privaatsuse kaitseks sõltumata sellest, kas inimesel on midagi varjata või kas isik tunneb ise otseselt vajadust privaatsuse kaitse järele. Samuti on väidetud, et üksnes suurte koguste andmete kogumisega elektrooniliste vahendite kaudu ei saa isikute privaatsusesse tungida, sest seda teevad masinad, mitte inimesed.[174] Need seisukohad viitavad sellele, et sageli alahinnatakse, milline väärtus privaatsusel on.

Põhjuseid, miks peaks jälgimist kartma, on mitmeid. Jälgimisega kaasnevad mitmed negatiivsed mõjud, mida sageli ei tunnistata. N. M. Richardsi hinnangul on kõige suurem jälgimise kahju oht „intellektuaalsele privaatsusele".[175] Intellektuaalse privaatsuse teooria kohaselt arenevad uued ideed kõige paremini eemal avalikkuse tähelepanust.[176] Avalikkusest eemal olek tagab isikule vajaliku anonüümsuse, mis on vajalik mõtlemisvabaduse, tegevusvabaduse ning avatud ühiskonna edendamiseks.[177] Jälgimisega kaasneb anonüümsuse kaotamine, mis tähendab seda, et inimesed ei saa tegutseda ilma, et neid identifitseeritaks või jäetaks märkamata teiste seas.[178] Seetõttu on intellektuaalne privaatsuse otseselt seotud ka mõtte-, usu- ning sõnavabadusega, samuti kogunemisvabadusega.[179]

Kui meid jälgitakse ning me teame seda, siis me ei tee reeglina midagi sellist, mida teised peaksid tavapärasest kõrvale kalduvaks.[180] Seda põhjusel, et kui isik teab, et teda jälgitakse, identifitseerib see isik ennast ka jälgijaga ning lisaks enda nägemusele oma tegevustes arvestab isik ka sellega, kuidas paistavad tema tegevused kõrvaltvaatajale, ning see paneb isikut teisiti

[170] N. M. Richards, lk 1939.
[171] *Ibid.*.
[172] D. J. Solove 2007, lk 746.
[173] *Ibid*.
[174] R. A. Posner. Our Domestic Intelligence Crisis. – Washington Post, 21.12.2005. – http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html (25.03.2016).
[175] N. M. Richards, lk 1945-1946.
[176] *Ibid*.
[177] C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal. 2002/72, lk 236. N. M. Richards, lk 1946.
[178] M. Paterson. Surveillance in Public Places. in Emerging Challenges in Privacy Law. Comparative perspectives. Edited by N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick, lk 203.
[179] N. M. Richards, lk 1946-1947.
[180] *Ibid*, lk 1948.

käituma.[181] Sealjuures ei ole vahet kui vähetähtsate tegevuste või kavatsustega on tegemist, sest isik mõtleb iga tegevuse hoolikalt läbi, mis muudab elu vähem spontaanseks ning rohkem kaalutletuks.[182] Kui inimesed lepivad jälgimise paratamatusega, muutuvad nende harjumused ning ka nemad ise.[183] Jälgimisega kaasneb seega nö enesetsensuur, mida kinnitavad mitmed uuringud ning sealjuures võib enesetsensuur puudutada ka kõne-, tegevus ning usuvabadust.[184] Seega on jälgimisel otsene mõju tsiviliseeritud ühiskonna vabadustele, samuti poliitilisele vabadusele, mis on demokraatliku ühiskonna alustalaks.[185] See muudab meie käitumise kooskõlas olevaks peavoolu ehk enamuse inimeste käitumisega, mis muudab meid paratamatult ka igavamaks, sest inimesed kardavad olla teistest erinevad või omapärased.[186] See ohustab nii intellektuaalset mitmekesisust kui ka individualismi.[187]

Teine oht seisneb selles, et jälgimine mõjutab jälgija ja jälgitava võimu tasakaalu, andes jälgijale suurema võimu mõjutada või suunata järelevalve subjekti.[188] Informatsioon on võim, mistõttu võib jälgimine tuua kaasa sellised negatiivsed tagajärjed nagu väljapressimine, sest kõigil on saladused või piinlikust valmistavad teod, mida soovitakse teiste eest varjata, samuti võib sellega kaasneda diskrimineerimine ning suurema veenmisjõu[189] saavutamine.[190]

Samuti võib jälgimisega kaasneda oht, et jälgimist kasutatakse automaatsete otsuste tegemiseks, tuginedes üksnes jälgimisega saadud informatsioonile. Sellisel juhul ei pruugi isik olla teadlik, et tema kohta andmeid kogutakse ning ta ei ole teadlik, milliseid tagajärgi võib see tema jaoks kaasa tuua.[191] See tähendab, et isikul võib puududa informatsiooni kogumise ja kasutamise protsessi üle igasugune kontroll.[192] Probleem seisnes ka selles, et isikul ei ole

[181] J. Reiman. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. – Santa Clara Computer ja High Technology Law Journal. 1995/11, lk 38. Viidatud C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal. 2002/72, lk 238.
[182] R. Wasserstrom. Privacy: Some Arguments and Assumptions, in Philosophical Dimension of Privacy. Ed. F. D. Schoeman. Cambridge University Press 1984. viidatud C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal. 2002/72, lk 238.
[183] N. C. Burbules, Privacy, Surveillance, and Classroom Communication on the Internet. – http://faculty.education.illinois.edu/burbules/papers/privacy.html (25.03.2016).
[184] N. M. Richards, lk 1949.
[185] *Ibid*, lk 1949, 1951.
[186] *Ibid*, lk 1948. J. Cohen. Examined lives: Informational Privacy and the Subject as Object. – Stanford Law Review. 2000/52, lk 1426.
[187] N. M. Richards, lk 1948.
[188] *Ibid*, lk 1953.
[189] Suurema veenmisjõu saavutamine ei ole alati halb, näiteks kui liikluskaamerad teedel distsiplineerivad sõiduki juhte liikluseeskirju järgima.
[190] N. M. Richards, lk 1953.
[191] M. Paterson. Surveillance in Public Places. in Emerging Challenges in Privacy Law. Comparative perspectives. Edited by N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick. Lk 203-204.
[192] D. J. Solove. Conceptualisation privacy. – California Law Review. 2002/90, lk 1087.

võimalik sellist salajast andmete kogumist vaidlustada ning õiguskaitsevahendeid efektiivselt kasutada. Näiteks USAs on olnud mitmed juhtumid, kus kohtupraktika põhjal on tekkinud paradoks, et kaebaja ei suuda tõendada, et tema telefoni on pealt kuulatud, sest valitsuse salateenistus ei ole kohustatud neid andmeid avaldamast, mistõttu ei saa isik oma õiguste rikkumisel kohtus kaitset, sest ei ole suuteline pealtkuulamist tõendama.[193]

Jälgimise võimalikku mõju privaatsusele on kirjeldatud ka kirjandusteostes, näiteks George Orwelli Suure Venna või inglise filosoofi Jeremy Benthami kujutatud panoptikumina. Filosoof ja ajaloolane Michel Foucault on kirjeldanud modernset ühiskonda kui Benthami kujutatud panoptikumina[194], kus inimesed teavad, et nende iga liigutust jälgitakse, mistõttu allutavad inimesed ennast automaatselt võimule, sest nad tunnetavad pidevat survet järgimaks ükskõik milliseid norme neile peale surutakse.[195] See võimaldab neutraliseerida kõik jõud, mis soovivad sellele valitsevale võimule vastu hakata.[196] George Orwelli teoses „1984“ oli sarnane olukord, kus Suureks Vennaks nimetatud partei juht jälgis kõiki ja kõike ning lisaks inimeste tegevustele ja sõnadele jälgiti ka inimese mõtteid, sealjuures olid karistatavad ka mõttekuriteod.[197] „1984“ kirjeldas seega, kuidas hirm olla jälgitud muudab inimeste mõtteid ning käitumisi. Kuigi need teosed on fiktsioon, aitavad need mõista, kuidas võib jälgimine inimesi mõjutada.

Kokkuvõtlikult näitab eelnev, et privaatsus on demokraatliku ning liberaalse ühiskonna alustalaks, olles lahutamatult seotud nii isiku vabaduse kui inimväärikusega. Jälgimisega võivad kaasneda mitmed negatiivsed mõjud, mis võivad ohustada inimese autonoomiat, tegevus- ning otsustusvabadust. Käesolevas peatükis käsitletud privaatsusõiguse erinevad elemendid näitasid, kui mitmekesine on privaatsusõiguse kui põhiõiguse olemus. Järgmises osas analüüsitakse seda, millistel alustel ja tingimustel on privaatsusõigusesse lubatud sekkuda ning kuidas toimub privaatsusõiguse riivete proportsionaalsuse kontroll.

[193] N. M. Richards, lk 1944.
[194] Inglise filosoof Jeremy Benthami kujutatud ringikujuline ehitis (vangla), mille tornist sai ülevaate kogu ehitises toimuva üle.
[195] C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal. 2002/72, lk 236-237.
[196] C. Slobogin, lk 236-237.
[197] G. Orwell. 1984. Tallinn: Perioodika 1990.

2. PRIVAATSUSÕIGUSE PIIRAMISE ALUSED

Käesolevas peatükis käsitletakse seda, millistel eesmärkidel lubab Euroopa inimõiguste konventsioon ja Euroopa Liidu põhiõiguste harta eraellu sekkumist ning millistel tingimustel on Euroopa Inimõiguste Kohus ja Euroopa Kohus pidanud oma lahendites õigustatuks sekkumist inimeste eraellu. Selleks tutvustatakse kõige pealt põhiõiguste piiramise alused üldiselt ning seejärel käsitletakse kõiki aluseid lähemalt. Vastavalt töö fookusele keskendutakse käesolevas osas eelkõige juhtumitele, kus riik sekkub isikute eraellu julgeoleku, kuritegude avastamise ja ärahoidmise või avaliku korra eesmärgil, pöörates erilist tähelepanu isikute salajasele jälgimisele ning massijälgimisele.

2.1. Põhiõiguste piiramise üldised alused

Euroopa inimõiguste konventsioonis sätestatud õigused võib tinglikult jaotada kolmeks õiguste grupiks: 1) õigused, mida ei ole lubatud piirata[198], 2) õigused, mida võib piirata üksnes hädaolukorras, ning 3) õigused, mida võib rahu ajal piirata, tingimustel, mis on konventsioonis loetletud.[199] Privaatsusõigus kuulub nende mitteabsoluutsete õiguste hulka, mille puhul Euroopa inimõiguste konventsioon loetleb mitmed olukorrad, millal on privaatsusõigusesse sekkumine lubatud. Euroopa inimõiguste konventsiooni artikkel 8 lõige 2 kohaselt ei sekku ametivõimud privaatsusõiguse kasutamisse muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks. Privaatsusõigust ning teisi õigusi, mida võib konventsioonis sätestatud põhjustel piirata, nimetatakse kvalifitseeritud õigusteks.[200]

Selleks, et EIÕK alusel oleks eraellu sekkumise riive lubatud, tuleb täita kolm tingimust: 1) riive peab olema seadusega ette nähtud („kooskõlas seadusega“); 2) riive eesmärk peab olema

[198] EIÕK-s on sellisteks säteteks nt piinamise keeld ja õigus elule. Esimene neist on absoluutne õigus ja keeld, millest Eesti põhiseadus ega rahvusvaheline õigus ei luba mingeid erandeid (R. Maruste. PõhiS § 18/1 – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012). Seoses õigusega elule samas on selline seisukoht vaieldav, sest Riigikogu on selgitanud, et “[Ü]hiskonnas ei saa olla absoluutseid – piiramatuid põhiõigusi. Mis tahes põhiõiguse realiseerimisvõimalused saavad piiramatult kesta vaid seni, kuni seejuures ei takistata mingi teise põhiõiguse realiseerimist. Sellises põhiõiguste konkurentsi olukorras tekib paratamatult põhiõiguste piiramise vajadus.” (RKKKo 3-1-1-80-97, p I).

[199] B. Sloot. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for o fourth one. – Information & Communications Technology Law 2015/24, lk 77.

[200] B. Sloot, lk 77.

konventsioonis ette nähtud; 3) riive peab olema demokraatlikus ühiskonnas vajalik.[201] Riive eesmärgi ning vajalikkuse kontroll (teine ja kolmas tingimus) moodustavad demokraatliku vajalikkuse testi, milles hinnatakse, kas sekkumine eraellu on vajalik lähtuvalt soovitud eesmärgist.[202]

Euroopa Liidu õiguses[203] tohib õiguste ja vabaduste teostamist piirata ainult seadusega ning arvestades nimetatud õiguste ja vabaduste olemust ning piiranguid võib seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele[204] või kui on vaja kaitsta teiste isikute õigusi ja vabadusi.

Sisuliselt on Euroopa Inimõiguste Konventsiooni süsteemis ning Euroopa Liidus põhiõiguste riive alused sarnased, nõudes vajalikkuse testi läbimist. Sisuliselt on selle vajalikkuse testi näol tegemist proportsionaalsuse testiga, mida on sisustatud sarnaselt ka Eesti kohtupraktikas. Riigikohus[205] on leidnud, et PS §-st 11 tuleneb nõue, et õiguste ja vabaduste piirangud peavad olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust. Riigikohus on lisanud, et piirangud ei tohi kahjustada seadusega kaitstud huvi või õigust rohkem, kui see on normi legitiimse eesmärgiga põhjendatav ning kasutatud vahendid peavad olema proportsionaalsed soovitud eesmärgiga. Järgnevalt käsitletakse neid tingimusi lähemalt, millal on eraellu sekkumise riive lubatud, keskendudes eelkõige salajase ja massijälgimisega seotud juhtumitele.

2.2. Seaduslik alus

„Kooskõlas seadusega“ ehk nn seadusliku aluse test tähendab EIÕK kontekstis seda, et seaduses peab olema selge õiguslik alus eraellu sekkumiseks, see alus peab olema isikutele kättesaadav ning see peab olemas kooskõlas õigusriigi põhimõttega.[206] „Kooskõlas seadusega“ seostub seaduse kvaliteediga, mis nõuab, et see oleks kooskõlas õigusriigi põhimõttega.[207] See tähendab aga, et seaduse peab olema piisavalt ettenähtav ning seaduses peavad olema kaitsemeetmed meelevaldse sekkumise eest. Oma olemuselt hõlmavad need Eesti

[201] B. Sloot, lk 77.
[202] B. Sloot, lk 77.
[203] Euroopa Liidu põhiõiguste harta artikli 52 lõige 1.
[204] Inglise keeles „*general interest recognised by the Union“*
[205] RKPJKo 3-4-1-6-00, p 13.
[206] EIKo 29.06.2006, 54934/00 *Weber and Saravia vs Germany*, p 84; EIKo 26.04.1979, 6538/74, *Sunday Times vs the United Kingdom*.
[207] EIKo 02.08.1984, 8691/79, *Malone vs the United Kingdom*, p 67.

kohtupraktika kohaselt määratuse ehk õigusselguse ning seadusereservatsioonipõhimõtteid, mida hinnatakse riive formaalse põhiseaduspärasuse hindamisel.[208] Näiteks nõuab õigusselguse põhimõte, et õigusaktid oleksid sõnastatud piisavalt selgelt ja arusaadavalt, et isikul oleks võimalik piisava tõenäosusega ette näha, milline õiguslik tagajärg kaasneb teatud tegevuse või tegevusetusega.[209]

Ka EIK kohtupraktikas on korduvalt selgitatud, et isik näeks mõistlikult ette oma tegude tagajärgi, peab õiguslik alus (säte) olema piisavalt selge ja täpne.[210] Samas on EIK märkinud, et riikliku julgeoleku valdkonnas ei saa ettenähtavus olla samasugune nagu teistes valdkondades, mistõttu ei pea isik täpselt ette nägema, millal ja milliseid kontrolle tema suhtes riikliku julgeoleku kaitseks tehakse, et ta saaks vastavalt sellele oma käitumist kohandada.[211] Ettenähtavus ei tähenda ka seda, et õigusaktis tuleks detailselt kirjeldada kõiki juhtumeid, mis võivad kaasa tuua salajase jälgimistegevus.[212] Siiski peaks seadus andma isikutele üldise indikatsiooni, millistes olukordades ning tingimustel on riigivõimul õigus sekkuda eraellu.[213] Kuna salajane jälgimine ei toimu isiku või avalikkuse järelevalve all, peab seadus võimorganitele ja kohtutele ette nägema selge kaalutlusõiguse ulatuse ning selle rakendamise viisi, mis peavad olema piisavalt selged, et anda üksikisikule piisav kaitse omavolilise sekkumise eest.[214] See on eriti oluline olukorras, kus kasutamiseks olemasolev tehnoloogia muutub järjest keerulisemaks.[215] Seega peavad salajase jälgimise tingimused olema selgelt kirjas seaduses, kuid ettenähtavuse hindamisel tuleb sellele lisaks arvesse võtta haldusesiseid juhiseid ning halduspraktikat ning mil määral on nende sisu avalikkusele teatavaks tehtud.[216]

Lisaks eelnevale peab seadus pakkuma ka efektiivseid kaitsemeetmeid meelevaldse sekkumise ning võimu kuritarvitamise vastu.[217] Eriti on see vajalik olukorras, kus täidesaatvat võimu teostatakse salajas, mille puhul on olemas risk kuritarvituste esinemiseks.[218] EIK on kujundanud oma kohtupraktikas välja loetelu miinimum tagatistest, mis peaksid olema

[208] RKPJKo 3-4-1-6-08, p 43.
[209] PõhiS § 13/5.2.1. – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012.
[210] B. Sloot, lk 77.
[211] EIKo *Leander vs Sweden*, p 51.
[212] EIKo 12.01.2016, 37138/14, *Szab and Vissy vs Hungary*, p 64.
[213] EIKo *Leander vs Sweden*, p 51.
[214] EIKo *Malone vs the United Kingdom*, p 67, EIKo 24.04.1990, 11105/84, *Huvig vs France*, p 29, EIKo *Leander vs Sweden*, p 51.
[215] EIKo *Kopp v. Switzerland*, p 72.
[216] EIKo *Leander vs Sweden*, p 51.
[217] B. Sloot, lk 77.
[218] EIKo *Malone vs the United Kingdom*, p 67.

sätestatud riigisisese õiguses, et hoida ära võimu kuritarvitamine.[219] Need tagatised on järgmised:

1) Süüteo olemus, mille korral võib eraelupuutumatust riivata;
2) Isikute ring, kelle suhtes sekkumist võidakse rakendada;
3) Eraellu sekkumise ajalised piirid;
4) Protseduur, mida järgitakse saadud andmete edastamiseks, kasutamiseks ja hoidmiseks;
5) Ettevaatusabinõud andmete jagamisel teistega;
6) Tingimused, millal võib või tuleb andmed kustutada või hävitada.[220]

Kohtuasjas Liberty vs United Kingdom leidis EIK, et telefonide ja e-mailide jälgimisega isiku eraellu sekkumine ei olnud kooskõlas seadusega, sest kohus andis väga laia kaalutlusõiguse, milliseid isikuid või kommunikatsiooni tohib salaja pealt kuulata või lugeda, samuti ei olnud avalikustatud ning määratletud, millise protseduuri järgi toimus jälgimisega saadud materjali hindamine, jagamine, säilitamine ja hävitamine (sh mille alused valiti välja andmed ning mille alusel valiti otsingumärksõnu).[221] Olukorras, kus jälgimismeetmete rakendamise osas on erinevad tõlgendused ning ei ole selge, millised reeglid on sätestatud seadustes ning mis on jäetud ametiasutuse otsustada, ei taga piisavalt kaitset kodanikele, millele neil oleks õigus vastavalt õigusriigi põhimõttele.[222]

Kokkuvõtlikult peab salajase jälgimise meetmete rakendamisel olema seaduses piisav alus, mis võimaldab isikutel riigipoolset sekkumist ette näha, samuti peavad olema täpselt määratletud võimorganite ja kohtute kaalutlusõiguse ulatus ning erinevad tagatised võimu kuritarvitamise vältimiseks. Järgnevalt käsitletakse, millised on need legitiimsed eesmärgid, millal võib seaduse alusel eraellu sekkuda.

2.3. Legitiimne eesmärk

Privaatsusõigusesse sekkumine on EIÕK artikkel 8 lõike 2 alusel lubatud järgmiste legitiimsete eesmärkide korral: 1) avaliku huviga seotud eesmärgid – riiklik julgeolek, ühiskondlik turvalisus, korrakaitse ja kuritegude ennetamine, riigi majandusliku heaolu, tervis, kõlblus, [223]

[219] EIKo 29.06.2006, 54934/00 *Weber and Saravia vs Germany*, p 95.
[220] *Ibid*, p 95.
[221] EIKo 01.07.2008, 58243/00, *Liberty vs United Kingdom*, p 64-69.
[222] EIKo *Malone vs United Kingdom*, p 79.
[223] Võrdluseks Eesti õiguses võib eraellu sekkuda tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks (PS § 26).

ning 2) erahuviga seotud põhjendused – kaasinimeste õiguste ja vabaduste kaitse.[224] Kohtupraktikas on EIK erahuviga seotud põhjendusi kasutanud harva ning enamasti on kohus tuginenud just ühiskondlikule või avalikule huvile.[225] Seoses konventsioonis sätestatud eranditega, on EIK märkinud, et neid tuleb tõlgendada kitsendavalt.[226]

Euroopa Liidu põhiõiguste harta artiklitega 7 ja 8 tagatud õiguste riive õigustatud üksnes siis, kui riive vastab üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi. Võrreldes Euroopa inimõiguste konventsiooniga, on harta sõnastus oluliselt umbmäärasem, jättes sisustamata, mida üldist huvi pakkuv eesmärk endast kujutab.

Üldist huvi pakkuvad liidu eesmärke võib leida nii Euroopa Liidu lepingu artiklist 3 kui ka erinevatest Euroopa Liidu toimimise lepingu (ELTL) sätetest.[227] Näiteks ELTL[228] artiklitest 36 ja 52 tuleneb, et riive on õigustatud kõlbluse, avaliku korra või avaliku julgeoleku seisukohalt, samuti inimeste, loomade või taimede elu ja tervise kaitsmiseks, sh rahvatervise kaitseks, kunstilise, ajaloolise ja arheoloogilise väärtusega rahvusliku rikkuse või tööstus- ja kaubandusomandi kaitsmiseks. Vastavalt Euroopa Kohut praktikale kuuluvad üldist huvi pakkuvate liidu eesmärkide hulka näiteks rahvusvaheline terrorismivastane võitlus rahvusvahelise rahu ja julgeoleku säilitamiseks.[229] Samuti kuuluvad selle hulka võitlus raske kuritegevuse vastu avaliku julgeoleku tagamiseks ning rahvatervise kaitse.[230] Üldisest huvist lähtuv eesmärk on näiteks ka harta artikliga 11 kaitstav sõna- ja teabevabadus.[231]

Järgnevalt tutvustatakse lähemalt põhilisemaid avaliku huviga seotud õiguspäraseid eesmärke kolmes grupis: 1) riiklik julgeolek, ühiskondlik turvalisus, avaliku korra rikkumine ning kuritegude ärahoidmine; 2) tervise ja kõlbluse kaitsmine ning 3) riigi majanduslik heaolu.

Esimese grupi kõige sagedasemad privaatsusõiguse rikkumist puudutavad kaasused on seotud kuritegude ennetamisega, eriti seoses politsei uurimistegevusega – pealtkuulamine,

[224] B. Sloot, lk 77.
[225] B. Sloot, lk 78.
[226] EIKo *Klass and Others vs Germany*, p 42.
[227] K. Lenaerts. Exploring the Limits of the EU Charter of Fundaments Rights. – European Constitutional Law Review. 2012/8, lk 391.
[228] Euroopa Liidu toimimise leping. http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.EST#C_2012326ET.01004701 (29.04.2016)
[229] EKo 3.09.2008, C-402/05 P ja C-415/05 P, *Kadi ja Al Barakaat International Foundation vs. nõukogu ja komisjon*, p 363. EKo 15.11.2012, C-539/10 P ja C-550/10 P, *Al-Aqsa vs. nõukogu*, p 130. EKo, 29.04.1999, C-293/97, *The Queen vs. Minister of Agriculture, Fisheries and Food, ex parte Standley jt.*
[230] EKo 23.11.2010, C-145/09, *Land Baden-Württemberg vs Panagiotis Tsakouridis*, punktid 46 ja 47.
[231] EKo 22.01.2016, C-283/11, *Sky Österreich*, p 52.

kirjavahetuse jälgimine, arreteerimine, läbiotsimine jne.[232] Korrakaitse eesmärk on olnud tavaliselt laiema ulatusega kui kuritegude ennetamine ning EIK on tunnustanud riigi õigustatud eesmärgina korrakaitset, kui puudub alus arvamaks, et eraellu sekkumisega hoitakse ära kriminaalne tegevus.[233] Ühiskondlik turvalisuse põhjendust privaatsusõiguse rikkumisel on kasutatud üsna harva ning seda üldisemate ning kaalukamate kaasuste puhul.[234]

EIK ei ole oma lahendites määratlenud, mis riiklikud julgeolekuhuvid täpsemalt on, kuid põhilisemad EIK kaasused selles valdkonnas viitavad sellele, et need on seotud ohtudega riigi julgeolekule ja demokraatlikule põhiseaduslikule korrale ning seda nii väliste kui sisemiste vaenlaste poolt.[235] Kohtuasjas Klass jt vs Germany märkis EIK järgmist: „Tänapäeval leiavad demokraatlikud ühiskonnad, et neid ähvardavad keerukad spionaaživormid ja terrorism, mille tõttu riik peab selle ohu vastu tõhusaks võitluseks olema suuteline varjatult jälgima tema territooriumil tegutsevaid riigikorda ohustavaid elemente. Seetõttu peab Kohus aktsepteerima, et mõni postisaadetiste varjatud läbivaatamise ning telegraafi ja telefoni teel edastavate sõnumite salajase pealtkuulamise volitusi andev õigusakt on erandtingimustel demokraatlikus ühiskonnas vajalik riigi julgeoleku huvides ja/või korratuse või kuriteo ärahoidmiseks.“.[236]

Kui terrorismivastase võitluse puhul keskendub julgeoleku või korrakaitseorganite tegevus ennetavatele meetmetele, siis igapäevane korrakaitse keskendub sageli juba toimepandud kuritegude uurimisele.[237] Lähtuvalt ennetustegevuse eesmärgist, on valitsused huvitatud nn andmekaevandamisest (*data mining*) ehk tehnoloogilise vahendi abil terroristide asukoha täpsest määratlemisest teiste inimeste seas.[238] Andmekaevandamisega kogutakse ning kombineeritakse isikuandmeid, millest luuakse profiilid ning seejärel analüüsitakse teatud käitumismustreid, mis tunduvad kahtlased.[239] See aitab ennustada, kes võiks järgmisena panna toime terroriakti.[240] Sealjuures on EIK pidanud vajalikuks julgeoleku huvides avaliku informatsiooni kogumist ja säilitamist vastavates registrites.[241] Kokkuvõtlikult on EIK pidanud erinevaid eraellu sekkumise meetmeid pidanud õigustatuks, sest need on teeninud riikliku

[232] B. Sloot, lk 79.
[233] B. Sloot, lk 78.
[234] B. Sloot, lk 78.
[235] S. Greer. The Exceptions to Articles 8 to 11 of the European Convention on Human Rights. Council of Europe, 1997, lk 19 http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf (25.03.2016)
[236] EIKo *Klass and Others vs Germany*, p 48.
[237] D. J. Solove. Data Mining and the Security-Liberty Debate. – The University of Chicago Law Review. 2008/75, lk 343.
[238] *Ibid*.
[239] *Ibid*.
[240] *Ibid*.
[241] EIKo *Leander vs Sweden*, p 59.

julgeoleku, ühiskondliku turvalisuse, avaliku korra rikkumise või kuritegude ärahoidmise eesmärki.

Tervise ja kõlbluse kaitse ettekäändel on riikide valitsused sekkunud eraellu eelkõige seoses lastekaitsega.[242] Tervisekaitsele on EIK praktikas tuginetud üsna vähestel juhtudel ning need juhtumid kuuluvad meditsiini valdkonda.[243] Näiteks kuuluvad nende hulka juhtumid, kus vaimuhaiguse tõttu on isik muutnud ohtlikuks iseendale ning ühiskonnale.[244] Riigipoolne eraellu sekkumine on loetud õigustuks ka juhul sadomasohistlike praktikate piiramisel lähtuvalt soovist kaitsta rahvatervist.[245] Moraalsetel ja kultuurilistel kaalutlustel on EIK lubanud ka ühiskonna vähemusgruppide õiguste piiramist, eelkõige seoses riigi positiivsete kohustustega.[246] Samuti on legitiimseks eesmärgina tunnustatud moraali kaitsmist olukorras, kus riik on sätestanud vanusepiirangu homoseksuaalsete harrastamiseks.[247] Kohus on pidanud moraalipõhimõtteid ning kohalikke traditsioone legitiimseteks eesmärkideks abordi, eutanaasia ning kehavälise viljastamise piiramise küsimustes.[248] EIK on põhimõtteliselt tunnistanud ka seda, et traditsioonilise pere toetamine ja julgustamine on iseenesest seaduslik ning isegi kiiduväärt eesmärk, kuid see ei tohi olla diskrimineerimise aluseks.[249]

Ka majanduslikku heaolu on EIK pidanud legitiimseks eesmärgiks mitmetele eraellu sekkumise juhtudel. Riigil on õigus piirata näiteks valuuta eksporti, sest see võib destabiliseerida riigi finantssüsteemi.[250] Samuti on peetud õigustatud elamute läbiotsimist ning arestimist seoses maksudest kõrvalehoidumisega ning terviseinfo jagamist sotsiaalkindlustusametiga, et hinnata sotsiaalkindluse poolt makstava kompensatsiooni vajalikust ning sobivust.[251] Järkjärgult on muutunud sellised põhjendused muutunud järjest olulisemaks, hõlmates üldjoontes kolme tüüpi juhtumeid. Esiteks, majanduslikku heaolu on peetud legitiimseks eesmärgiks immigratsiooni küsimustes, sest see puudutab rahvastiku tihedust ning tööjõu turgu.[252] Teiseks, majandusliku heaoluga on õigustatud juhtumeid, kus öised lennud rikuvad lennujaama läheduses elava inimeste öörahu ning elamupiirkonna lähedal asuvatest tehastest tulenev reostus vähendab

[242] B. Sloot, lk 81.
[243] *Ibid*.
[244] EIKo 5.07.1999, 31534/96, *Matter vs Slovakia*.
[245] B. Sloot, lk 81.
[246] *Ibid*, lk 82.
[247] *Ibid*.
[248] *Ibid*. EIKo 04.12.2007, 44362/04, *Dickson vs the United Kingdom*; EIKo 10.04.2007, 6339/05, *Evans vs the United Kingdom*.
[249] EIKo 13.06.1979, 6833/74, *Marcks vs Belgium*, p 40.
[250] B. Sloot, lk 83.
[251] *Ibid*.
[252] *Ibid*, lk 84.

elukvaliteeti.[253] Kolmanda tüübina on majanduslik heaolu legitiimse eesmärgina põhjendatud juhtudel, kui riigil on positiivne kohustus isiku eraelu kaitseks, kuid nende positiivsete kohustuste elluviimisega kaasnevad riigile olulised avaliku sektori raha kulutused.[254]

Need olid lühidalt peamised eesmärgid, mida on Euroopa Inimõiguste Kohus pidanud eraellu sekkumisel legitiimseteks eesmärkideks. Järgnevalt analüüsitakse seda, kuidas on Euroopa Inimõiguste Kohus ning Euroopa Kohus hinnanud eraellu sekkumise vajalikkust või proportsionaalsust, juhul kui riik sekkub isikute eraellu julgeoleku, kuritegude avastamise ja ärahoidmise või avaliku korra eesmärgil. Erilist tähelepanu pööratakse nendele kohtulahenditele, mis käsitlevad isikute salajast jälgimist, massijälgimist ning automaatset andmete kogumist.

2.4. Vajalikkuse ehk proportsionaalsuse test

Kuigi vajalikkuse või proportsionaalsuse põhimõtet ei ole Euroopa inimõiguste konventsioonis või selle lisaprotokollides sõnaselgelt mainitud, on EIK tunnustanud seda konventsiooni ühe olulisema printsiibina, mis aitab tagada konventsioonis sätestatud õiguseid ja vabadusi.[255] EIK on märkinud, et sekkumine vastab vajalikkuse kriteeriumile, kui riive vastab tungivale ühiskondlikule vajadusele (*pressing social need*), kui see on proportsionaalne soovitud legitiimse eesmärgi suhtes ning kui riigivõimu põhjused riive põhjendamiseks on asjakohased ning piisavad.[256] „Vajalikkus“ ei ole EIK praktika järgi samatähenduslik terminiga „asendamatu“, kuid sellel ei ole ka sellist paindlikkust, mis iseloomustab väljendeid nagu „lubatav“, „tavaline“, „kasulik“ või „mõistlik“.[257]

EIK on oma lahendites viidanud proportsionaalsusele kui mõistlikule suhtele vahendite ning soovitud eesmärkide vahel[258], mis aitab tagada õiglast tasakaalu konfliktsete erahuvi ning avaliku huvi vahel.[259] Näiteks kohtuasjas Leander vs Sweden[260] leidis EIK, et riiklike julgeolekuhuvide kaitsmist tuleb kaaluda võrreldes sellega, kui tõsine on sekkumine isiku

[253] B. Sloot, lk 84.
[254] *Ibid*, lk 84.
[255] J. McBride, Proportionality and the European Court of Human Rights. In The Principle of Proportionality in the Laws of Europe, edited by E. Ellis, 23–36. Oxford: Hart Publishing 1999, lk 23.
[256] EIKo *Leander vs Sweden*, p 58, EIKo *S and Marper vs the United Kingdom*, p 101.
[257] EIKo 25.03.1983, 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, *Silver and Others vs the United Kingdom*, p 97. EIKo 07.12.1976, 5493/72, *Handyside v. the United Kingdom*, p 48.
[258] EIKo 21.02.1986, 8793/79, *James and Others vs The United Kingdom*, p 50.
[259] EIKo *Peck vs the United Kingdom*, p 77.
[260] EIKo *Leander vs Sweden*, p 59.

eraellu. Ka kohtuasjas S. ja Marper vs United Kingdom märkis kohus, et tänapäeva teaduslike ja tehniliste vahendite kasutamisest tulenevaid kasusid kuritegevusega võitlemisel tuleb kaaluda võrreldes oluliste eraeluliste huvidega.[261] Proportsionaalsuse põhimõttest tuleneb ka see, et põhiõigusesse sekkumine ei tohiks kahjustada selle õiguse põhiolemust.[262] Proportsionaalsuse põhimõttega on loetud mittekooskõlas olevaks seda, kui riik ei ole teinud kõiki vajalikke korraldusi selleks, et tagada isiku õiguse kaitsmise efektiivsus.[263]

Proportsionaalsuse põhimõtet on nähtud seotuna EIK kohtupraktikas tunnustatud riikide kaalutlusõigusega (*margin of appreciation*)[264]. Seoses riikliku julgeolekuga on kohus märkinud, et riikidel on lai kaalutlusõigus või vabadus valimaks vahendeid, kuidas tagada riiklikku julgeolekut.[265] Sõltumata laiast kaalutlusõigusest, võib süsteemne salajane jälgimine kujutada ohtu demokraatiale, mistõttu peavad seaduses eksisteerima piisavad ning efektiivsed tagatised.[266] See ei tähenda, nagu oleks lepinguosalisel riigil piiramatu valikuvabadus kohaldada oma jurisdiktsiooni piires isikute varjatud jälgimist.[267] Kuivõrd sellised riigisisesed õigusaktid võivad seada demokraatliku ühiskonna selle kaitsmise põhjendusel ohtu või isegi hävitada, on EIK kinnitanud, et lepinguosalised riigid ei või spionaaži ja terrorismi vastu võitlemise nimel võtta vastu ükskõik milliseid meetmeid, mis nende arvates on sobivad.[268] Seega on riikidel jälgimismeetmete kasutusele võtmisel olemas kaalutlusõigus, kuid see ei tähenda, et see kaalutlusõigus on piiramatu.

Seda kaalutlusõigust piiravad eelkõige erinevad tagatised. Hindamaks, kas tagatised on piisavad ning tõhusad, sõltub võimalike meetmete olemusest, ulatusest, kestusest, nende meetmete määramiseks vajalikest põhjustest, lubamiseks pädevatest võimudest, nende meetmete teostamise ja järelevalve ning siseriikliku õigusega ettenähtud õiguskaitsevahenditest.[269] Sealjuures tuleb kindlaks teha, kas piiravate meetmete määramise ja rakendamise järelevalvekord suudab tagada, et õigusaktiga lubatud „sekkumine“ on selline, mis on „demokraatlikus ühiskonnas vajalik“.[270]

---

[261] EIKo *S and Marper vs the United Kingdom*, p 112.
[262] EIKo 17.10.1986, 9532/81, *Rees vs The United Kingdom*, p 50.
[263] EIKo *Marckx v. Belgium*, p 31.
[264] Selle põhimõtte sisuks on see, et riigisisestel kohtutel on ainuõigus tõlgendada ja rakendada riigisisest õigust üksikjuhtumile vastavalt kohalikele oludele (Y. Arai-Takahashi. The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR. Antwerpen: Intersentia 2002, lk 1-2).
[265] EIKo *Weber and Saravia vs Germany*, p 106; EIKo *Klass and Others vs Germany*, p 49.
[266] EIKo *Weber and Saravia vs Germany*, p 106.
[267] EIKo *Klass and Others vs Germany*, p 49.
[268] *Ibid*, p 49.
[269] *Ibid*, p 50.
[270] *Ibid*, p 54; EIKo *Weber and Saravia vs Germany*, p 117.

Kaalutlusõigus on kitsam olukorras, kus kaalul olev õigus ülioluline isiku isiklike või võtmetähendusega õiguste nautimiseks.[271] Riigi kaalutlusõigus on piiratud olukorras, kus kaalul on indiviidi olemasolu või tema identiteedi olulisemad küljed.[272] Nendel juhtudel, kui Euroopa Nõukogu liikmesriikidel ei ole ühist arusaama, mis need isikute huvid on olulised või kuidas neid parimal moel kaitsta, on riikide kaalutlusõigus suurem.[273] See kaalutlusõigus kuulub siiski Euroopa (EIK) järelevalve alla ning järelevalve puudutab nii seadusandlust kui otsuseid, mis sellel seadusandlusel põhinevad.[274] Kontrollimaks, kas riigivõim on ületanud oma kaalutlusõigust, hindab kohus meetme vastavust proportsionaalsuse põhimõttele.[275]

Olukordades, kus töödeldakse isikuandmeid automaatselt, on EIK leidnud, et garantiide või tagatiste olemasolu veelgi vajalikum, et vältida võimalikke väär- ja kuritarvitusi.[276] Risk kuritarvituseks on eriti kõrge juhul, kui julgeolekuteenistusel ja politseil on tehniliselt otsene ligipääs kõigile mobiiltelefoni kommunikatsioonile.[277] Riigisisene õigus peab tagama, et töödeldavad andmed on asjakohased ning ei ole liigsed võrreldes nende andmete hoidmise eesmärgiga.[278] Samuti tuleb tagada, et andmed on säilitatud vormis, mis lubab andmesubjekti teha kindlaks mitte kauemaks, kui perioodiks, mis on vajalik andmete kogumise eesmärkide saavutamiseks.[279]

Seoses isikute massilise jälgimisega on EIK tunnistanud, et on paratamatu, et praeguse aja terrorismiga võitlemiseks ning terroriaktide ennetamiseks kasutavad valitsused kaasaegset tehnoloogiat, sealhulgas infotehnoloogilisi lahendusi, millega on võimalik isikute massiline jälgimine.[280] Jälgimisvõimalused on viimastel aastatel oluliselt arenenud, lubades automaatset ning süsteemset andmekogumist, mistõttu on nende võimaluste tase on nii kõrge, et tavaline inimene ei suuda seda hoomata.[281] EIK hinnangul on seetõttu oluline see, kas jälgimismeetmete arenguga on kaasnenud ka sobivad tagatised inimeste kaitseks.[282] Teisisõnu viitab EIK sellele, et kui on võimalik massijälgimine, siis tagatised peaksid vastavalt riive intensiivsusele olema

[271] EIKo *S and Marper vs the United Kingdom*, p 102.
[272] *Ibid*.
[273] *Ibid*.
[274] EIKo *Szab and Vissy vs Hungary*, p 57.
[275] Y. Arai-Takahashi, lk 14.
[276] EIKo *S and Marper vs the United Kingdom*, p 103; EIKo 18.04.2013, 19522/09, *M.K. vs France*, p 32.
[277] EIKo 04.12.2015, 47143/06, *Roman Zakharov vs Russia*, p 302
[278] EIKo *S and Marper vs the United Kingdom*, p 103.
[279] *Ibid*.
[280] EIKo *Szab and Vissy vs Hungary*, p 68.
[281] *Ibid*.
[282] *Ibid*.

veelgi tugevamad. Sel põhjusel viitas EIK, et salajase jälgimise meetmed on lubatud üksnes siis, kui need on rangelt vajalikud (*strictly necessary*).[283] See tähendab esiteks seda, et salajane jälgimistegevus on kooskõlas konventsiooniga siis, kui see on demokraatlike institutsioonide kaitseks rangelt vajalik, ning teiseks seda, et see on rangelt vajalik ka konkreetsel üksikjuhtumil, nt konkreetse operatsiooni raames.[284]

Kuivõrd vajalikkuse ehk proportsionaalsuse testis on kohus märkinud, et tagatised on otseselt seotud sellega, kas sekkumine on demokraatlikus ühiskonnas vajalik[285], on kohus sageli hinnanud vajalikkust koos seaduslikkuse testiga, sest mõlemad nõuavad teatud tagatisi eraellu sekkumise juhtumiteks.[286] Näiteks kohtuasjas S. & Marper vs United Kingdom[287] märkis kohus, et seaduse kvaliteediga seotud reeglid, sh tagatised, on otseselt seotud sellega, kas sekkumine on demokraatlikus ühiskonnas vajalik.[288] Vajalikkuse hindamisel on EIK lisaks kuriteo olemusele, ajalistele piiridele ning andmete edastamise ja kasutamise tingimustele rõhku pööranud ka järelevalvesüsteemile ning isiku teavitamisele. Kokkuvõtlikult hindab EIK seda, kas sekkumine õigusesse on suurem, kui on vajalik soovitud eesmärgi saavutamiseks.[289]

Euroopa Liidu õiguses on proportsionaalsuse põhimõte sätestatud Euroopa Liidu põhiõiguste harta artiklis 52, mille kohaselt võib kohaselt piiranguid seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi. Proportsionaalsuse põhimõte sisustati Euroopa Kohtu poolt aga juba oluliselt varem, 1970ndatel aastatel kohtuasjas Internationale Handelsgesellschaft.[290] Proportsionaalsus on üks õiguse üldprintsiipe, mille eesmärgiks on olnud kaitsta üksikisikut Euroopa Liidu institutsioonide ja liikmesriikide tegevuse eest.[291]

Vastavalt Euroopa Kohtu väljakujunenud praktikale, nõuab proportsionaalsuse põhimõte, et liidu institutsioonide aktid oleksid vastava õigusaktiga taotletavate õiguspäraste eesmärkide saavutamiseks sobivad ega läheks kaugemale sellest, mis on nende eesmärkide saavutamiseks

[283] *Ibid*, p 73.
[284] *Ibid*, p 73.
[285] *Ibid*, p 78
[286] *Ibid*, p 58.
[287] EIKo *S and Marper vs the United Kingdom*, p 99.
[288] EIKo *Szab and Vissy vs Hungary*, p 78
[289] N. Taylor. Policing, Privacy and Proportionality. – European Human Rights Law Review. 2003, lk 3.
[290] J. Milaj. Invalidation of the data retention directive: extending the proportionality test. – Computer Law & Security Review 2015/31, lk 609. EKo C-11/70, *Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide*.
[291] J. Milaj, lk 610.

sobiv ja vajalik.[292] Juhul, kui on võimalik valida mitme sobiva meetme vahel, tuleb rakendada kõige vähem piiravat meedet, ning tekitatud piirangud või ebamugavused peavad olema vastavuses seatud eesmärkidega.[293] Proportsionaalsuse kohtuliku kontrolli osas on kohus märkinud, et liidu seadusandja kaalutlusõigus võib olla piiratud sõltuvalt reast teguritest, mille hulka kuuluvad asjassepuutuv valdkond, hartaga tagatud õiguse olemus, riive laad ja raskus ning riive eesmärk.[294]

Euroopa Kohus on seda printsiipi praktikas kasutanud erinevalt, sõltuvalt sellest, kas hinnatakse Euroopa Liidu või riigisiseseid meetmeid.[295] EL õiguse kehtivuse küsimustes on Euroopa Kohus hinnanud seda, kas meede on ilmselgelt ebaproportsionaalne (*manifestly inappropriate*).[296] Sealjuures peaks kohus kaaluma erahuve avalike huvidega.[297] Hinnates aga riigisisese meetme või akti kehtivust, mis mõjutab Euroopa Liidu mõnda põhivabadust, rakendab Euroopa Kohus rangemat testi ning hindab seda, kas liikmesriik oleks saanud vastu võtta vähem piiravama alternatiivi.[298] Sealjuures peab kohus kaaluma liidu huvisid riiklike huvidega ning seda kasutatakse integratsiooni mehhanismina, mille intensiivsus on palju tugevam.[299]

Seoses eraelu puutumatusega ning riivete proportsionaalsusega, on Euroopa Kohus tuginenud oma otsustes paljuski Euroopa Inimõiguste Kohtu praktikale. Seoses inimeste massilise jälgimisega tegi EK tõenäoliselt kõige olulisema otsuse kohtuasjas Digital Rights Ireland[300], mis puudutas elektroonilise side andmete (meta-andmete) säilitamist. Direktiivi 2006/24 osas võttis EK seisukoha, et see direktiiv kujutab endast eraelu ning isikuandmete kaitse põhiõiguste ulatuslikku riivet, mida tuleb pidada eriti raskeks.[301] Seda seetõttu, et direktiiv riivas peaaegu

---

[292] EKo 08.07.2010, C-343/09, *Afton Chemical Limited vs Secretary of State for Transport*, p 45; EKo 09.11.2010, C-92/09 ja C-93/09, *Volker und Markus Schecke ja Hartmut Eifert vs Land Hessen*, p 74; EKo 23.10.2012, C-581/10 ja C-629/10, *Nelson jt* vs *Deutsche Lufthansa AG*, punkt 71; EKo 22.01.2013, C-283/11, *Sky Österreich vs Österreichischer Rundfunk*, p 50.
[293] EKo 22.01.2013, C-283/11, *Sky Österreich vs Österreichischer Rundfunk*, p 50; EKo 12.07.2001, C-189/01, *Jippes jt*, p 81.
[294] EKo *Digital Rights Ireland*, p 47.
[295] J. Milaj, lk 610.
[296] *Ibid*.
[297] T. Tridimas. Proportionality in European Community Law: Searching for the Appropriate Standard of Scrutiny. In The Principle of Proportionality in the Laws of Europe, edited by E. Ellis, 65–84. Oxford: Hart Publishing 1999, lk 66.
[298] J. Milaj, lk 610.
[299] *Ibid*.
[300] EKo *Digital Rights Ireland*. Selle otsusega tunnistati kehtetuks Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, millega pandi üldkasutatavate elektroonilise side teenuste ja sidevõrkude pakkujatele kohustus säilitada mitte vähem kui kuue kuu ja kõige rohkem kahe aasta jooksul alates side toimumise päevast kommunikatsiooni liiklus- ja asukohaandmed.
[301] EKo *Digital Rights Ireland*, p 37.

kogu Euroopa elanikkonna põhiõigusi.[302] Riive olemuse kohta märkis EK, et eraelu puutumatuse põhiõiguse riive tuvastamisel ei ole oluline, kas edastatud isikuandmed on delikaatsed või mitte või kas asjaomased isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi.[303] Riivet kujutas endast nii andmete säilitamine kui ka pädevate riigisiseste asutuste juurdepääs nendele andmetele.[304] EK hinnangul võis asjaolu, et andmete säilitamine ja hilisem kasutamine toimuda isikut sellest teavitamata, tekitada isikutes tunde, et nende eraelu jälgitakse pidevalt.[305]

Kuigi Euroopa Liidu meetmete puhul on Euroopa Kohus tavaliselt kasutanud ilmselge ebaproportsionaalsuse testi, viitas Euroopa Kohus seekord kohtulahendile IPI[306] ja märkis, et eraelu puutumatuse kaitse nõuab, et isikuandmete kaitse erandite ja piirangute puhul tuleb piirduda rangelt vajalikuga.[307] Sealjuures tugines Euroopa Kohus muuhulgas analoogia korras Euroopa Inimõiguste Kohtu otsustele[308] ning märkis, et liidu õigusakt peab sätestama selged ja täpsed reeglid meetme ulatuse ja kohaldamise kohta ning kehtestama miinimumnõuded, nii et isikutel, kelle andmeid säilitatakse, oleksid piisavad garantiid, mis võimaldavad tõhusalt kaitsta nende isikuandmeid kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Garantiide olemasolu on EK hinnangul veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt, ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult.[309] Kuivõrd direktiiv 2006/24 ei sätestanud selgeid ja täpseid reegleid, mis oleksid reguleerinud harta artiklites 7 ja 8 ette nähtud põhiõiguste riive ulatust, ei olnud tagatud, et riive piirduks tõepoolest vaid vältimatult vajalikuga.[310]

Sisuliselt oli Euroopa Kohtu seisukoht väga sarnane Euroopa Inimõiguste Kohtu erinevate lahenditega. Kui Euroopa Kohus viitas kohtuasjas Digital Rights Ireland Euroopa Inimõiguste Kohtu lahenditele, siis teatud juhtudel on Euroopa Inimõiguste Kohus viidanud ka Euroopa Kohtu praktikale.[311] Mõlemad kohtud on näinud ohtu olukorras, kus kogutakse automaatselt massilises koguses kõigi isikute kohta andmeid, mistõttu on mõlemad kohtud näinud vajadust kehtestada selle väga täpsed tingimused ning pakkuda piisavaid tagatisi võimalike

[302] *Ibid*, p 56.
[303] *Ibid*, p 33.
[304] *Ibid*, p 34, 35.
[305] *Ibid*, p 37.
[306] EKo 07.11.2013, C-473/12, *IPI vs Geoffrey Englebert, Immo 9 SPRL, Gregory Francotte*, p 39.
[307] EKo *Digital Rights Ireland Ltd*, p 52.
[308] Kohus viitas järgmistele lahenditele: *Liberty jt vs. Ühendkuningriik, Rotaru vs. Rumeenia* ning *S ja Marper vs. Ühendkuningriik*.
[309] EKo *Digital Rights Ireland Ltd*, p 55.
[310] *Ibid*, p 65.
[311] Kohtuasjas EIKo *Szab and Vissy vs Hungary* viitas EIK Euroopa kohtuasjale EKo *Digital Rights Ireland Ltd*.

kuritarvitamise jaoks. Nagu eelnevalt märgitud sõltub see, kas tagatised on piisavad ning tõhusad, võimalike meetmete olemusest, ulatusest, kestusest, nende meetmete määramiseks vajalikest põhjustest, lubamiseks pädevatest võimudest, nende meetmete teostamise ja järelevalve ning siseriikliku õigusega ettenähtud õiguskaitsevahenditest.

Järgnevalt käsitletakse lähemalt seda, mida on Euroopa Inimõiguste Kohus ning Euroopa Kohus pidanud piisavateks tagatisteks või kaitsemeetmeteks tagamaks, et riik ei sekkuks üleliia eraellu ning oleks tagatud, et eraellu sekkumisest saadud andmeid ei kuritarvitataks.

2.4.1. Sekkumise aluseks oleva süüteo olemus

Euroopa Inimõiguste Kohtu hinnangul peab riigisisene õigus esmalt ette nägema täpse jälgimismeetmete rakendamise ulatuse, millest selgub, milliste süütegude puhul neid meetmeid võib kasutusele võtta ning kelle suhtes võib neid meetmeid kasutada.[312] Teisisõnu ei tohiks õigused andmete edastamiseks on olla õigustamatult laiad.[313] Samas ei tähenda see ka seda, et seaduses peaksid olema kõik süüteod ammendavalt loetletud, vaid olemas peaks olema kirjeldus nende süütegude põhilisest olemusest.[314] EIK hinnangul peaks strateegilise jälgimise raames kogutud informatsiooni edastama teistele ametiasutustele üksnes piiratud juhtudel, näiteks tõsiste kuritegude ennetamiseks või nende kuritegu eest süüdimõistmiseks.[315] Näiteks kohtuasjas M.K. vs France oli üheks põhjuseks, miks kohus pidas sõrmejälgede säilitamist ning kasutamist ebaproportsionaalseks, see, et sõrmejälgede andmebaasi kasutati kõiksuguste, sh vähetähtsate kuritegude lahendamiseks, sest kasutusotstarvet ei piiritletud tõsiste kuritegude või süüdistusega.[316]

Isegi, kui riigisiseses õiguses on määratletud, et pealtkuulamisi või muud salajast jälgimist võib teostada juhul, kui esineb oht riiklikule julgeolekule, peaks olema määratletud, millised sündmused või teod kujutavad sellist ohtu ning kas see oht on piisavalt tõsine, et õigustada salajast jälgimist.[317] Vastasel juhul jäetakse täidesaatvale võimule piiramatu otsustusõigus ise määratleda, mis kujutab ohtu riiklikule julgeolekule.[318]

[312] EIKo *Zakharov vs Russia*, p 243.
[313] EIKo *Weber and Saravia vs Germany*, p 123.
[314] EIKo *Zakharov vs Russia*, p 244; EIKo 18.05.2010, 26839/05, *Kennedy*, p 159.
[315] EIKo *Weber and Saravia vs Germany*, p 125-126.
[316] EIKo *M.K. vs France*, p 38.
[317] EIKo *Zakharov vs Russia*, p 248.
[318] *Ibid*.

Ka Euroopa Kohus on märkinud, et õigusaktis peavad olema objektiivsed kriteeriumid, mis võimaldaks tagada, et pädevatel siseriiklikel asutustel on andmetele juurdepääs ja nad saavad hiljem andmeid kasutada üksnes selliste kuritegude ennetamise, avastamise või kohtus menetlemise eesmärgil, mida võib harta artiklites 7 ja 8 ette nähtud põhiõiguste riive ulatust ja raskust arvestades pidada piisavalt rasketeks kuritegudeks, et õigustada sellist riivet. Olukord, kus viidatakse üldiselt rasketele kuritegudele, kuid raskete kuritegude sisustamine jäetakse liikmesriikide otsustada oma siseriiklikus õiguses, ei ole kooskõlas proportsionaalsuse põhimõttega.[319] Samuti on EK heitnud ette seda, et direktiiv 2006/24 ei nõudnud, et peaks olema üldse mingisugune seos säilitatavate andmete ning avaliku julgeoleku vahel.[320] Kokkuvõtlikult peab olukorras, kus toimub massiline või salajane jälgimine, olema andmete kogumine ja kasutamine piiritletud üksnes väga tõsiste kuritegudega ning riigisisene õigus peab selgelt defineerima, mida selliste kuritegude all mõeldakse, vältimaks liiga suurt kaalutlusõigust riigivõimu teostatavatele asutustele.

2.4.2. Ajalised piirangud ning isikute ringi piiritlemine

Periood, mille jooksul on lubatud jälgimistegevusi läbi viia või kui kaua võib jälgimisega saadud andmeid säilitada, mõjutab otseselt isiku eraellu sekkumise riive tugevust. EIK on leidnud, et pealtkuulamise kestuse võib jätta otsustada vastavale ametiasutusele, kellel on pädevus vastavaid volitusi väljastada ja pikendada, tingimusel, et on olemas piisavad tagatised.[321] Sellisteks tagatisteks on näiteks see, et seadus sätestab volituse aegumisaja, tingimused, millal volitust saab uuendada või pikendada ning millal tuleb volitus tühistada.[322]

Kohtuasjas M. K. vs France lubas siseriiklik õigus isikuandmete (sõrmejälgede) säilitamist 25 aastat.[323] Kuivõrd andmete kustutamise võimalus oli üksnes hüpoteetiline, mitte reaalne, leidis kohus, et seaduses sätestatud periood on tegelikult võrdsustatav tähtajatu perioodiga.[324] See oli üks põhjustest, miks EIK leidis, et ei ole leitud õiglast tasakaalu kaalul olevate avalike ja erahuvide vahel, mistõttu on eraellu sekkumine ebaproportsionaalne ja mittevajalik.[325]

[319] EKo *Digital Rights Ireland Ltd,* p 60.
[320] *Ibid,* p 58-59.
[321] EIKo *Roman Zakharov,* p 250.
[322] *Ibid*.
[323] EIKo *M.K. vs France,* p 42.
[324] *Ibid*.
[325] *Ibid,* p 43.

Samuti on EK selgitanud, et proportsionaalsuse põhimõttega on vastuolus olukord, kus õigusakt ei piira andmete säilitamist nende andmetega, mis kuuluvad kindlasse ajavahemikku.[326] Olukord, kus õigusakt kehtestab andmete säilitamise miinimumaja ning maksimumaja, kuid ei ole täpsustanud objektiivseid kriteeriume, mille alusel tuleks määrata andmete säilitamise aeg, sh tegemata vahet erinevatel andmeliikidel nende olulisuse või puudutatud isikute alusel, ei taga seda, et riive puhul piirdutakse vältimatult vajalikuga.[327] Teisisõnu peab riigisisene õigus ette nägema selged ajaperioodid, millal jälgimistegevusi võib teostada või kogutud andmeid säilida, ning kui ametiasutustele või liikmesriikidele antakse nende osas kaalutlusõigus, tuleb ette näha selged ning objektiivsed kriteeriumid selle kaalutlusõiguse teostamiseks.

Mõistliku andmete säilitamisperioodi kohta EIK on näiteks leidnud, et 6-kuuline ajapiir on mõistlik, kuid automaatselt hoiustatakse ka ebaolulisi andmeid, ei ole 6-kuuline tähtaeg õigustatud.[328] Kokkuvõtlikult peaksid ajavahemikud, mille jooksul on lubatud jälgimistegevusi läbi viia või kui kaua võib jälgimisega saadud andmeid säilitada, olema seadusega sätestatud ning need ajavahemikud peaksid olema mõistlikud. Võimalik on anda ajavahemik rakendava ametiasutuse otsustada, kuid sellisel juhul peaks seadus põhilised tingimused või piirid siiski seaduses sätestama.

Nii EIK kui ka EK on leidnud, et isikute ring, kelle suhtes jälgimismeetmeid läbi viiakse, peab olema selgelt määratletud. Kohtuasjas Digital Rights Ireland heitis Euroopa Kohus ette, et direktiiv 2006/24 riivas peaaegu kogu Euroopa elanikkonna põhiõigusi, ilma et oleks ette nähtud mingisugust eristamist, piirangut või erandit.[329] Sealjuures rakendati direktiivi ka nende isikutele, kelle kohta polnud mingeid tõendeid selle kohta, et nad oleksid seotud raskete kuritegude toimepanemisega või et nad võiksid muul põhjusel kaasa aidata raskete kuritegude ennetamisele, avastamisele või menetlemisele.[330] Olukord, kus andmeid kogutakse isikute kohta, kelle kohta pole mingeid tõendeid, mille põhjal võiks arvata, et nende käitumisel oleks kasvõi kaudne või kauge seos raskete kuritegudega, sh isikutele, kelle sideseansid kuuluvad siseriikliku õiguse kohaselt ametisaladuse alla, ei ole EK hinnangul kooskõlas

[326] EKo *Digital Rights Ireland Ltd*, p 59.
[327] *Ibid*, p 63-64.
[328] EIKo *Roman Zakharov*, p 253.
[329] EKo *Digital Rights Ireland Ltd*, p 56, 57.
[330] *Ibid*, p 58-59.

proportsionaalsuse põhimõttega.[331] Samuti peaks EIK hinnangul olema piiritletud see isikute ring, kellele võib need andmed avalikustada.[332]

Pealtkuulamisi võib läbi viia mitte üksnes kahtlustatava või süüdistatava suhtes, vaid ka isiku suhtes, kellel võib olla informatsiooni süüteo kohta või muud olulist informatsiooni seoses kriminaalasjaga.[333] Samas peaks riigisisene õigus või kohtupraktika piisavalt selgitama, kuidas rakendatakse või sisustatakse praktikas termineid „isik, kellel võib olla informatsiooni süüteo kohta“ või „isik, kellel võib olla muud olulist informatsiooni seoses kriminaalasjaga“.[334]

Weber & Saravia vs Germany kaasuses, mis puudutas strateegilist isikute telekommunikatsiooni jälgimist, leidis EIK, et nende isikute ring, kelle suhtes jälgimist teostatakse, on väga laialt defineeritud, mistõttu peab olema täidetud rida piiravaid tingimusi, enne kui eraellu sekkumise meetmeid kasutada saab.[335] Eeskätt peaks see olema lubatud üksnes väheste eriti tõsiste kuritegude ennetamiseks või avastamiseks.[336] Seega tuleb erinevaid tagatisi vaadata komplektis, mitte üksikuna, mis tähendab seda, et laiema hulga inimeste strateegiline jälgimine võiks olla lubatud üksnes juhul, kui teised tagatised, nt ajaperiood või kuritegude olemus, on väga kitsalt või rangelt piiritletud.

2.4.3. Tingimused andmete töötlemisele

Riigisisene õigus peab sätestama täpseid reegleid hoiustamise, kasutamise, edastamise ja hävitamise jaoks, et vähendada riski, et andmetele pääsetakse ligi ilma volituseta või avalikustatakse ilma loata.[337] EK peamised etteheited kohtuasjas Digital Rights Ireland olid muuhulgas seotud sellega, et direktiiv 2006/24 ei kehtestanud materiaal- ega menetlusõiguslikke tingimusi pädevate siseriiklike asutuste juurdepääsu suhtes andmetele ja nende hilisema kasutamise suhtes.[338] Sealhulgas ei sätestanud direktiivi 2006/24 sõnaselgelt, et andmetele juurdepääs ja andmete hilisem kasutamine peaksid olema rangelt piiratud eesmärgiga ennetada ja avastada täpselt piiritletud raskeid kuritegusid või viia läbi nendega seotud menetlusi. Selle asemel piirdus direktiiv sätestamisega, et iga liikmesriik kehtestab

[331] EKo *Digital Rights Ireland Ltd,* p 58, 69
[332] EIKo *Kennedy vs United Kingdom*, p 163.
[333] EIKo *Zakharov vs Russia*, p 245.
[334] *Ibid*.
[335] EIKo *Weber and Saravia vs Germany,* p 115.
[336] *Ibid*.
[337] EIKo *Roman Zakharov*, p 253.
[338] EKo *Digital Rights Ireland Ltd,* p 61.

menetluse, mida tuleb järgida, ja tingimused, mis peavad olema täidetud säilitatud andmetele juurdepääsu saamiseks vastavalt vajalikkuse ja proportsionaalsuse nõuetele.[339] Need ei olnud aga Euroopa Kohtu hinnangul piisavad juhised, vaid andmetele juurdepääsuks ning edastamiseks oleks pidanud kehtestama täpsed tingimused.

Samuti heitis Euroopa Kohus direktiivile 2006/24/EÜ ette seda, et see ei näinud ette ühtegi objektiivset kriteeriumi, mis võimaldaks piirata isikute arvu, kellel on andmetele juurdepääsu ja nende hilisema kasutamise luba, vastavalt sellele, mis on taotletava eesmärgi seisukohast vältimatult vajalik.[340] Sealjuures nägi EK puudusena seda, et nende andmetele ligipääs ei eeldanud kohtu või muu sõltumatu organi eelnevat luba ning direktiiv kohustanud liikmesriike sa selliseid piiranguid kehtestada.[341]

Strateegilise jälgimise raames saadud andmete edasiandmise osas on EIK nõustunud riigisisese kohtuga, et andmete edasiandmine teistele riigiorganitele peab toimuma tuginedes konkreetsetele faktidele, mis annavad selge aluse kahtluseks, et isik on toime pannud kuriteo (mitte lihtsalt märkidele, mis võivad viidata võimalikule seosele kuriteoga).[342] Kui on võimalik esitada jälgimise kohta kokkuvõte, siis tuleks eelistada kokkuvõtte esitamist algandmete edastamisele.[343]

EIK on piisavaks pidanud ka seda, et kui isik, kes otsustab andmete edastamise üle, on piisavalt kvalifitseeritud, tegemaks kindlaks tingimused, mille korral võib andmeid edastada.[344] Sealjuures on oluline ka kontrollisüsteemi olemasolu, tagamaks, et andmete edastamine vastas ette nähtud tingimustele.[345]

Euroopa kohtu hinnangul peavad selliste andmete säilitamiseks olema spetsiaalsed reeglid, mis oleksid kohandatud vastavalt direktiivi alusel säilitatavate andmete suurele hulgale, andmete delikaatsusele ja neile ebaseadusliku juurdepääsu ohule. Sellised reeglid peaksid eeskätt selgelt ja rangelt reguleerima kõnesolevate andmete kaitset ja turvalisust, et tagada andmete täielik terviklus ja konfidentsiaalsus.[346]

---

[339] EKo *Digital Rights Ireland Ltd,* p 61.
[340] *Ibid,* p 62.
[341] *Ibid*.
[342] EIKo *Weber and Saravia vs Germany,* p 127.
[343] EIKo *Kennedy vs United Kingdom,* p 163.
[344] EIKo *Weber and Saravia vs Germany,* p 128.
[345] *Ibid*.
[346] EKo *Digital Rights Ireland Ltd,* p 66.

Võrreldes Euroopa Inimõiguste Kohtuga on Euroopa Kohus käsitlenud ka vajadust tagada andmete kaitseks piisavad tehnilised meetmed. Kohtu hinnangul ei taganud direktiiv seda, et teenuste või võrkude pakkujad rakendaksid tehniliste ja korralduslike meetmetega eriti kõrge kaitse- ja turbetaseme, vaid lubab neil teenuste või võrkude pakkujatel võtta rakendatava turbetaseme kindlaksmääramisel arvesse majanduslikke kaalutlusi seoses turbemeetmete rakendamise kuludega.[347] Sealjuures oli kohus seisukohal, et direktiiv 2006/24/EÜ ei taga andmete pöördumatut hävitamist pärast säilitamistähtaja lõppu.[348]

2.4.4. Järelevalvesüsteem ja isiku teavitamine

Kaheks väga oluliseks tagatiseks isiku õiguste kaitsel on tõhusa järelevalvesüsteemi olemasolu ning isiku teavitamine tema suhtes kasutusevõetud meetmest ehk isiku teavitamine tema põhiõiguste riivest.

Järelevalvesüsteemidest on kõige klassikalisem kohtulik järelevalve, kuid selle kõrval või asemel võib rakendada ka teisi järelevalvesüsteeme, näiteks õiguskantsleri või parlamendi ombudsmani järelevalvet, erinevaid järelevalvekomisjone, sh parlamendiliikmete osalusega komisjone, justiitsministri järelevalvet jne.[349] Jälitustegevust või jälgimismeetmeid võib kontrollida kolmes staadiumis: kui otsustatakse jälitustegevust alustada, jälitustegevuse ajal või pärast selle lõpetamist.[350] Esimese kahe staadiumi puhul on salajase jälitustegevuse jaoks väga loomulik ja loogiline määrata, et nii jälitustegevus ise kui ka selle kontroll toimub isiku teadmata.[351] Sellisel juhul ei saa isik omal algatusel taotleda tõhusat õiguskaitsevahendit või osaleda otseselt kontrollimenetluses, mistõttu on oluline, et kehtestatud kord suudaks ise tagada isiku õiguste piisava ja võrdse kaitse.[352] Oluline on, et järelevalvesüsteem aitaks tagada, et sekkumine on üksnes selline, mis on demokraatlikus ühiskonnas vajalik.[353]

Sellistes valdkonnades, kus õiguste kuritarvitamine on üksikjuhtudel väga kergesti võimalik ning võib kaasa tuua demokraatlikule ühiskonnale tervikuna kahjulikke tagajärgi, on soovitatav

[347] EKo *Digital Rights Ireland Ltd,* p 67.
[348] *Ibid*.
[349] EIKo *Leander vs Sweden,* p 62.
[350] EIKo *Klass and Others vs Germany,* p 55.
[351] *Ibid*.
[352] *Ibid*.
[353] EIKo *Weber and Saravia vs Germany,* p 117.

usaldada kontroll kohtunikule.[354] Seaduse ülimuslikkusest tuleneb, et täitevvõimu sekkumist isiku õigustesse tuleb tõhusalt kontrollida ning tavaliselt tagab selle kohtunik (kohtulik kontroll), pakkudes parimaid sõltumatuse, erapooletuse ja õiglase menetluse tagatisi.[355] Näiteks on täiendav kohtulik kontroll on vajalik eelkõige siis, kui ametiasutustele on antud lai kaalutlusõigus või tõlgendusvabadus, kelle suhtes jälgimismeetmeid kasutada.[356]

Kohtuasjas Szab and Vissy vs Hungary heitis EIK ette seda, et jälitustegevuseks andis loa justiitsminister ning kohtul puudus võimalus hinnata, kas jälitusmeetmed olid kooskõlas rangelt vajaliku põhimõttega.[357] Kohtu hinnangul võib konventsiooniga olla kooskõlas olukord, kus loa pealkuulamiseks annab kohtuväline organ, kuid seda üksnes tingimusel, see organ on sõltumatu täitevvõimust ning sellel organil piisavalt võimu ning pädevust teostada tõhusat ning pidevat kontrolli.[358] Alternatiivselt peaks see õigus olema kohtul.[359] Igasugune poliitilise iseloomuga loa andmine ning jälgimine suurendab riski, et meetmeid kuritarvitatakse, mistõttu võib eeldada, et poliitiline isik nagu justiitsminister ei suuda anda piisavalt tagatisi.[360] Kohtulik kontroll aitab tagada kodanike usaldust õigusriigi tagatiste vastu ning heastada võimalikke kuritarvitusi.[361] EIK hinnangul ei saa ülehinnata kohtuliku kontrolli väärtust võttes arvesse, millistes tohututes kogustes on ametiasutustel võimalik saada informatsiooni ning seda töödelda peaaegu kõigi isikute kohta.[362]

EIK on märkinud, et eelnev (*ex ante*) volituse andmine ei ole ilmtingimata vajalik, kui on olemas tugev kohtulik järelkontroll, mis võib tasakaalustada algse volituse andmise puudujääke.[363] Kohtuasjas Szab and Vissy vs Hungary tunnistas EIK, et praegusele terrorismiohule on iseloomulik, et ootamatult võivad esile kerkida hädaolukorrad, kus eelneva kohtuloa taotlemine ei ole võimalik või on ebaefektiivne.[364] Siiski märkis EIK, et isegi kui need ekstreemsed hädaolukorrad esinevad, peab olema tagatud *post factum* kohtulik kontroll. Samuti peavad need õigusaktid, mis lubavad erakorralist (hädaolukorras) jälgimist või pealtkuulamist, sätestama täpsed kriteeriumid, milliseid juhtumeid loetakse erakorraliseks jälgimiseks ning kui

[354] EIKo *Klass and Others vs Germany*, p 56.
[355] *Ibid*, p 55.
[356] EIKo *Szab and Vissy vs Hungary*, p 73.
[357] *Ibid*, p 75.
[358] *Ibid*, p 77. EIKo *Klass and others vs Germany*, p 56.
[359] EIKo *Szab and Vissy vs Hungary*, p 77.
[360] *Ibid*, p 77.
[361] *Ibid*, p 79.
[362] *Ibid*, p 79.
[363] *Ibid*, p 77; EIKo *Kennedy*, p 167.
[364] EIKo *Szab and Vissy vs Hungary*, p 80.

kaua selliseid tegevusi võib läbi viia.[365] Teatud juhtudel on eelnev kontroll siiski hädavajalik, näiteks olukordades, kus salajane jälgimine on suunatud ajakirjanduse suhtes, sest tagant järele kontroll ei saa taastada ajakirjanike allikate konfidentsiaalsust.[366]

Isegi kui siseriiklikus korras on ette nähtud eelnev kohtulik kontroll, peab selline kohtulik kontroll vastama teatud tingimustele. Kohtul peaks olema sisuline pädevus hinnata (koos tõenditega), kas esineb tõepoolest põhjendatu kahtlus, et isik on süüteo toime pannud, või kas taotletud meede on kooskõlas vajalikkuse ja proportsionaalsuse nõudega.[367] EIK hinnangul on olukorrad, kus peaaegu kõik kohtunike poolt antud loa taotlused pealtkuulamiseks on heaks kiidetud ja seaduses ei ole sätestatud, et jälitustoiminguid võib teostada üksnes juhul, kui teiste meetoditega on võimatu taotletavaid eesmärke saavutada, „murettekitavad".[368] Pealtkuulamise loa andmisel peab kohus selgelt määratlema need isikud, kes jälgimise alla seatakse, identifitseerides need kas nimede, aadresside, telefoninumbrite või muu olulise informatsiooni alusel.[369]

Olukorras, kus puudub kohtulik kontroll, on EIK ette heitnud ka parlamentaarse komitee kontrolli puuduseid. Näiteks on puuduseks see, kui parlamentaarse kontrolli menetlus ei võimalda üksikisikule kuritarvitamise heastamist.[370] Üheks kontrollivahendiks on ka aruannete esitamine parlamendile. Selles osas on EIK leidnud, et kui neid aruandeid ei avalikustata, siis ei taga see avalikkuse kontrolli, mis on üheks kuritarvitamise vältimise tagatiseks.[371] Seda, kas järelevalvemeetmed on ka praktikas efektiivsed, peab suutma näidata riik.[372]

Euroopa Liidu õigusest tuleneb, et andmekaitse ja andmeturbega seotud nõuete täitmist kontrollib eraldi sõltumatu asutus,[373] kelleks on riiklikud andmekaitse inspektsioonid. Sõltumatute järelevalveasutuste loomine liikmesriikides on seega oluline tegur üksikisikute kaitsmisel seoses isikuandmete töötlemisega.[374] Liikmesriikide järelevalveasutuste ülesanne on hoolitseda selle eest, et isikuandmete kaitse tagamiseks oleksid tasakaalus ühelt poolt eraelu

[365] EIKo *Roman Zakharov*, p 266.
[366] EIKo 22.11.2012, 39315/06, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands*, p 101; EIKo *Kopp v. Switzerland.*
[367] EIKo *Roman Zakharov*, p 262.
[368] EIKo 24.09.2009, 25198/02, *Iordachi and Others v. Moldova,* p 51.
[369] EIKo *Roman Zakharov*, p 264.
[370] EIKo *Szab and Vissy vs Hungary*, p 82.
[371] EIKo *Roman Zakharov*, p 283; EIKo *Szab and Vissy vs Hungary*, p 82.
[372] EIKo *Szab and Vissy vs Hungary*, p 88.
[373] EKo *Digital Rights Ireland Ltd*, p 68.
[374] EKo 16.10.2012, C-614/10 *European Commission vs Austria*, p 37.

puutumatuse kui põhiõiguse austamine ja teiselt poolt huvid, mida teenib isikuandmete vaba liikumine.[375]

Isiku teavitamine jälgimismeetmetest või jälitustoimingutest on lahutamatult seotud õiguskaitsevahendite kasutamise efektiivsusega, mida tuleb vaadata koos olemasoleva järelevalvesüsteemiga.[376] Olukorras, kus puudub tugev ning tõhus järelevalvesüsteem, on oluline roll just isiku teavitamisel. Kui pärast jälitustoimingu tegemist ei teavitada seda isikut jälitustoimingu tegemisest, ei saa need isikud ennast efektiivselt kohtutes kaitsta.[377] Küsimuse osas, kas pärast jälitustoimingute teostamist peaks isikut tingimata sellest teavitama, on EIK märkinud, et hilisem teatamine igale isikule, kelle suhtes kohaldatud meede on lõpetatud, võib ohustada jälitustegevuse pikaajalist eesmärki, mistõttu on teatud juhtudel teavitamata jätmine õigustatud.[378] Selline teavitamine võib näiteks paljastada luureteenistuse töömeetodid ning tegevusalad.[379] Samas on EIK märkinud, et kui isiku teavitamine enam jälitustegevuse eesmärki ei ohusta, tuleks selle isikule jälitustegevuse kohta informatsiooni anda.[380]

Samas nõustus EIK samas kohtuasjas (Weber & Saravia vs Germany) Saksamaa Föderaalse Konstitutsioonikohtuga, et teavitamata jätmine on õigustatud ka siis, kui inimese kohta on andmed kogutud, kuid kolme kuu jooksul neid andmeid ei kasutatud ning need kustutati.[381] See tundub minema vastuollu EIK varasema seisukohaga, mille kohaselt juba andmete kogumine ja hoidmine kujutab endast olulist riivet eraellu ning nende andmete kasutamine kujutab endast täiendavat riivet. Näiteks kohtuasjas S & Marper ei nõustunud kohus Saksamaa väitega, et kui andmeid DNA kohta ei kasutata (ei leita vastet), siis ei mõjuta see kuidagi seda isikut, kelle DNA koht infot hoitakse.[382] Kui isikut ei pea teavitama juhtudel, kui andmeid ei kasutatud ning kui teavitamine võib seada ohtu uurimise eesmärgi, tekib küsimus, millistel juhtudel siis üldse teavitamine aset leiab.

Teavitamiskohustuse või -võimaluse hindamise puhul on kohus arvesse võtnud ka seda, kas isikul on reaalselt võimalik saada ametiasutustelt informatsiooni selle kohta, kas teda on pealtkuulatud või muid jälitustoiminguid teostatud.[383] Samuti tuleb teavitamiskohustuse juures

[375] EKo 06.10.2016, C-362/14, *Schrems vs Data Protection Commisioner*, p 42.
[376] EIKo *Weber and Saravia vs Germany*, p 135.
[377] EIKo *Klass and Others vs Germany*, p 57.
[378] *Ibid*, p 58.
[379] EIKo *Weber and Saravia vs Germany*, p 135.
[380] *Ibid*, p 135, EIKo *Klass and Others vs Germany*, p 58.
[381] EIKo *Weber and Saravia vs Germany*, p 136.
[382] EIKo *S and Marper vs the United Kingdom*, p 121.
[383] EIKo *Roman Zakharov*, p 290.

hinnata seda, kas isikul on võimalik kasutada õiguskaitsevahendeid ametiasutuste suhtes, kes on isikut õigusliku aluseta pealtkuulanud, kuid mille kohta ei ole isikul võimalik esitada faktilisi tõendeid, et pealkuulamine tõesti toimus.[384]

EIK praktikast ei tulene aga selgelt lahendust olukorrale, kui pole selget kindlust selles osas, kas seaduses sätestatud piirangud või tingimused ka tegelikult efektiivset kaitset võimaldavad. Näiteks kohtuasjas Klass leidis EIK, et vastavas riigisiseses seaduses olid tagatised olemas, kuid puudus informatsioon teistsugusest rakenduspraktikast, mistõttu leidis kohus, et isegi kui võimalikku kuritarvitamist ei ole võimalik täielikult välistada, tuleb eeldada, et ametivõimud kohaldavad seadust õigesti.[385] Selline seisukoht teeb murelikuks seetõttu, et kui üksikisikul ei ole võimalik tõendada riigiasutuste poolset seaduse rikkumist, ei ole võimalik ka tõendada seda, et isiku eraellu tungitakse põhjendamatult. Olukorras, kus isik pole jälitustegevusest teadlik ning teda ei teavitatagi, ei ole isikul seda ka kuidagi võimalik tuvastada ning võimalik võimudepoolne kuritarvitamine jääb avastamata. Seega on inimeste teavitamine väga oluline tagatis ning seda eelkõige olukorras, kus puuduvad tugevad järelevalvemehhanismid.

Kokkuvõtlikult on nii Euroopa Inimõiguste Kohus kui ka Euroopa Kohus pidanud vajalikuks jälgimise proportsionaalsuse puhul hinnata, kas piiravate meetmete määramise ja rakendamise järelevalvekord suudab tagada, et õigusaktiga lubatud sekkumine on selline, mis on demokraatlikus ühiskonnas rangelt vajalik. Nii Euroopa Kohtu kui ka Euroopa Inimõiguste Kohtu praktika kohaselt peavad massilise ja automaatse jälgimise korral olema riigisiseses õiguses määratletud selged tingimused ning kaalutlusõiguse piirid. Sealjuures peavad olema piisavad tagatised kuritarvitamiste vältimiseks. Eelkõige tuleks piiritleda kitsalt süüteo olemus, millal on lubatud jälgimismeetmeid kasutada. Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikast kumab sealjuures läbi põhimõte, et jälgimismeetmeid ja selle teel saadud andmeid on põhjendatud kasutada üksnes tõsiste kuritegude lahendamiseks. Lisaks on oluline piiritleda isikute ring, kelle suhtes jälgimismeetmeid kasutatakse ning isikute ring, kes võivad kogutud andmetele ligi pääseda. Oluline on piirata ka meetmete ajalist kestust, mille jooksul võib isikuid jälgida ning kogutud andmeid säilitada või kasutada, sest see mõjutab otseselt riive intensiivsust. Kuritarvitamiste ärahoidmiseks peavad olema ka selged protseduurireeglid jälgimisega saadud andmete hoiustamise, kasutamise, edastamise ja hävitamise jaoks. Lisaks

[384] EIKo *Roman Zakharov*, p 295-298.
[385] EIKo *Klass and Others vs Germany*, p 58-59.

eelnevale on tõenäoliselt kõige olulisemateks tagatisteks ka piisava järelevalvesüsteemi olemasolu ning isikute teavitamise kohustus.

Need põhimõtted võivad leida olulist täiendust juba lähiajal. Nimelt on Euroopa Kohtus kui ka Euroopa Inimõiguste kohtus menetluses mitu olulist kohtuasja. Rootsi apellatsioonikohus esitas 4. mail 2015 eelotsuse taotluse Euroopa Kohtule kohtuasjas Tele2 Sverige AB versus Post- och telestyrelsen[386], milles palus vastust küsimusele, kas üldine kohustus säilitada kuritegevuse vastu võitlemise eesmärgil andmeliiklusandmeid, mis hõlmavad eranditult kõiki isikuid, seadmeid ja andmeid on kooskõlas põhiõiguste harta ning proportsionaalsuse põhimõttega. 28. detsembril 2015 esitas eelotsuse taotluse Ühendkuningriikide apellatsioonikohus kohtuasjas Davis jt[387], milles palus sisuliselt vastust küsimustele, kas liikmesriigid on kohustatud elektroonilise side andmete kasutamisel lähtuma kohtuasjas Digital Rights Ireland tehtud otsusest ning kas see kohtuotsus laiendab eraelu kaitseala EL põhiõiguste hartas EIÕK artikliga 8. Seega on tulemas kaks väga olulist elektroonilise side andmete säilitamist puudutavat otsust, mis peaksid veelgi täpsemalt selgitama, millistel tingimustel loetakse elektroonilise side andmete säilitamist ning kasutamist proportsionaalseks meetmeks.

Euroopa Inimõiguste Kohtus on menetluses taotlus kohtuasjas Big Brother Watch and Others v. The United Kingdom[388], milles survegrupp Big Brother Watch väidab, et Ühendkuningriikide julgeolekuteenistus on nende kommunikatsiooni jälginud (sh jälgimisprogrammi TEMPORA abil) ilma piisava õigusliku aluseta ning on saanud sarnast informatsiooni ka USA Riiklikult Julgeolekuagentuurilt NSA. See taotlus on otseselt tingitud Edward Snowdeni poolt avalikustatud informatsioonist. Seega on oodata privaatsusõiguse piiramise õiguslikku raamistiku lähiaastatel olulist täiendust.

[386] EK C-203/15, *Tele2 Sverige AB versus Post- och telestyrelsen*, eelotsuse taotlus.
[387] EK C-698/15, *Davis jt*, eelotsuse taotlus.
[388] EIK taotlus nr 58170/13, *Big Brother Watch and Others v. The United Kingdom*.

3. ELEKTROONILISE SIDE ANDMETE SÄILITAMISE REGULATSIOON EESTIS

Järgnevalt käsitletakse elektroonilise side andmete säilitamise kohustust elektroonilise side seaduse (ESS) § 111[1] alusel, olles näide sellest, kuidas toimub Eestis suures ulatuses andmete kogumine ja säilitamine, mida kasutavad erinevatel eesmärkidel mitmed riigiasutused. Selle regulatsiooni käsitlemine on oluline seetõttu, et kuigi see regulatsioon kehtestati direktiivi 2006/24/EÜ ülevõtmiseks, mille Euroopa Kohus tunnistas 8. aprillil 2014. aastal kohtuasjas Digital Rights Ireland[389] kehtetuks, ei ole Eesti õiguses direktiivi ülevõtvaid sätteid kehtetuks tunnistatud. Direktiivi kehtetuks tunnistamine ei too automaatselt kaasa ka ESS ja muude õigusaktide vastavate sätete kehtetust.[390]

Kuigi õiguskantsler on varasemalt analüüsinud elektroonilise side seaduse § 111[1] vastavust põhiseadusele[391] ning on leidnud, et andmete ennetava kogumise ja säilitamise regulatsioon, nagu see on ette nähtud ESS §-s 111[1], ei ole selgelt ebamõõdukas ja ei ole seega ka põhiseadusega vastuolus, on käesolevas töös siiski vajalik seda regulatsiooni põhjalikumalt analüüsida. Eelkõige seetõttu, et õiguskantsler pidas esmalt võimalikuks hinnata sideandmete töötlemise põhiseaduspärasust üksnes osas, mis puudutab andmete kogumise ja säilitamise võimalikkust sideettevõtja juures, märkides, et sel hetkel ei olnud võimalik anda lõplikku hinnangut regulatsiooni osa kohta, mis käsitleb sideandmete nõudmist avaliku võimu asutuste poolt ja nende edasise töötlemise põhiseaduspärasust (sh menetluslike garantiide küllaldasust).[392] 22.04.2016 lisandus õiguskantsleri täiendav seisukoht, mis täiendas õiguskantsleri esimest seisukohta ning puudutas kogutud andmete kasutamist.[393] Selles seisukohas jõudis õiguskantsler seisukohale, et läbi viidud abstraktne põhiseaduslikkuse analüüs ei võimaldanud teha järeldust ESS § 111[1] ja muude normidega ette nähtud sideandmete säilitamise ning edasise töötlemise süsteemi vastuolu kohta põhiseadusega, märkides siiski, et kehtiv sideandmete töötlemise regulatsioon on ebaühtlane ja lünklik ning tuleb terviklikult üle vaadata.[394] Sellegi poolest on regulatsiooni põhjalikum analüüsimine vajalik põhjusel, et

[389] EKo *Digital Rights Ireland*.
[390] RKKKKo 3-1-1-51-14, p 21.
[391] Õiguskantsleri seisukoht elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta, 20.07.2015. http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf (15.04.2016), lk 10.
[392] Õiguskantsleri seisukoht 2015, lk 2.
[393] Elektroonilise side seaduse § 111[1] alusel sideandmete töötlemise põhiseaduspärasus. 22.04.2016. http://oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (29.04.2016).
[394] Õiguskantsleri seisukoht 2016, lk 1 ja 12.

õiguskantsleri esitatud analüüsi esimeses ega teises osas esitatud seisukohad ei ole veenvad. Sellisel seisukohal on olnud õiguskantsleri esimese analüüsi osas ka Uno Lõhmus.[395] Oma artiklis analüüsis Uno Lõhmus[396] ESS §-s 111[1] võimalikku kooskõla põhiseadusega Digital Rights Ireland kohtuotsuse valguses, kuid see ei sisaldanud põhjalikumat garantiide analüüsi vastavalt nii Euroopa Kohtu kui ka Euroopa Inimõiguste Kohtu praktikale.

Järgnevalt analüüsitakse seda, milliseid tagatisi pakub Eesti õigus sellele meetmetele ning kuidas see vastab Euroopa Inimõiguste Kohtu ning Euroopa Kohtu sätestatud tingimustele. Seega ei ole käesoleva analüüsi eesmärgiks põhjalikult analüüsida selle põhiseaduspärasust, nagu näeb ette Eesti väljakujunenud kohtupraktika kolmeastmelisest proportsionaalsuse hindamise testis, vaid keskendutakse Eesti regulatsiooni hindamisele lähtuvalt eelmises peatükis väljatoodud tingimustele.

Aga enne veel kui minna sisulise analüüsi juurde, tutvustatakse mõne sõnaga elektroonilise side andmete regulatsiooni. Elektroonilise side seaduse § 111[1] paneb sideettevõtjatele kohustuse säilitada kommunikatsiooni liiklus- ja asukohaandmeid ühe aasta jooksul alates side toimumise ajast. Säilitatavate andmete hulka kuuluvad erinevad meta-andmed telefoni- ja mobiiltelefoni teenuste kasutamise kohta ning interneti-ühenduse, elektronposti ja interneti-telefoni teenuste kasutamise kohta.[397] Päringud sideettevõtjale võivad seega ESS §-i 111[1] järgi hõlmata erinevaid sideandmeid, nagu andmeid kliendi nime, asukoha või sideseansside sageduse kohta.

Nagu eelnevalt märgitud, kehtestati elektroonilise side andmete säilitamise kohustus elektroonilise side andmete direktiivi 2006/24/EÜ ülevõtmiseks. Direktiivi 2006/42/EÜ põhjenduspunkti 9 alusel oli elektroonilise side andmete säilitamine osutunud vajalikuks ja tõhusaks õiguskaitsevahendiks mitmes liikmesriigis toimunud uurimiste käigus, eriti selliste raskete juhtumite puhul nagu organiseeritud kuritegevus ja terrorism, mistõttu oli tekkinud vajadus säilitatud andmete kättesaadavuseks õiguskaitseasutustele teatava ajavahemiku jooksul. Nagu ülalpool käsitletud, leidis Euroopa Kohus kohtuasjas Digital Rights Ireland, et direktiiv piirab ebaproportsionaalselt Euroopa Liidu põhiõiguste harta artikleid 7 ja 8, mis sätestavad eraelu ja isiku andmete kaitse. Euroopa Kohtu[398] hinnangul võimaldavad need andmed teha väga täpseid järeldusi selliste isikute eraelu kohta, näiteks nende igapäevaelu

[395] U. Lõhmus 2015, lk 741.
[396] U. Lõhmus 2015.
[397] ESS § 111[1] lg-d 2 ja 3.
[398] EKo *Digital Rights Ireland*, p 27.

harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad.

Elektroonilise side andmete põhiregulatsioon asub elektroonilise side seaduses, kuid nendele andmetele ligipääsu ning kasutamist puudutavad sätted on ka teistes õigusaktides, näiteks kriminaalmenetluse seadustikus[399] (KrMS), julgeoleku asutuste seaduses[400] (JAS), väärteomenetluse seadustikus[401] (VTMS), väärtpaberituru seaduses[402] (VPTS), kaitseväe korralduse seaduses[403] (KKS), maksukorralduse seaduses[404] (MKS), politsei ja piirivalve seaduses[405] (PPVS), relvaseaduses[406] (RelvS), strateegilise kauba seaduses[407] (StrKS), tolliseaduses[408] (TS), tunnistajakaitse seaduses[409] (TuKS), turvaseaduses[410] (TurvS), vangistusseaduses[411] (VangS), välismaalaste seaduses[412] (VMS), korrakaitseseaduses[413] (KorS) ning isikuandmete kaitse seaduses[414] (IKS). Järgnevalt hinnatakse ESSis ja teistes seadustes olevaid tagatisi lähtuvalt Euroopa Inimõiguste Kohtu ning Euroopa Kohtu praktikast tulenevatest nõuetest piisavatele tagatistele: süüteo olemus, isikute ring, ajaline piir, järelevalvesüsteem, teavitamine ning edastamisele, hoidmisele, kasutamisele ning hävitamisele sätestatud protseduurireeglid.

3.1. Süüteo olemus

Võrreldes direktiiviga 2006/24/EÜ sätestab ESS säilitatavate andmete kogumise ja kasutamise oluliselt laiematel eesmärkidel kui direktiiviga taotletud vahetu raskete kuritegude tõkestamine ja menetlemine. ESS § 111^1 lg 11 p-d 1–6 ning eelnevalt viidatud eriseadused kohustavad sideettevõtjaid edastama säilitatavaid andmeid pädevatele asutustele kuritegude avastamiseks, tõkestamiseks ja menetlemiseks, riigi julgeoleku ja põhiseadusliku korra tagamiseks, kõrgendatud ohu väljaselgitamiseks või tõrjumiseks, väärtegude menetlemiseks, riikliku

[399] RT I, 06.01.2016, 19.
[400] RT I, 17.12.2015, 38.
[401] RT I, 19.03.2015, 37.
[402] RT I, 14.11.2015, 2.
[403] RT I, 12.03.2015, 19.
[404] RT I, 09.02.2016, 3.
[405] RT I, 31.12.2015, 28.
[406] RT I, 19.03.2015, 19.
[407] RT I, 12.03.2015, 48.
[408] RT I, 10.11.2015, 4.
[409] RT I, 29.06.2012, 46.
[410] RT I, 30.12.2015, 53.
[411] RT I, 23.03.2015, 141.
[412] RT I, 17.12.2015, 14.
[413] RT I, 23.03.2015, 207.
[414] RT I, 06.01.2016, 10.

järelevalve teostamiseks (finantsjärelevalve teostamiseks, isikuandmete kaitse alase järelevalve teostamiseks) tsiviilkohtumenetluses otsuse tegemiseks, kriminaalmenetluse väliste toimingute tegemiseks (kuritegude ärahoidmiseks ning tagaotsitavaks kuulutamise määruse täitmiseks) ning isikute julgeoleku- ja taustakontrolli teostamiseks. Kuivõrd Eesti õigus sisaldab mitmeid erinevaid eesmärke nende andmete kogumiseks ning kasutamiseks, käsitletakse neid eesmärke järgnevalt eraldi.

ESS § 111^1 lg 11 p 1 alusel kogutakse ning kasutatakse elektroonilise side andmeid kriminaalmenetluses tõe välja selgitamiseks või kuritegude tõkestamiseks. Sealjuures ei eristata kuritegusid nende raskusastme järgi, vaid ESS ja KrMS võimaldavad nõuda andmete edastamist mistahes kuriteo menetlemiseks.[415] See ei ole kooskõlas Euroopa Inimõiguste Kohtu ning Euroopa Kohtu praktikaga, mille kohaselt ei tohiks põhjused andmete kogumiseks ning õigused andmete edastamiseks on olla õigustamatult laiad ning andmete automaatse ja massilise kogumisega saadud andmeid tohiks kasutada üksnes väga raskete kuritegude lahendamiseks. Kuni aastani 2013 oligi elektroonilise side andmete päring seotud loetletud kuritegudega, kuid 2013. aastast jõustunud kriminaalmenetluse seadustiku muudatusega on ESS §-s 111^1 sätestatud päringud tavalised menetlustoimingud[416], mida ei ole piiratud konkreetsetele kuritegudele. Seega võib elektroonilise side andmeid kasutada ka kelmuse või korterivarguse lahendamiseks ning teiste mitte niivõrd raskete kuritegude avastamiseks ning lahendamiseks. See ei ole kooskõlas ei Euroopa Inimõiguste Kohtu kui ka Euroopa Kohtu kohtupraktikaga.

Teiseks säilitatakse ning kasutatakse elektroonilise side andmeid riigi julgeoleku ja põhiseadusliku korra kaitseks.[417] Nii Euroopa Kohus kui Euroopa Inimõiguste Kohus on tunnustanud vajadust võtta tarvitusele laialdast andmete kogumist (sh elektroonilise side andmete kogumist) eriti raskete kuritegude puhul, sh riigi julgeoleku ning põhiseadusliku korra kaitsmise eesmärgil. Seega riigijulgeoleku ning põhiseadusliku korra kaitse on EK ja EIK kohtupraktika kohaselt sellised eesmärgid, mille puhul andmete massiline kogumine lubatud on.

Eesti õigus (ESS § 111^1 lg 11 p 3) lubab elektroonilise side andmete säilitamist ja kasutamist ka väärtegude menetlemiseks. Kuivõrd ESS ja väärteomenetluse seadustik piiritlevad elektroonilise side andmete kasutamist üksnes pädevate asutuste kaudu, võib sellest järeldada,

[415] Õiguskantsleri seisukoht 2015, lk 4-5.
[416] A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Riigikohus: Tartu 2015. Kättesaadav: http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf (14.04.2016)
[417] ESS § 111^1 lg 11 p 2 ja JAS § 1 lg 1.

et elektroonilise side andmeid on lubatud koguda, säilitada ja kasutada enamuse väärtegude menetlemiseks. Kehtetuks tunnistatud elektroonilise side andmete direktiiv lubas andmete säilitamist üksnes raskete kuritegude uurimise, avastamise ja kohtus menetlemise eesmärgil. Ka Euroopa Inimõiguste Kohtu lahendites, mis käsitlesid näiteks telekommunikatsiooni jälgimist[418] ning DNA ja sõrmejälgede säilitamist[419], on kohus märkinud, et andmete kogumine ja edasine kasutamine peab toimuma kitsalt piiritletud kuritegude uurimiseks ning lahendamiseks, eelkõige raskete kuritegude uurimiseks, nagu seda on terrorism. Eelnevalt käsitletud Euroopa Inimõiguste Kohtu lahenditest ei puudutanud ükski eraellu sekkumist väärtegude menetlemise eesmärgil. Kuivõrd väärteod ei kujuta endast raskeid kuritegusid, võib Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikale tuginedes teha järelduse, et väärtegude hõlmamisega laiendatakse ülemäära süütegude nimekirja, mille puhul on elektroonilise side andmete kogumine ja kasutamine lubatud. Seetõttu võib järeldada väärtegude menetlemiseks andmete kogumine ja kasutamine ei ole lähtuvalt Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikast kooskõlas proportsionaalsuse põhimõttega.

Lisaks kriminaalmenetlusele kogutakse ja kasutatakse elektroonilise side andmeid kriminaalmenetluse väliste toimingute tegemiseks olukorras, kus on kahtlus, et isik paneb toime kuriteo või kui isik on kuulutatud tagaotsitavaks.[420] Teisisõnu on päringu esitamine õigustatud siis, kui esineb vajadus koguda teavet kuriteo ettevalmistamise kohta selle avastamise või tõkestamise eesmärgil või tagaotsitavaks kuulutamise määruse täitmiseks. Need on küll seotud kuritegude ennetamisega, kuid kuritegude ringi, mille puhul võib seda meedet kasutada, ei ole piiritletud. Seetõttu võivad jälitusasutused seda kasutada erinevate kuritegude ärahoidmiseks, sh vähem tähtsate kuritegude ärahoidmiseks, mis ei ole kooskõlas Euroopa Kohtu ja Euroopa Inimõiguste kohtu seisukohtadega. Samuti on probleemiks see, et kuriteo tõkestamise mõistet ei ole seaduses avatud ning seda ei ole piisavalt selgitatud ka kohtupraktikas, mis tähendab seda, et juurdepääsutingimused andmetele on ebaselged.[421]

Kuigi ESS sellele otse ei viita, võimaldatakse elektroonilise side andmeid kasutada ka korrakaitseseaduse § 35 alusel kõrgendatud ohu väljaselgitamiseks või tõrjumiseks. KorS § 5 lg 4 alusel esineb kõrgendatud oht siis, kui esineb oht isiku elule, kehalisele puutumatusele, füüsilisele vabadusele, suure väärtusega varalisele hüvele, suure keskkonnakahju tekkimise oht või karistusseadustiku 15. peatükis sätestatud I astme kuriteo või 22. peatükis sätestatud kuriteo

[418] nt EIKo *Weber & Saravia vs Germany*.
[419] EIKo *S & Marper vs the United Kingdom*.
[420] KKS, MKS, PPVS, TS ja VangS.
[421] U. Lõhmus 2015, lk 744.

toimepanemise oht. KorSis sätestatud alused hõlmavad seega ka kriminaalmenetluse väliste toimingute tegemist, mis on suunatud kuriteo tõkestamiseks, kuigi KorS-is sätestataud alused on mõneti konkreetsemad.

Elektroonilise side andmeid kogutakse ning kastutatakse ka tausta- ja julgeolekukontrolli[422] läbiviimiseks KKS, MKS, PPVS, TS, VangS, RelvS, StrKS, TurvaS, VMS ja riigisaladuse ja salastatud välisteabe seaduse (RSVS) alusel. Kuigi enamusel juhtudest on andmepäringute tegemine põhjendatav julgeoleku kaalutlustega, kasutatakse taustakontrolli tegemist ka haldusmenetluse raames. Sellised seadused on näiteks RelvS – relvaloa ja tegevusloa andmiseks, StrKS – erinevate toimingute tegemiseks, nt üldloa, litsentsi, ettevõtja sertifitseerimiseks, TurvaS – tegevusloa andmiseks, ja VMS – haldusakti andmiseks või toimingu sooritamiseks. Neid juhtumeid võib pidada vähemalt kaudselt pidada seotuks julgeoleku ning kuritegude ärahoidmisega.

Elektroonilise side andmete kasutamine nähakse ette ka väärtpaberituru seaduse alusel riikliku järelevalve teostamiseks, nt turukuritarvituse, turul olulise osaluste omandamisest või võõrandamisest teatamata jätmise või ebaõige teatamise ning õigusvastase ülevõtmispakkumise ärahoidmiseks (VPTS §-d 230, 230^3). Riikliku järelevalve teostamiseks võimaldatakse seda ka IKS § 32^2 alusel, lubades seda kasutada üksnes omanikupäringu tegemiseks. Ka see ei ole seotud raskete kuritegude uurimise, avastamise või menetlemisega, mistõttu lubab Eesti õigus andmete kogumist ja kasutamist olulisemalt laiematel eesmärkidel kui 2014. aastani kehtinud elektroonilise side andmete direktiiv. Euroopa Kohtu selgituste valguses kohtuasjas Digital Rights Ireland võib riikliku järelevalve eesmärgil andmete kogumist ja kasutamist pidada lubamatuks, sest selline intensiivne põhiõiguste riive saab olla õigustatud üksnes väga raskete kuritegude avastamiseks.

Lisaks eelnevale kogutakse ning kasutatakse elektroonilise side andmeid tunnistajakaitse seaduse alusel tunnistajakaitse andmiseks. Sellel puudub samuti seos raskete kuritegude avastamise või menetlemisega, mistõttu on äärmiselt kaheldav, et elektroonilise side andmete kogumine ja kasutamine on selle eesmärgil proportsionaalne.

[422] Julgeolekukontroll tähendab füüsilise või juriidilise isiku vastavuse hindamist riigisaladuse ja salastatud välisteabe seaduses (RSVS) sätestatud nõuetele riigisaladuse või salastatud välisteabe töötlemisloa, sellele juurdepääsu loa või sertifikaadi saamiseks või selle kehtivuse pikendamiseks. Taustakontroll tähendab laiemalt isiku sobivuse hindamist teatud ameti- või töökohale. A. Lott, lk 16.

Samuti võimaldab Eesti õigus kasutada elektroonilise side andmeid eraõiguslike vaidluste lahendamiseks tsiviilkohtumenetluses ESS § 111^1 lg 11 p 5 ja § 114^1 alusel. Sealjuures ei piiritle ESS ega ka mõni teine õigusakt, millistel eesmärkidel täpsemalt tsiviilkohtumenetluses neid andmeid taotleda võib, jättes ka piiritlemata need asjaolud, millal võiks selliste andmete küsimine üldse põhjendatud olla (mis liiki nõuete puhul jne). See eesmärk on selgelt hoopis teistsugune, kui nägi ette elektroonilise side andmete direktiiv.

Kokkuvõtvalt kasutatakse elektroonilise side andmeid väga mitmesugustel eesmärkidel, mis ei ole seotud kitsalt raskete kuritegudega (sh terrorikuritegudega). Sealhulgas kogutakse ning kasutatakse neid andmeid ka vähem tähtsate kuritegude uurimiseks, väärtegude uurimiseks, haldusmenetlustes taustakontrolli tegemiseks, riikliku järelevalve teostamiseks ning andmeid on lubatud kasutada ka tsiviilkohtumenetluses. Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktika kohaselt võib sellist massilist andmete kogumist kasutada üksnes raskete kuritegude avastamiseks, ärahoidmiseks ning menetlemiseks, mistõttu peab nende süütegude loetelu olema väga kitsalt piiritletud, mille puhul võib andmeid koguda ning kasutada. Vastaselt juhul ei vasta regulatsioon vältimatult vajalikkuse põhimõttele, mistõttu võib meedet pidada ebaproportsionaalselt. Käesoleval juhul ei ole Eesti regulatsiooni sätestatud kitsalt, milliste süütegude puhul võib neid andmeid kasutada, mistõttu ei vasta Eesti regulatsioon eelnimetatud tingimustele, mistõttu ei vasta see Euroopa Kohtu ning Euroopa Inimõiguste Kohtu lahendite valguses proportsionaalsuse põhimõttele.

3.2. Ajalised piirangud ja isikute ringi piiritlemine

Järgnevalt hinnatakse, kuidas on elektroonilise side andmete regulatsioonis piiritletud isikute ring ning sätestatud ajalised piirid andmete kogumisel, säilitamisel ja kasutamisel. Isikute ringi hindamisel tuleb silmas pidada esmalt nii neid isikuid, kelle kohta võib elektroonilise side andmeid koguda ja kasutada, kui ka neid isikuid, kellel on nendele kogutud andmete hiljem ligipääs. ESS § 111^1 alusel säilitatakse andmeid kõigi teostatud sideseansside ja kõigi isikute suhtes. Sealjuures ei piiritleta säilitatavaid andmeid geograafilise, isikulise, ajalise või muu tunnuse alusel, nagu pidas vajalikuks Euroopa Kohus kohtulahendis Digital Rights Ireland[423], mistõttu võiks teha sellest järelduse, et Eesti regulatsioon on üleliia riivav. Samas avaldas õiguskantsleri oma seisukohas[424] arvamust, et ei ole selge, kuidas ja millistest

[423] EKo *Digital Rights Ireland*, p 57-58.
[424] Õiguskantsleri seisukoht 2015, lk 7.

valikukriteeriumidest lähtuvalt saaks toimuda sideandmete valikuline säilitamine sellisel viisil, et see tagaks efektiivse isikute õiguste ja vabaduste kaitse, sealhulgas raskete kuritegude tõkestamise ja menetlemise. Õiguskantsler lisas, et kui isegi kui valikukriteeriumide seadmine oleks võimalik, tooks selliste kriteeriumite kehtestamine kaasa meelevaldsuse ja isikute põhjendamatu ebavõrdse kohtlemise ohu. Sisuliselt viitab õiguskantsler sellele, et Euroopa Kohtu lahendis nõutav, ei ole praktikas teostatav, sest see ei tagaks piisavat tõhusust kuritegude avastamiseks ja ärahoidmiseks, tuues kaasa seajuures diskrimineerimisohu.

Isikulised piirangud, kelle kohta võib nimetatud andmeid sideettevõtjate käest küsida, on vastavalt regulatsioonile erinevad. Kriminaalmenetluse raames ei ole piiritletud, milliste isikute kohta võivad uurimisasutused, prokuratuur ja kohus neid andmeid küsida. Seega võib see hõlmata nii kahtlustatavaid kui ka kolmandaid isikuid, kes omavad kriminaalmenetluse jaoks olulist teavet. Jälitusasutused võivad kaitseväe korralduse seaduse, maksukorralduse seaduse, politsei ja piirivalve seaduse, relvaseaduse, strateegilise kauba seaduse, tolliseaduse, tunnistajakaitse seaduse, turvaseaduse, vangistusseaduse ja välismaalaste seaduse alusel andmeid küsida isikute kohta, kelle puhul on põhjendatult alust arvata, et ta paneb toime kuriteo või kes on kuulutatud tagaotsitavaks.[425] Väärtpaberituru seadus, väärteomenetluse seadustik ega ka julgeolekuseadus sellist isikulist piirangut ette ei näe. Samuti ei ole piiritletud neid isikuid, kelle kohta võib andmeid küsida tsiviilkohtumenetluse raames. Seega võib öelda, et mitmetel juhtudel on jäetud määratlema, kelle kohta täpsemalt võib andmeid sideettevõtjatelt küsida. See ei ole kooskõlas EK ja EIK praktikaga, mis nõuab nende isikute ranget piiritlemist.

Asutused, kellel on õigus pääseda ligi elektroonilise side meta-andmetele, on samuti äärmiselt lai. EES § 111^1 lg 11 alusel edastatakse andmeid järgmistele asutustele:

1) kriminaalmenetluse seadustiku kohaselt uurimisasutusele, jälitusasutusele, prokuratuurile ja kohtule;
2) julgeolekuasutusele;
3) väärteomenetluse seadustiku kohaselt Andmekaitse Inspektsioonile, Finantsinspektsioonile, Keskkonnainspektsioonile, Politsei- ja Piirivalveametile, Kaitsepolitseiametile ning Maksu- ja Tolliametile;
4) väärtpaberituru seaduse kohaselt Finantsinspektsioonile;
5) tsiviilkohtumenetluse seadustiku kohaselt kohtule;

[425] KrMS § 126^2 lg 3.

6) jälitusasutusele kaitseväe korralduse seaduses, maksukorralduse seaduses, politsei ja piirivalve seaduses, relvaseaduses, strateegilise kauba seaduses, tolliseaduses, tunnistajakaitse seaduses, turvaseaduses, vangistusseaduses ja välismaalaste seaduses sätestatud juhtudel.

Seega on erinevate seaduste alusel ligipääs nendele andmetele kümnel ametiasutusel (Politsei- ja Piirivalveamet, Kaitsepolitseiamet, Teabeamet, Maksu- ja Tolliamet, Konkurentsiamet, Sõjaväepolitsei, Keskkonnainspektsioon, Justiitsministeeriumi vanglate osakond, Andmekaitse Inspektsioon, Finantsinspektsioon) ning vanglatel ja tsiviilkohtutel. See on tingitud sellest, et EES ei piira andmetele juurdepääsu ning hilisemat kasutamist eesmärgiga ennetada ja avastada täpselt piiritletud raskeid kuritegusid, vaid sisuliselt võib andmeid kasutada kõikide kuritegude ja väärtegude menetlemisel ning lisaks ka taustakontrolli tegemiseks (näiteks maksukorralduse seaduse alusel § 81^2 teenistusse võtmisel või turvaseaduse § 46^1 alusel tegevusloa andmisel).

Lähtuvalt Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikale peaks isikute ring, kellel on õigus neid andmeid töödelda, olema piiratud ning tagama selle, et see oleks taotletava eesmärgi seisukohast vältimatult vajalik. Käesoleval hetkel isikute ringi, kes nendele andmetele ligipääsevad ning neid töödelda saavad, piiratud ei ole, mistõttu ei ole see kooskõlas Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikaga. Samuti puudub regulatsioon selle kohta, kes nende asutuste töötajatest on õigustatud nendele andmetele ligi pääsema.

Ajalise piiri osas säilitatakse sideandmeid vastavalt ESS § 111^1 lg-le 4 üks aasta, alates side toimumise ajast, kui need sideteenuse osutamise käigus on loodud või neid on töödeldud. Kui asutus on esitanud sideettevõttele järelepärimise, siis ESS § 111^1 lg 4 alusel säilitab järelepärimise esitaja (ametiasutus) kaks aastat päringu alusel antud teavet. Avaliku korra ja riigi julgeoleku huvides võib Vabariigi Valitsus neid tähtaegasid piiratud ajavahemikuks pikendada (ESS § 111^1 lg 6).

Riigikohus on ESS § 111^1 lg 4 osas leidnud (kriminaalmenetluslikus kontekstis), et ühe aasta pikkune tähtaeg ei ole ülemäära pikk. [426] Samas ei vasta see seisukoht sellele, kas selle perioodi puhul on tegemist vältimatult vajaliku perioodiga, nagu nõuab Euroopa Kohtu kohtupraktika. Kaheaastane tähtaeg võib olla põhjendatud olukorras, kus kriminaalmenetluse läbiviimine võtab aega mitu aastat. Samas võib see olla õigustamatu, kui saadud andmed ei osutu

[426] RKKKo 3-1-1-51-14, p 22.3.

kriminaalmenetluses vajalikuks või on muul põhjusel võimalik neid andmeid varem hävitada. Varem andmete kustutamist regulatsioon ei võimalda.

Isegi, kui üheaastane ja kaheaastane tähtaeg ei ole ülemäära pikad, ei ole üheselt selge, millistel juhtumitel täpsemalt võib Vabariigi Valitsus neid tähtaegasid pikendada ning kui pikaks perioodiks. Kui riigi julgeolek võib olla lihtsamini mõistetav, siis avalik kord võib tähendada sisuliselt hulgaliselt erinevaid olukordi.[427] Vastavalt Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikale peaksid aga need olukorrad olema väga täpselt määratletud, millistel tingimustel võib tähtaegasid pikendada. Sealjuures peaks olema selge, millistes olukordades võib pikendamist nõuda ning kui pikaks perioodiks. Need tingimused on käesoleval juhul täitmata.

Seoses ajalise piiriga tuleb vaadata ka seda, kas seadus sätestab, millise perioodi kohta võib näiteks ühe isiku kohta andmeid küsida. Mõistagi on see piiritud ühe aastase perioodiga (sideettevõtjad ei ole kohustatud kauem andmeid säilitama), kuid vältimatult vajaliku tagamiseks ehk vajalikkuse põhimõttele vastamiseks peaksid ka siinkohal olema teatud piirangud. Erinevatest seadustest, mis andmete küsimist reguleerivad, märgivad kriminaalmenetluse seadus, kaitseväe korralduse seadus, maksukorralduse seadus, politsei ja piirivalve seadus, tolliseadus ning vangistusseadus, et prokuratuuri poolt antud loas märgitakse kuupäevalise täpsusega ajavahemik, mille kohta andmete nõudmine on lubatud. Millest lähtuda ajavahemiku määramisel, sellele juhiseid ei anta. KrMS § 90^1 lõikes 3 märgitakse üksnes seda, et päringu võib teha siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. See käsitleb põhimõtteliselt päringu tegemise vajalikkust, kuid ei anna juhiseid perioodi määratlemise kohta. Samas peab Euroopa Inimõiguste Kohtu praktika kohaselt seadus sätestama asutustele täpselt kaalutlusõiguse piirid meetme kasutuselevõtmiseks. Sellele Eesti regulatsioon ei vasta.

3.3. Tingimused andmete töötlemisele

Eesti regulatsioon näeb teatud juhtudel ette tingimused, millal võib ametiasutus andmeid küsida ehk teisisõnu, reeglid, millal võivad sideettevõtjad andmeid edastada ning ametiasutused andmeid kasutada. Väärteomenetluse seadustiku § 31^2 lg 3 alusel võib päringu sideettevõtjale

[427] Vastavalt korrakaitseseadusele on avalik kord ühiskonna seisund, milles on tagatud õigusnormide järgimine ning õigushüvede ja isikute subjektiivsete õiguste kaitstus.

teha üksnes siis, kui see on vältimatult vajalik väärteomenetluse eesmärgi saavutamiseks. Ka kriminaalmenetluse seadustiku § 90^1 lg 3 alusel võib päringu teha üksnes siis, kui see on vältimatult vajalik kriminaalmenetluse eesmärgi saavutamiseks. Julgeolekuasutuste seadus päringute esitamisele tingimusi ei sea, kuid julgeolekuasutuste seaduse üldpõhimõtetest (JAS § 3 lg 2) tuleneb, et mitme võimaliku abinõu olemasolul kasutab asutus sellist, mis isikute põhiõigusi seoses julgeolekuasutuse ülesande täitmisega võimalikult vähe piirab, ning kasutada võib abinõu, mis ei piira üksikisiku põhiõigusi ülemääraselt, võrreldes julgeolekuasutuse taotletava eesmärgiga. ESS § 114^1 alusel võib tsiviilkohtumenetluses andmeid küsida tõe tuvastamiseks. Andmete edastamisele väärtpaberituru seaduse kohaselt Finantsinspektsioonile ning ESS §111^1 lg 11 p 6 nimetatud juhtudel jälitusasutustele, ei ole seadustes tingimusi sätestatud.

Väärteomenetluse seadustik (§ 31^2) seab piirangu andmete edastamisele aga selliselt, andmete nõudmiseks õigustatud asutus võib esitada sideettevõtjale üksikpäringu, milleks on kirjalik päring konkreetse telefonikõne, elektronkirja, elektroonilise kommentaari või muu üksiksõnumi edastamisega seotud sideseansi kohta. Ka ESS § 114^1 alusel on kohtul tsiviilkohtumenetluses õigus esitada sideettevõtjale üksikpäringu. Muid piiranguid või erisusi, samuti tingimusi selliste andmete hoidmisele, kasutamisele ja hävitamisele, ei ole ESSis ega tsiviilkohtumenetluses sätestatud. IKS § 32^2 alusel võib Andmekaitse Inspektsioon teha päringu omanikupäringu kohta.

Kõigil ülejäänutel juhtudel seadus päringute ulatust ei täpsusta, mistõttu võivad ülejäänud asutused esitada massipäringuid. Näiteks KrMS § 90^1 lg 2 alusel märgitakse päringu tegemise loas kuupäevalise täpsusega ajavahemik, mille kohta andmete nõudmine on lubatud. Selline massipäringute tegemine ei taga paraku seda, et andmeid küsitakse üksnes asjas tähtsust omavate faktide kohta, mistõttu on võimalik, et eraelu riive võib olla suurem kui konkreetses asjas vajalik.

Andmete järelepärimine võib toimuda nii ESS § 112 alusel nii kirjalikus, elektroonilises kui ka suulises vormis. Suulises vormis, kinnitades selle parooliga, võib esitada järelepärimise aga üksnes nn omanikupäringute kohta. ESS § 112 lg 3 kolmanda lause kohaselt on asutustel võimalik lisaks päringute esitamisele saada ligipääs ka püsivalt. Nimelt võib kirjaliku lepingu alusel tagada asutustele andmetele juurdepääsu pideva elektroonilise ühendusega. See tähendab sisuliselt pädeva asutuse võimalust saada enda hinnangul talle vajalikke sideandmeid vahetult

ilma eraldi järelepärimist esitamata.[428] Kuivõrd järelepärimiseta saadud teavet ESS § 112[1] alusel ei nimetata sideettevõtjate poolt Tehnilise Järelevalve Ametile esitatavates statistilistes andmetes, on ebaselge, kas riigil on terviklik ülevaade elektroonilise püsiühenduse alusel tehtud teabepäringute hulgast.[429] Sealjuures puudub ESSis regulatsioonis juurdepääsuteabe säilitamise kord, sh logifailide säilitamise ja hävitamise kord.[430]

Teine oluline küsimus nende menetlusreeglite juures on see, kuidas toimub pärast päringu esitamist andmete edasine säilitamine, kasutamine, edastamine ja kustutamine pärast. ESS § 111[1] lg 4 reguleerib üksnes olukorda selliselt, et kui asutus on esitanud sideettevõttele järelepärimise, siis selle alusel antud teavet säilitab järelepärimise esitaja (ametiasutus) kaks aastat. Kuidas toimub aga täpsemalt nende andmete kasutamine, edastamine ja kustutamine, seda ei ole Eesti õiguses täpsemalt reguleeritud. Näiteks ei ole selge, kas juba kogutud andmeid võib kasutada ka teistes kriminaalmenetlustes või muudes menetlustes ning milliseid andme säilitamise ning hävitamise nõudeid peab sellisel juhul järgima.

Seoses andmete hoidmisega sideettevõtja juures, sätestab ESS järgmised nõuded. Esiteks, ESS § 111[1] lg 5 kohustab säilitama sideandmeid Euroopa Liidu liikmesriigi territooriumil. ESS § 113 lg 7 alusel on ette nähtud logifailide, taotluste, andmete ja järelepärimiste säilitamise, Tehnilise Järelevalve Ametile üleandmise ning kustutamise ja hävitamise kord. Samuti näeb ESS § 111[1] lg 9 ette, et sideettevõtja peab tagama:

1) sama kvaliteedi, turvalisuse ja andmekaitse nõuete täitmise, mida kohaldatakse teistele elektroonilise side võrgus olevatele analoogsetele andmetele;
2) andmete kaitse nende juhusliku hävimise või ebaseadusliku hävitamise, kadumise või muutmise, loata või ebaseadusliku säilitamise, töötlemise, juurdepääsu või avalikustamise eest;
3) vajalikud tehnilised ja korralduslikud abinõud andmetele juurdepääsu piiramiseks;
4) side sisu kajastavate andmete säilitamata jätmise.

ESS-st tulenevad ka mitmed teised isikuandmete kaitsega seotud nõuded (IKS, ESS §-d 102, 102[1], 106), näiteks kohustus teavitada Andmekaitse Inspektsiooni ja klienti isikuandmetega seotud rikkumistest, isikuandmetega seotud rikkumiste kohta arvestuse pidamine, töötlemiseks õigustatud isikute ringi piiritlemine ainult sideteenuse osutaja ja tema poolt volitatud isikutega.

[428] Õiguskantsleri seisukoht 2016, lk 6.
[429] *Ibid*.
[430] *Ibid*.

ESSi alusel kogutud ning ametiasutustele edastatud andmete säilitamise, töötlemise ja hävitamise kohta erinõudeid sätestatud ei ole. Ka õiguskantsler on märkinud, et üldiste andmekaitsenõuete kõrval ei ole sideandmete edasiseks töötlemiseks andmete turvalisuse tagamiseks või kuritarvituste vältimiseks seaduste või määrustega ette nähtud eraldi menetluslikke garantiisid, järelevalvekorda või muid piiritlevaid nõudeid.[431]

Eelnevalt nimetatud tingimused on sõnastatud väga üldiselt ja umbmääraselt ning selle põhjal on keeruline hinnata seda, kas need tingimused tagavad tegelikult andmete kõrge kaitse- ja turvalisuse tasemel, nagu seda on nõutud Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikas. ESS § 111^1 põhiseaduslikkuse hindamisel küsitles õiguskantsler suures mahus sideteenust osutavaid ettevõtjaid (mobiilsideoperaatorid), mille esindajad väitsid, et neil on ESS §-s 111^1 nimetatud andmed muudest sideteenuse osutamisel tekkivatest andmetest eraldatud omaette andmekogumina, millele juurdepääs on asutusesiseselt kitsendatud ja kontrollitav.[432] Käesoleval hetkel puuduvad andmed, mis annaksid alust nendes väidetes kahelda. Samas aitaksid täpsemad tehnilised tingimused (nt standardid) tagada, et kõik ettevõtjad rakendavad ühesuguseid ning piisava kvaliteediga meetmeid. Arvestades võimalikku kuritarvitamise ohtu, vajaks andmete säilitamise turvalisuse küsimus kindlasti täiendavat analüüsi ning praktika hindamist, mil määral on tegelikkuses andmete kaitse tagatud.

Kokkuvõtlikult on andmete hoiustamise, kasutamise, edastamise ja hävitamise reeglid üldiselt ning ei ole võimalik kindlaks teha, kas need reeglid välistavad kuritarvitamise ohu. Esiteks puudub regulatsioon selle kohta, kas juba kogutud andmeid võib kasutada ka teistes kriminaal- või muudes menetlustes ning milliseid andme säilitamise ning hävitamise nõudeid peab sellisel juhul järgima. Lisaks on murettekitav see, et asutustel on võimalik lisaks päringute esitamisele saada ligipääs ka püsivalt, mille puhul on võimalike kuritarvituste oht suurem.

3.4. Järelevalvesüsteem ja isikute teavitamine

Järgnevalt analüüsitakse, millist järelevalvesüsteemi erinevates olukordades regulatsioon pakub ning kas ja kuidas toimub isikute teavitamine. Nii järelevalvesüsteemi kui isikute teavitamise osas toimus 2013. aastal oluline muudatus. ESS §-i 111^1 alusel tehtud päringud olid jälitustoiminguteks 2012. a lõpuni kehtinud jälitustegevuse seaduse[433] § 12 lõike 1 punkti 5

[431] Õiguskantsleri seisukoht 2016, lk 11.
[432] Õiguskantsleri seisukoht 2015, lk 9.
[433] Jälitustegevuse seadus. – RT I, 29.06.2012, 38.

järgi, milleks oli vaja kohtuniku luba. Alates 2013. aastast jõustunud kriminaalmenetluse seadustiku muudatusega on ESS §-s 111^1 sätestatud päringud tavalised menetlustoimingud.[434] Muudatuse ettevalmistajad põhjendasid muudatust sellega, et „Ka mitmed Euroopa Liidu liikmesriigid lubavad selliseid andmeid kasutada kuritegude avastamiseks, uurimiseks ja kohtus menetlemiseks. Seega ei pea ka mujal alati tegemist olema jälitustoimingutega ning sageli ei käsitletagi omanikupäringuid ja kõneeristusi kui jälitustoiminguid“.[435] Tegelikult eeldab valitseva lähenemise kohaselt Euroopas meta-andmete kogumine kohtuniku luba.[436]

Kriminaalmenetluses võib uurimisasutus vastavalt KrMS § 90^1 lg-le 1 lõppkasutaja tuvastamiseks (edaspidi *omanikupäring*) vajalike andmete saamiseks esitada sideettevõtjale taotluse ilma eelnevalt ühtegi luba küsimata. Muude elektroonilise side seaduse § 111^1 lõigetes 2 ja 3 loetletud andmete (nn kõneeristuste) saamiseks võib uurimisasutus teha päringu elektroonilise side ettevõtjale prokuratuuri loal kohtueelses menetluses või kohtu loal kohtumenetluses. Julgeolekuasutused võivad julgeolekuasutuste seaduse alusel koguda andmeid elektroonilise side võrgu kaudu edastatavate sõnumite edastamise fakti, kestuse, viisi ja vormi ning edastaja või vastuvõtja isikuandmete ja asukoha kohta ilma prokuratuuri või kohtu loata. Isiku õiguse piiramise kodu, perekonna- või eraelu puutumatusele otsustab julgeolekuasutuse juht või tema poolt volitatud ametnik korraldusega (JAS § 27 lg 3).

Sarnane lahendus esineb ka kaitseväe korralduse seaduses, maksukorralduse seaduses, politsei ja piirivalve seaduses, tolliseaduses ja vangistusseaduses: omanikupäringu tegemiseks ühte eelnevat luba vaja ei ole, kuid muudel juhtudel asutusel peab olema andmete küsimiseks prokuratuuri luba.

Väärtpaberituru seaduse § 231 lg 4 kohaselt eeldab Finantsinspektsioonile andmetele ligipääsu saamine halduskohtu luba. Väärteomenetluse seadustiku § 31^2 lg 1 kohaselt võivad Andmekaitse Inspektsioon, Finantsinspektsioon, Kaitsepolitseiamet, Keskkonnainspektsioon, Maksu- ja Tolliamet ning Politsei- ja Piirivalveamet teha omanikupäringu ilma ühegi eelneva loata. Muude kui omanikupäringu juhtudel (ESS § 111^1 lõigetes 2 ja 3 loetletud andmete kohta)

[434] A. Lott, lk 25.
[435] Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, lk 5. http://www.riigikogu.ee/?op=ems&page=eelnou&eid=86dde8ff-c50e-48ba-a39ea325fe15a3f0& (14.04.2016).
[436] A. Lott, lk 25.

peab nimetatud asutustel olema kohtu luba üksikpäringu[437] tegemiseks elektroonilise side ettevõtjale. Asutused võivad selle päringu teha üksnes siis, kui see on vältimatult vajalik väärteomenetluse eesmärgi saavutamiseks (VTMS § § 31^2 lg 3).

Maksukorralduse seaduses, politsei ja piirivalve seaduses, relvaseaduses, strateegilise kauba seaduses, tolliseaduses, turvaseaduses, vangistusseaduses ja välismaalaste seaduses sätestatud juhtudel võib andmeid küsida isiku nõusolekul ning need juhtumid puudutavad eelkõige isikute taustakontrolli nt teenistusse võtmisel või haldusakti või toimingu tegemiseks[438]. Tunnistajakaitse seaduse § 18^1 sätestatud tunnistaja kaitse taotluse menetluse raames võib andmeid küsida taotlust menetleva asutuse juhi või tema poolt volitatud isiku loal.

Seega toimub andmetele juurdepääs väga erinevalt: omanikupäringute puhul reeglina ilma ühegi loata, muude kui omanikupäringute puhul on vaja prokuratuuri luba, väärteomenetluse seadustiku alusel ning väärtpaberiseaduse kohaselt peab olema kohtu luba, tausta kontrolli tegemiseks peab olema isiku nõusolek ning tunnistajakaitse seaduse alusel taotlust menetleva asutuse juhi või tema poolt volitatud isiku luba. Julgeolekuasutused saavad ligipääsu andmetele ühegi loata.

EK ja EIK praktikast tulenevalt annab kohtulik kontroll kõige tugevama kaitse. Olukorras, kus prokuratuur juhib kohtueelset menetlust ja esindab riiklikku süüdistust kohtus, ei saa prokuratuuri pidada sõltumatuks järelevalveasutuseks. Üksnes prokuratuuri kontrolli ei saa pidada piisavaks ka seetõttu, et kohtulik järelkontroll on tagatud üksnes nende juhtudel, kui näiteks kriminaalmenetluse raames esitatakse süüdistusaktis tõendid, mis on saadud elektroonilise side andmete päringu kaudu. Samuti puuduvad käesoleval hetkel andmed sh selle kohta, kui palju selliseid lubasid taotletakse, kui palju neist rahuldatakse ning kas prokuratuur hindab neid taotlusi praktikas põhjalikult, et oleks tagatud see, et luba antakse üksnes põhjendatud juhul. Nagu eespool märgitud, ei ole prokuratuurile antud väga selgeid juhiseid, millal ja mis tingimustel võib loa anda. Kuivõrd elektroonilise side andmete päring ning selle kasutamist ei ole enam jälitustoiming, ei ole sellele ette nähtud ka kindlaid vorminõudeid. Vorminõuete olemasolu, st kindlate elementide käsitlemine loa andmisel, aitab muuhulgas tagada seda, et prokuratuur järgib põhjendamiskohustust. Põhjendamiskohustuse järgimine on vajalik esiteks seetõttu, et see paneb loa andja põhjalikumalt läbi mõtlema loa andmise, ning

[437] Üksikpäring on kirjalik päring elektroonilise side seaduse § 111^1 lõigetes 2 ja 3 nimetatud andmete saamiseks konkreetse telefonikõne, elektronkirja, elektroonilise kommentaari või muu üksiksõnumi edastamisega seotud sideseansi kohta. VTMS § 31^2 lg 2.
[438] Nt strateegilise kauba seadus § 76; välismaalaste seadus § 31^1.

teiseks, võimaldab see hiljem teostada järelkontrolli, kas päringu tegemine oli selles situatsioonis tõepoolest vajalik. Eelnevast tulenevalt võib järeldada, et Eesti õiguses ei ole prokuratuuri loa puhul piisavat järelevalvesüsteemi tagatud.

Nende olukordade puhul, kus andmetele ligipääsu saamine eeldab kohtu luba, on formaalselt järelevalvesüsteemi nõue täidetud. Samas peab vastavalt Euroopa Inimõiguste Kohtu praktikale olema tagatud ka see, et kohtul on tõepoolest sisuline pädevus hinnata (koos tõenditega), kas esineb põhjendatu kahtlus, et isik on süüteo toime pannud, või kas taotletud meede on kooskõlas vajalikkuse ja proportsionaalsuse nõudega.[439] Eesti regulatsiooni nendele tingimustele vastavuses võib kahelda, sest regulatsioon ei näe ka kohtu loale ette konkreetset vormi, mis annaks kohtule juhised, mida loa andmisel hinnata tuleb, ning mis teeb võimalikuks selle, et kohus saab langetada otsuse ilma seda otsust piisavalt põhjendamata. Sellisel juhul on tagant järele keeruline kindlaks teha, kas kohus hindas kõiki asjaolusid põhjalikult, mis on aluseks sellele, et tehtud otsus on kooskõlas proportsionaalsuse põhimõttega.

Olukorras, kus andmete küsimiseks ei ole vaja ei prokuratuuri ega kohtu luba ning puudub selge järelkontroll, on ilmselge, et selline korraldus ei ole kooskõlas EK ja EIK praktikaga, mille kohaselt peab selliste andmetele ligipääs toimuma sõltumatu asutuse eelkontrolli või väga tugeva järelkontrolli alusel. Tugevat järelkontrolli Eesti õiguses sätestatud ei ole. Üheks alternatiivseks tagatiseks on ka isikute teavitamine, kuid täielikult see sõltumatut kontrolli asendada ei saa. Lisaks on teavitamist on lubatud edasi lükata või teavitamata jätta, kui see seab ohtu menetluse eesmärgi. Samuti ei ole isiku teavitamist kõigil juhtudel ka ette nähtud (nt väärteomenetluse või kriminaalmenetluse raames). Probleemne on ka see, et omanikupäringute puhul on lubatud suulise päringu esitamine (kinnitades seda parooliga). Selliste päringute üle on väga raske, kui mitte võimatu järelevalvet teostada. Sellisel juhul muudab see süsteemi haavatavaks võimalikele kuritarvitustele. ESS § 112[1] alusel on sideettevõtjal kohustus koguda andmeid järelepärimiste kohta ning edastada see Tehnilise Järelevalve Ametile, kuid regulatsioonist ei selgu, kas neile andmetele võiks juurde pääseda ka asutus, kes peaks teostama järelevalvet nii erinevate uurimisasutuste kui ka teiste asutuste üle, kes sideandmetele ligi pääsevad.

Veelgi problemaatilisem on küsimus, kuidas toimub järelevalve ESS § 112 lg 2 lause 3 alusel, kui asutus saab püsivalt ligipääsu elektroonilise side andmetele. Mida sellisel juhul hinnatakse,

[439] EIKo *Roman Zakharov*, p 262.

kas selleks peaks olema eriluba, seda pole sätestatud, mistõttu võib see tähendada, et näiteks julgeolekuasutused saavad ilma ühegi loata püsiva ligipääsu sideandmetele. Nagu ülalpool märgitud, ei ole selge, kuidas jääb nendest tegevustest maha jälg (reguleeritud ei ole logifailide säilitamist ja hävitamist), ei ole võimalik tagada ka tegelikku järelevalvet selle üle.

Alates 2015. aasta 1. jaanuarist teostab õiguskantsler järelevalvet põhiõiguste ja -vabaduste järgimise üle täidesaatva riigivõimu asutuste poolt varjatult isikuandmete ja nendega seonduva teabe kogumise, töötlemise, kasutamise ja järelevalve korraldamisel (ÕKS[440] § 1 lg 9). Seega on olemas sõltumatu isik, kellel on pädevus sellist kontrolli teostada. Samas on seatud õiguskantslerile ka teatud piirangud, näiteks ÕKS § 11^1 lg 6 alusel ei ole õiguskantsleril juurdepääsu salastatud välisteabele või riigisaladusele, mis puudutab:

1) salajasele koostööle kaasatud isikut;
2) julgeolekuasutuse tegevuse salajasel või täiesti salajasel tasemel salastatud meetodeid;
3) julgeolekuasutuse poolt teabe kogumist julgeolekuasutuste seaduse §-s 25 või 26 sätestatud viisil, kui see ei ole veel lõppenud;
4) julgeolekuasutuste rahvusvahelisi ühisoperatsioone või välisriigi või rahvusvahelise organisatsiooni poolt edastatud teavet, kui teabe edastaja ei ole juurdepääsuks nõusolekut andnud.

Seega on julgeolekuasutuste tegevuse üle järelevalve ikkagi piiratud ning ei saa tõsikindlat väita, et õiguskantsleri kontroll on piisav tagatis kuritarvitamiste vastu.

Seoses julgeolekuasutuste tegevusega tuleb peatuda veel ühel järelevalvemeetmel. Nimelt teostab julgeolekuasutuste üle julgeolekuseaduse § 36 alusel järelevalvet Riigikogu julgeolekuasutuste järelevalve komisjon. Selle alusel teavitavad peaminister ja asjaomane minister komisjoni julgeolekuasutuste ja jälitusametkondade tegevusest ja järelevalvest nende tegevuse üle, sealhulgas esitavad vähemalt kord kuue kuu jooksul ülevaate nimetatud küsimustes. Samas on avaldatud kahtlust, kas selle komisjonil on piisavalt pädevust ning ressursse tõhusaks kontrolliks.[441] Kaheldav on ka, kui palju on sellel komisjonil soovi ning ka võimalusi kontrollida seda, kas konkreetsel üksikjuhul oli päringu esitamine sideettevõtjale on piisavalt põhjendatud ning proportsionaalne. Sealjuures on Riigikohtu praktika analüüsis[442]

[440] Õiguskantsleri seadus. - RT I, 30.12.2015, 105.
[441] U. Lõhmus. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. – Juridica 2008/VII, lk 472.
[442] M. Kruusamäe, T. Reinthal. Jälitustegevuse kohtulik eelkontroll Eestis: kohtupraktika analüüs. Tartu 2013, lk 29. http://www.nc.ee/?id=1252 (29.04.2016).

märgitud, et Riigikogu komisjonil võiks lisaks formaalsele ärakuulamiskohustusele olla oluliselt aktiivsem roll, näiteks juhiste või suuniste väljatöötamise õigus.

Järelevalve mehhanismi võib toimuda ka erinevate aruannete avaldamine. Need ülevaated, mida vähemalt kord kuue kuu jooksul esitatakse Riigikogu julgeolekuasutuste järelevalve komisjonile esitatakse, ei ole avalikkusele otseselt kättesaadavad. Avalikkusele on kättesaadavad Riigikogu julgeolekuasutuste järelevalve komisjoni aastaaruanded, milles on lühidalt välja toodud jälitusstatistika.[443] Kuivõrd alates 2013. aastast ei ole elektroonilise side andmete küsimine enam jälitustoiming, siis ei sisalda need aastaaruanded enam neid andmeid, samuti ei sisalda neid enam ka jälitusstatistika aruanded, mida koostab Justiitsministeerium.[444] Seega võib väita, et ESS alusel tehtud andmete päringute üle puudub selge avalikkuse kontroll. Seega kokkuvõtlikult, kuivõrd julgeolekuasutuste puhul ei ole eelkontroll nõutav ning ka järelkontrolli efektiivsuse osas on kahtlused, võib selliseid tagatisi vastavalt EK ja EIK praktikale pidada ebapiisavaks.

Andmete kogumise ja säilitamise üle sideettevõtjate juures ei ole ette nähtud eraldi järelevalvemehhanismi, kuid sellele laieneb Andmekaitse Inspektsiooni järelevalvepädevus ESS § 133 lõike 4 alusel. Vastavalt Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikale peab kontrolli teostama sõltumatu asutus. Käesoleval hetkel puuduvad alusel kahtlemaks Andmekaitse Inspektsiooni sõltumatuses. Samas puudub ka informatsioon selle kohta, kui efektiivne on Andmekaitse Inspektsiooni kontroll tagamaks sideettevõtjate juures hoitavate andmete salajasus. Andmekaitse Inspektsiooni järelevalve ja isikuandmete kaitse seaduse nõuded laienevad ka riigiasutustele. Samas ei kohaldu need nõuded ning Andmekaitse Inspektsiooni järelevalve luure, vastuluure ning ka tausta- ja julgeolekukontrolli käigus kogutud teabele.[445] See näitab taaskord, et julgeolekuasutuste tegevuse osas puudub kindel ning efektiivne järelevalve kord.

Järelevalvesüsteemi kõrval on oluline roll ka isiku teavitamisel. JAS § 29 alusel teavitab julgeolekuasutus isikut, kelle põhiõigusi piiratakse, sh sideandmete edastamisega, kasutatud abinõudest ja põhiõiguste piiramise asjaoludest viivitamatult, kui see ei ohusta piirangu

[443] Ülevaade Riigikogu julgeolekuasutuste järelevalve erikomisjoni tegevusest. 13.01.2014—16.02.2015 Kättesaadav: Riigikogu dokumendiregister.
[444] Aruanne jälitusstatistikast 2013. aastal. Justiitsministeerium http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/jalitusstatistika_aruanne_2013_14022014.pdf (15.04.2016)
[445] A. Lott, lk 34.

eesmärki, või sellise ohu lõppemisel. Riigikogu julgeolekuasutuste järelevalve komisjoni aastaaruandest[446] võib välja lugeda üldise arvu, keda on jälitustegevusest teavitatud. Samas ei anna see informatsiooni selle kohta, kui palju on isikuid teavitatud ESS alusel tehtud päringutest. Lisaks on õiguskantsler oma analüüsis[447] välja toonud, et julgeolekuasutuste poolt kogutud sideandmed on käsitletavad riigisaladuseks oleva teabena RSVS tähenduses, mis salastatakse kuni 50 aastaks (RSVS § 9 p 4). Samuti ei tulene kehtivatest õigusaktidest selget järelevalvemehhanismi teavitamata jätmise põhjendatuse kontrollimiseks ning julgeolekuasutusel on teavitamise võimalikkuse hindamisel lai kaalumisruum, mistõttu on kaheldav, kas teavitamise kohustus on ikka tõhus vahend isiku õiguste kaitsmiseks.[448]

Kriminaalmenetlus seevastu menetlustoimingust teavitamist selgelt ette ei näe, võrreldes näiteks jälitustoimingutega, mille puhul isikut tuleb teavitada. Ebaselge on isikute teavitamine ka väärteomenetluse raames, sest vastavasisulist kohustust seaduses sõnaselgelt ette ei nähta. Isiku teavitamist ei nähta ette ka kriminaalmenetluse väliste toimingute tegemisel, juhul kui on alust arvata, et isik paneb toime kuriteo või kes on kuulutatud tagaotsitavaks. Samas sätestavad isiku taustakontrolli puudutavad seadused[449], et andmete pärimine toimub isiku eelneval kirjalikul nõusolekul ning isikut teavitatakse tema suhtes ettenähtud toimingu tegemisest ning talle tutvustatakse toiminguga kogutud andmeid tema soovil. Erandiks on strateegilise kauba seadus, mille kohaselt tegevusloa andmisel küsitakse isiku andmete kogumiseks kirjulikku nõusolekut, kuid isikut ei teavitata toimingu tegemisest ega võimaldata toiminguga kogutud andmetega tutvuda. Samuti ei teavitata isikut elektroonilise side andmete päringutest tunnistajakaitse seaduse alusel ning seadus ei selgita, kas tsiviilkohtumenetluses raames andmete päringu esitamisel teavitatakse ka kolmandaid isikuid, kes ei ole kohtuasja pooled, kuid kelle sideandmeid see päring puudutab.

Olukorras, kus päringuid tegemisel ei ole eelnevat kohtulikku kontrolli (enamus juhtudel on prokuratuuri kontroll) ning puudub isiku teavitamiskohustus, ei anna regulatsioon üksikisikule piisavalt tagatisi, et riigiasutusele antud õigust ei kuritarvitata. Raskendatud võib olla ka kohtulik järelkontroll. Nimelt on Riigikohus[450] olnud seisukohal, et juhul kui jälitustoiminguga saadakse tõend kriminaalasjas ja kriminaalasi jõuab kohtusse, saab isik kriminaaltoimikuga tutvudes teadlikuks tema suhtes tehtud jälitustoimingust, mille alusel saab isik kohtumenetluses

[446] Ülevaade Riigikogu julgeolekuasutuste järelevalve erikomisjoni tegevusest. 13.01.2014—16.02.2015.
[447] Õiguskantsleri seisukoht 2016, lk 8.
[448] Õiguskantsleri seisukoht 2016, lk 8.
[449] KKVS, MKS, PPVS,TS, VangS, RelvS ja TurvS.
[450] RKPSJKo 3-4-1-42-13, p 49.

taotleda jälitustoimingute seaduslikkuse kontrollimist. Samas ei pruugi enne kriminaalmenetlust kuriteo ärahoidmiseks ja tõkestamiseks ning kriminaalmenetluses tõe väljaselgitamiseks tehtava jälitustoiminguga saadud teave muutuda tõendiks kriminaaltoimikus, näiteks põhjusel, et prokuratuur ei pea vajalikuks või võimalikuks kasutada saadud teavet kriminaalasjas tõendina.[451] Samuti ei pruugi kolmandad isikud, kes ei ole kriminaalmenetluses osalised, kuid kelle põhiõigusi jälitustoiming samuti puudutas, saada teadlikuks jälitustoimingutest.[452] Lisaks ei jõua kõik kriminaalmenetlused, milles jälitustoiminguid tehakse, alati kohtusse.[453] Riigikohus oli seega seisukohal, et olukorras, kus isik ei ole oma põhiõigusi riivavast jälitustoimingust teadlik, on praktiliselt välistatud võimalus kasutada põhiõigust pöörduda oma õiguste kaitseks kohtu poole. Kuivõrd on võimalik, et paljudel juhtudel ei saa isikud nende kohta tehtud päringutest teada, ei saa isikud ennast efektiivselt kaitsta.

Eelnevast võib järeldada, et isikute teavitamise sätestab regulatsioon üksnes üksikutel juhtudel. Samas puudub usaldusväärne ülevaade selle kohta, kui palju praktikas sellest teavitamiskohustusest kinni peetakse. Isiku teavitamata jätmist saaks pidada õigustada aga üksnes juhul, kui on tagatud piisav sõltumatu kontroll – kas siis eelneva kontrolli või järelkontrolli näol, kuid nagu eelnevalt märgitud, on ka kontrolli efektiivsuse suhtes tugevad kahtlused.

3.5. Olemasolevate seisukohtade ümberhindamise vajadus

Elektroonilise side andmete regulatsioonile on andnud hinnangu nii õiguskantsler kui ka Riigikohus. Nagu eespool selgitatud, leidis õiguskantsler[454] oma analüüsi esimeses osas, et andmete ennetava kogumise ja säilitamise regulatsioon, nagu see on ette nähtud ESS §-s 111^1, ei ole selgelt ebamõõdukas ja ei ole seega ka põhiseadusega vastuolus. Hiljuti lisandunud täiendatud seisukohas leidis õiguskantsler lisaks, et läbiviidud abstraktne põhiseaduslikkuse analüüs ei võimaldanud teha järeldust ESS § 111^1 ja muude normidega ette nähtud sideandmete säilitamise ning edasise töötlemise süsteemi vastuolu kohta põhiseadusega, märkides siiski, et

[451] RKPSJKo 3-4-1-42-13, p 49.
[452] RKPSJKo 3-4-1-42-13, p 49.
[453] RKPSJKo 3-4-1-42-13, p 49.
[454] Õiguskantsleri seisukoht 2015, lk 10.

kehtiv sideandmete töötlemise regulatsioon on ebaühtlane ja lünklik ning tuleb terviklikult üle vaadata.[455]

Riigikohtu kriminaalkolleegium on analüüsinud elektroonilise side andmete regulatsiooni lähtuvalt tõendite lubatavuse vaatenurgast ning on leidnud, et see regulatsioon ei ole vastuolus põhiseadusega ulatuses, mis võimaldab taotleda ja kasutada sideettevõtja andmeid kriminaalmenetluses.[456] Nii Riigikohtu kui õiguskantsleri seisukohtadel esineb mitmeid puuduseid, millest järgnevalt tuuaksegi esile olulisem. Nende seisukohtade põhjal tuuakse esile ka olulisemad põhjused, miks nii õiguskantsler kui Riigikohus sellistele hinnangutele on jõudnud.

Õiguskantsler analüüsi esimese osa suurimaks puuduseks oli see, et õiguskantsler hindas üksnes andmete säilitamist, jättes kõrvale andmete kasutamise ning piisavate tagatiste olemasolu kuritarvitamiste vältimiseks. Kuigi vastavalt Euroopa Inimõiguste Kohtu ning Euroopa Kohtu praktikale kujutavad andmete säilitamine ning andmete kasutamine endast eraldiseisvaid riiveid, ei saa siiski neid omavahel lahus käsitleda. Seda seetõttu, et andmete säilitamisel on piisavate tagatiste olemasolu seotud paratamatult sellega, millistele isikutele on tagatud ligipääs ning kuidas hoitakse ära võimalikud kuritarvitused. Sellisel seisukohal oli ka kohtujurist P. C. Villalon kohtuasjas Digital Rights Ireland.[457] Seega on äärmiselt kaheldav, kas üksnes andmete säilitamist saab hinnata eraldi sellest, kellel ja mis tingimustel on nendele andmetele ligipääs ning kellel ja mis tingimustel on õigus neid andmeid kasutada. Seetõttu võib kahtluse alla seada õiguskantsleri seisukoha asjakohasuse elektroonilise side andmete säilitamise regulatsiooni põhiseaduslikkuse kohta.

U. Lõhmus on heitnud õiguskantsleri seisukohale lisaks ette seda, et õiguskantsler õigustas riive mõõdukust kuritegevusega vastase võitlusega, kuid unustas tõenäoliselt asjaolu, et andmete säilitamise regulatsiooni eesmärk ulatub oluliselt kaugemale raskete kuritegude tõkestamisest ja menetlemisest.[458] Nagu käesoleva peatüki esimeses osas leiti, kasutatakse elektroonilise side andmeid tõepoolest väga paljudel erinevatel eesmärkidel, mille puhul tekib nii mõnegi eesmärgi osas kahtlus selle vajalikkusest. Hinnates aga õiguskantsleri analüüsi teist osa, siis selles puudub sisuline riive vajalikkuse kui ka mõõdukuse hindamine ehk põhiõiguse riive tõsisuse ning taotletava eesmärgi tähtsuse kaalumine. Õiguskantsler on siinkohal võtnud mõõdukuse

[455] Õiguskantsleri seisukoht 2016, lk 1 ja 12.
[456] RKKKo 3-1-1-51-14, p 22.4.
[457] EKo 12.12.2013, C-293/12 ja C-594, *Digital Rights Ireland*, kohtujurist P. C. Villalon ettepanek, p 121-122.
[458] U. Lõhmus 2015, lk 744.

hindamisel lähtekohaks EIK ja EK praktikast tulenevad põhimõtted, hinnates mõõdukuse puhul eelkõige järgmist: „Riive intensiivsus on seda suurem, mida kaalukam on riivatav õigus ja mida väiksemad riivega seotud menetluslikud garantiid, kontrollivõimalused jne. Seevastu küllaldaste ja selgete piiritlevate tingimuste, menetluslike garantiide ja kontrollivõimaluste olemasolu võib tasakaalustada ja muuta seega proportsionaalseks ka tõsise eraeluvabadusse sekkumise.“[459] Õiguskantsler tõi esile küll erinevate menetlusgarantiide olemasolu, osaliselt ka nende puudused, kuid ei hinnanud sealjuures üldse seda, kas näiteks haldusmenetluse või väärteomenetluse raames on üldse vajalik elektroonilise side andmetele juurdepääsu ning kas elektroonilise side andmete säilitamine ja kasutamine on selleks eesmärgiks mõõdukas meede.

Kuivõrd õiguskantsler ei hinnanud erinevatel eesmärkidel kehtestatud elektroonilise side andmete regulatsiooni sisuliselt ja põhjalikult, ei ole ka selles toodud lõppjäreldused üllatavad. „Kokkuvõttes tuleb möönda, et sideandmete nõudmise ja edasise töötlemise menetlus on igal konkreetsel alusel erineva eesmärgi ja sisuga, erineva ulatusega menetluslikke garantiisid ja järelevalvemehhanisme sisaldav.“[460] Riive intensiivsuse osas jäi õiguskantsler paljasõnaliseks, viidates, et omanikupäringu ja kõneeristuse tegemisel ei ole eelduslikult tegemist väga intensiivse põhiõiguste riivega, mis ei nõua jälitustoiminguga võrdseid tagatisi.[461] Õiguskantsler lisas: „Abstraktsel hindamisel ei ole seega võimalik väita, et ühelgi ESS § 111^1 lg-s 11 nimetatud alusel teabe töötlemine oleks kitsendavaid asjaolusid arvestades selgelt põhjendamatu ja ebamõõdukas põhiõiguse riive. Ka ei ole võimalik järeldada, et kehtivast sideandmete nõudmise ja edasise töötlemise regulatsioonist puuduks selgelt või täielikult mõni menetluslik garantii või muu menetlust piiritlev asjaolu, milleta ei saa andmete töötlemist kindlasti pidada põhiseaduspäraseks.“[462] „… ei ole välistatud, et kontrollides, kuidas rakendub sideandmete säilitamise ja edasise töötlemise regulatsioon isiku suhtes konkreetsel juhtumil, võib mõni ka käesolevas analüüsis hinnatud norm osutuda (eraldiseisvalt või koostoimes muude normidega) põhiseadusega vastuolus olevaks.“[463]

Õiguskantsler tõi oma analüüsis esile mitmed tõsised puudujäägid, mistõttu jääb arusaamatuks, kuidas sai õiguskantsler sellise võrdlemisi ettevaatliku järelduseni jõuda. Näiteks tõi õiguskantsler välja, et pädeval asutusel on võimalus saada püsiva ligipääsu talle vajalike sideandmete saamiseks vahetult ilma eraldi järelepärimist esitamata, mille üle on praktikas

[459] Õiguskantsleri seisukoht 2016, lk 2.
[460] *Ibid*, lk 11.
[461] *Ibid*, lk 11.
[462] *Ibid*, lk 11.
[463] *Ibid*, lk 12.

võimatu kontrolli teostada.[464] Julgeolekuasutuste laia vabaduse osas viitas õiguskantsler sellele, et kogutav teave on riigisaladus, mis salastatakse 50 aastaks ning JAS-ist ega muudest õigusaktidest ei tulene teavitamata jätmise põhjendatuse kontrollimise selget mehhanismi ning teavitamise võimalikkuse hindamisel on julgeolekuasutusel lai kaalumisruum. Julgeolekuasutuste puhul on ainukeseks efektiivseks menetluslikuks garantiiks isikute teavitamine, mille tegelik toimimine ei ole teada ning mille osas on õiguskantsleri enda sõnul julgeolekuasutustel lai kaalutlusruum. Paljasõnaline on ka järeldus julgeolekuasutuste järelevalvemehhanismi kohta: „Kuigi andmete nõudmine ei eelda julgeolekuasutuse-välise loa saamist, on andmeid võimalik saada siiski ainult julgeolekuasutuse juhi või tema poolt volitatud ametniku korralduse alusel, mis ei kehti kauem kui kaks kuud (JAS § 27 lg 3 ja 4). Seega toimub andmete pikaajalisel kogumisel sama andmesubjekti või sama juhtumi suhtes selle põhjendatuse regulaarne kontrollimine.“[465] Eelnevast tulenevalt on raske mõista, kuidas õiguskantsleril ei tekkinud kahtlusi nende meetmete põhiseaduslikkuses. Formaalselt ühe või kahe menetlusliku garantii olemasolu ei tähenda veel seda, et see on ka piisav ja tõhus.

Põhjused, miks õiguskantsler eelnevalt kirjeldatud seisukohtadele jõudis, on eelkõige see, et elektroonilise side andmete säilitamist ja kasutamist ei nähta sõnumi saladuse kaitsealas olevat ning seda ei nähta niivõrd intensiivse riivena kui seda näeb näiteks Euroopa Kohus. Samuti oli Riigikohtu kriminaal Nii õiguskantsler kui ka Riigikohtu kriminaalkolleegium[466] lähtusid seisukohast, et andmete kogumine, säilitamine ja kriminaalmenetluses kasutamine riivavad õigust eraelu puutumatusele (PS § 26).[467] Õigus eraelu kaitsele on kvalifitseeritud seadusereservatsiooniga põhiõigus, mis tähendab, et seda õigust võib piirata tervise, kõlbluse, avaliku korra või teiste inimeste õiguste ja vabaduste kaitseks, kuriteo tõkestamiseks või kurjategija tabamiseks. PS §-s 43 sätestatud sõnumisaladust on lubatud rikkuda üksnes kohtu loal kuriteo tõkestamiseks või kriminaalmenetluses tõe väljaselgitamiseks. Elektroonilise side andmete kogumist on peetud nii seadusandja poolt[468] kui ka õiguskirjanduses[469] kuuluvaks just PS §-s 26 sätestatud eraelu kaitsealasse, mitte PS §-s 43 sätestatud sõnumisalade kaitsealasse.[470]

[464] *Ibid*, lk 6.
[465] *Ibid*, lk 8.
[466] RKKKo 3-1-1-51-14, p 22.
[467] *Ibid*.
[468] Näiteks KrMS muutmise seaduse muutmise eelnõus. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri, Kättesaadav: http://www.riigikogu.ee/?op=ems&page=eelnou&eid=86dde8ff-c50e-48ba-a39ea325fe15a3f0& (14.04.2016). Lk 4.
[469] S. Laos. PõhiS § 43/6 – Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012.
[470] Vt lisaks A. Lott, lk 27.

U. Lõhmuse selgituste kohaselt välistas Eesti sõnumite edastamise andmed sõnumite saladuse kaitsealast USA eeskujul.[471]

See selgitab, miks õiguskantsler leidis oma analüüsi esimeses osas riive mõõdukuse hindamisel, et „riive intensiivsust vähendab selle piirdumine üksnes side tehniliste andmetega ning sõnumite sisu mittekajastumine salvestatavate andmete hulgas.“[472] Seega ei ole seadusandja, Riigikohus ning õiguskantsler näinud elektroonilise side andmete säilitamist ja kasutamist niivõrd intensiivse riivena. Just sellel põhjusel pidas õiguskantsler lubatavaks neid elektroonilise side regulatsiooni eesmärke, mis ei ole seotud otseselt kuritegude menetlemisega.[473]

See lähenemine erineb oluliselt Euroopa Kohtu[474] seisukohast, kellel hinnangul võimaldavad meta-andmed teha väga täpseid järeldusi isikute eraelu kohta, näiteks nende igapäevaelu harjumuste, alalise või ajutise elukoha, igapäevaste või muude liikumiste, tegevuste, sotsiaalsete suhete ja ühiskonnagruppide kohta, kellega nad läbi käivad. Samuti on Euroopa Inimõiguste Kohus mitmel juhul käsitlenud elektroonilise side andmeid kuuluvat just sõnumisaladuse kaitsealasse. Näiteks kohtuasjas Copland vs the United Kingdom[475] leidis EIK, et isiku telefoni, e-maili ja interneti kasutamise informatsiooni kogumise ja säilitamisega sekkutakse nii isiku eraelusse kui ka sõnumisaladusse. Kohtuasjas Malone vs the United Kingdom[476] oli EIK samuti seisukohal, et andmed valitud numbrite kohta kommunikatsiooni osaks. Sõnumite edastamise andmed kuuluvad sõnumisaladuse kaitsealasse samas erinevates Euroopa riikides, näiteks Saksamaal ja Prantsusmaal, kaitsetes samamoodi nii kommunikatsiooni sisu kui ka kommunikatsiooni protsessi.[477]

Siinkohal kerkib küsimus, kas Eesti õiguses on vahetegu sõnumisaladuse ning elektroonilise side andmete kaitsetasemes õigustatud. A. Lotti[478] hinnangul võib selline seadusandja otsus käsitada metaandmeid väljaspool PS § 43 kaitseala olla vastuolus sõnumite saladuse kaitseala eesmärgiga. Seda seetõttu, et meta-andmed võimaldavad luua väga selge ülevaate isiku elust ning nende andmete roll infoühiskonnas viitab pigem selliste andmete kaitse taseme

[471] U. Lõhmus 2008, lk 467.
[472] Õiguskantsleri seisukoht 2015, lk 7.
[473] Õiguskantsleri seisukoht 2015, lk 5.
[474] EKo *Digital Rights Ireland*, p 27.
[475] EIKo 03.04.2007, 62617/00, *Copland vs the United Kingdom*, p 41, 44.
[476] EIKo *Malone vs the United Kingdom*, p 84.
[477] U. Lõhmus 2008, lk 467.
[478] A. Lott, lk 27.

vähendamise asemel pigem tugevdamise või säilitamise vajadusele.[479] See seisukoht ühtib kahtlemata Euroopa Kohtu seisukohaga, mille kohaselt kujutab ka meta-andmete säilitamine väga intensiivset riivet. Nagu eelnevalt selgitatud, ei nähta sageli sellist inimeste jälgimist nii riivava meetmena, mida kinnitavad ka õiguskantsleri ning Riigikohtu seisukohad. Loodetavasti hakkab selline arusaam siiski lähitulevikus muutuma, võttes rohkem arvesse nii Euroopa Kohtu kui Euroopa Inimõiguste Kohtu praktikat.

Lootust selleks annab näiteks riigikohtunike Saale Laose ja Eerik Kergandbergi eriarvamus kriminaalasjas nr 3-1-1-51-14, milles riigikohtunikud avaldasid kahtlust, kas spetsiifiliselt kriminaalmenetluses kehtivad lisapiirangud nagu nt seotus teatud raskusega kuriteoga ja vältimatu vajadus konkreetses kriminaalmenetluses legitimeeriksid kõigi isikute andmete võrdlemisi pikaajalist säilitamist. Nende hinnangul jääb alles küsimus menetlusgarantiide piisavusest ja see oleks vajanud ka selles kriminaalasjas põhjalikumat analüüsida.[480] Selle põhjalikum analüüsimise oleks toonud ehk teistsuguse lahendi, sest nagu käesolevas töös leiti, ei ole pakutavad menetlusgarantiid vastavalt Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikale piisavad, mistõttu ei pruugi kõigi isikute andmete säilitamine ning võrdlemisi pikaajaline säilitamine olla õigustatud.

Olulise suunamuutuse kehtivas praktikas ning hinnangutes võivad kaasa tuua lähiaastatel vastuse saavad kohtumenetlused, eelkõige eelotsusetaotlusega kohtuasjades Tele2 Sverige AB versus Post- och telestyrelsen ja Davis jt ning Euroopa Inimõiguste kohtus menetluses oleva taotlusega kohtuasjas Big Brother Watch and Others v. The United Kingdom (vt selgitusi eespool). Esimesed kaks neist on eriti olulised, sest need puudutavad otseselt seda, millistele tingimustele peab elektroonilise side andmete regulatsioon vastama. Sealjuures on oluline meeles pidada, et isikuandmete kaitset elektroonilise side sektoris reguleerib direktiiv 2002/58/EÜ, mis tähendab seda, et andmete säilitamise regulatsioon kuulub Euroopa Liidu põhiõiguste harta kohaldamisalasse ning Euroopa Kohtul on selles asjas oluline sõnaõigus.[481] Sealjuures tähendab see seda, et Euroopa Kohtu tõlgendused on Eesti kohtutele siduvad. Seega sõltub elektroonilise side andmete regulatsiooni tulevik paljuski Euroopa Kohtu tõlgendustest ning on tõenäoline, et Eesti peab sellest tulenevalt selle regulatsiooni lähiajal üle vaatama, et viia see kooskõlla proportsionaalsuse põhimõttega.

[479] A. Lott, lk 27.
[480] RKKKKo 3-1-1-51-14, Riigikohtunike Saale Laose ja Eerik Kergandbergi eriarvamus, p 6.
[481] U. Lõhmus 2015, lk 742.

KOKKUVÕTE

Käesoleva töö eesmärgiks oli välja selgitada, milline on privaatsusõiguse piiramise õiguslik raamistik ning milliseid aspekte tuleks riigipoolsete jälgimismeetmete kehtestamisel arvesse võtta. Töö fookuses oli seega küsimus, kuidas peaks toimuma riigipoolse jälgimistegevuse kui privaatsusõiguse riive proportsionaalsuse hindamine, et saavutada tasakaalu privaatsusõiguse ja julgeoleku huvide vahel. Töö eesmärgist tulenevalt püstitati töös kaks hüpoteesi. Esiteks seati hüpotees, et inimeste privaatsusesse sekkumine selliste meetmetega, mis lubavad automaatselt paljude isikute kohta andmete kogumist, on lubatud üksnes väga rangetel ning erandlikel tingimustel. Teiseks hüpoteesiks püstitati väide, et Eestis toimuv elektroonilise side andmete lauskogumine väljub lubatud julgeoleku eesmärkide raamidest, mis ei vasta Euroopa Kohtu ja Euroopa Inimõiguste Kohtu rangetele ning erandlikele tingimustele.

Uurimistöö hüpoteesi kontrollimiseks analüüsiti esmalt seda, milline tähendus on privaatsusõigusel ning milliseid tagajärgi võib tuua kaasa liigne privaatsusesse sekkumine. Privaatsusõigusele ei ole ühtset kindlat definitsiooni, kuid seda võib määratleda isiku eraelulist sfääri, milles isikul on õigus otsustada, kas ja kui palju ta oma eraelu teiste inimeste, avalikkuse ja riigiga jagab. Selle sisu aitavad paremini mõista privaatsuse erinevad elemendid, mis määravad privaatsusõiguse kaitseala. Olulisemad neist on näiteks õigus kehalisele ja vaimsele terviklikkusele, mis hõlmab õigust olla kaitstud kehaliste rünnete ja paljastuste eest, samuti soovimatu jälgimise eest ning tungimise eest koju ja töökohta eest. Samuti hõlmab privaatsusõiguse kaitseala isikuandmeid, mis tähendab seda, et isikul on õigus kontrollida temaga seotud andmete kogumist, kasutamist ja avalikustamist.

Privaatsus on demokraatliku ning liberaalse ühiskonna alustalaks, olles lahutamatult seotud nii isiku vabaduse kui inimväärikusega. Oluline on sealjuures silmas pidada seda, et privaatsus ei ole üksnes isiku erahuvi, vaid see on samaaegselt ka avalik huvi, olles kasulik ühiskonnale laiemalt. Privaatsus on oluline ühiskonnale seetõttu, et see võimaldab isikul ennast realiseerida ning olla ühiskonnas vaba teiste sekkumisest, mis aitab tagada ühiskonnas vabatahtlikku käitumisreeglite järgimist. Inimestele on oluline omaette olemise ruum ning võimalus suhelda teiste inimestega vabalt ja ausalt. Privaatsus on oluline ka majanduslikus ja poliitilises mõttes, sest võimaldab inimestel olla innovaatilised ning vabad oma mõtlemises, argumenteerimises ja otsustamises.

Igal isikul on õigus privaatsuse kaitseks sõltumata sellest, kas inimesel on midagi varjata või kas isik tunneb ise otseselt vajadust privaatsuse kaitse järele. Inimeste massilise jälgimisega võivad kaasneda mitmed negatiivsed mõjud, näiteks ei julge inimesed välja tulla uute, teistsuguste ideedega ning ei julgeta teha midagi sellist, mida teised peaksid tavapärasest teistsugusest. Seda seetõttu, et kui inimene teab, et teda jälgitakse, võtab ta paratamatult arvesse seda, kuidas tema tegevused tunduvad kõrvaltvaatajale. See toob kaasa enesetsensuuri. Sealjuures mõjutab jälgimine paratamatult jälgija ja jälgitava omavahelist võimu tasakaalu, andes jälgijale suurema võimu mõjutada või suunata järelevalve subjekti.

Teiseks analüüsiti käesolevas töös seda, millistel eesmärkidel ning juhtudel on privaatsusõigusesse sekkumine lubatud. Euroopa inimõiguste konventsiooni kohaselt ei tohi ametivõimud privaatsusõigusesse sekkuda muidu, kui kooskõlas seadusega ja kui see on demokraatlikus ühiskonnas vajalik riigi julgeoleku, ühiskondliku turvalisuse või riigi majandusliku heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks. Euroopa Liidu õiguses tohib õiguste ja vabaduste teostamist piirata ainult seadusega ning arvestades nimetatud õiguste ja vabaduste olemust ning piiranguid võib seada üksnes juhul, kui need on vajalikud ning vastavad tegelikult liidu poolt tunnustatud üldist huvi pakkuvatele eesmärkidele või kui on vaja kaitsta teiste isikute õigusi ja vabadusi. Nii Euroopa inimõiguste konventsioon kui ka Euroopa Liidu õigus peavad riigi julgeolekut, ühiskondlikku turvalisust ning korratuse või kuritegude ärahoidmist legitiimseteks eesmärkideks, mille jaoks on riikidel õigus võtta kasutusele salajase jälgimise meetmeid.

Kolmandana analüüsiti seda, kuidas on Euroopa Kohus ja Euroopa Inimõiguste Kohus hinnanud jälgimise, eelkõige isikute salajase jälgimise, massijälgimise ning automaatse andmete kogumise kui privaatsusõiguse riive proportsionaalsust julgeoleku, kuritegude avastamise ja ärahoidmise või avaliku korra eesmärgil. Esiteks on kohtupraktika nõudnud seda, et eraellu sekkumiseks peab olema piisav seaduslik alus. Selle on osas märgitud, et kuna salajane jälgimine ei toimu isiku või avalikkuse järelevalve all, peab seadus võimorganitele ja kohtutele ette nägema selge kaalutlusõiguse ulatuse ning selle rakendamise viisi, mis peavad olema piisavalt selged, et anda üksikisikule piisav kaitse omavolilise sekkumise eest. Kohtute hinnangul on olemas selge risk kuritarvituste esinemiseks olukorras, kus täidesaatvat võimu teostatakse salajas. Selle ärahoidmiseks on kohtupraktikas kujundatud loetelu miinimumtagatistest, mis peaksid olema sätestatud riigisisese õiguses. Nende tagatiste piisavust on Euroopa Inimõiguste Kohus sageli hinnanud koos meetme proportsionaalsuse hindamisega,

sest kohtu hinnangul on tagatised otseselt seotud sellega, kas sekkumine on demokraatlikus ühiskonnas vajalik.

Kohtute hinnangul vastab sekkumine vajalikkuse kriteeriumile, kui riive vastab tungivale ühiskondlikule vajadusele, kui see on proportsionaalne soovitud legitiimse eesmärgi suhtes ning kui riigivõimu põhjused riive põhjendamiseks on asjakohased ning piisavad. Seoses riikliku julgeolekuga on Euroopa Inimõiguste Kohus märkinud, et riikidel on lai kaalutlusõigus valimaks vahendeid, kuidas tagada riiklikku julgeolekut. Sõltumata laiast kaalutlusõigusest ei või riigid terrorismi vastu võitlemise nimel võtta vastu ükskõik milliseid meetmeid, mis nende arvates on sobivad, vaid seaduses peavad eksisteerima piisavad ning efektiivsed tagatised.

Tagatiste olemasolu on Euroopa Inimõiguste Kohtu hinnangul eriti oluline olukordades, kus isikuandmeid töödeldakse automaatselt ning riigiasutustel on tehniliselt otsene ligipääs kõigi isikute kommunikatsioonile. Ka Euroopa Kohus on elektroonilise side andmete massilise kogumise osas võtnud seisukoha, et see kujutab endast eraelu ning isikuandmete kaitse põhiõiguste ulatuslikku riivet, mida tuleb pidada eriti raskeks. Kohtu hinnangul võib asjaolu, et andmete säilitamine ja hilisem kasutamine toimuda isikut sellest teavitamata, tekitada isikutes tunde, et nende eraelu jälgitakse pidevalt. Seega, kui on võimalik massijälgimine, siis peaksid tagatised vastavalt riive intensiivsusele olema veelgi tugevamad. Sel põhjusel on nii Euroopa Inimõiguste Kohus kui ka Euroopa Kohus leidnud, et salajase jälgimise meetmed on lubatud üksnes siis, kui need on rangelt vajalikud. Seega on proportsionaalsuse puhul peetud vajalikuks hinnata seda, kas piiravate meetmete määramise ja rakendamise järelevalvekord suudab tagada, et õigusaktiga lubatud sekkumine on selline, mis on demokraatlikus ühiskonnas rangelt vajalik.

Nii Euroopa Kohus kui Euroopa Inimõiguste Kohus on üheks kõige olulisemaks tagatiseks pidanud jälgimismeetmete täpse rakendamise ulatuse piiritlemist, millest selgub, milliste süütegude puhul neid meetmeid võib kasutusele võtta. Massilise või salajase jälgimise puhul peab andmete kogumine ja kasutamine olema piiritletud üksnes väga tõsiste kuritegudega ning riigisisene õigus peab selgelt defineerima, mida selliste kuritegude all mõeldakse.

Teiseks oluliseks tagatiste grupiks on isikute ringi ning aja piiritlemine riigisiseses õiguses. Periood, mille jooksul on lubatud jälgimistegevusi läbi viia või kui kaua võib jälgimisega saadud andmeid säilitada, mõjutab otseselt isiku eraellu sekkumise riive tugevust. Seega peab riigisisene õigus ette nägema selged ajaperioodid, millal jälgimistegevusi võib teostada või kogutud andmeid säilida, nähes ette vajadusel asutuste selged kaalutlusõiguse piirid nende

perioodide määratlemiseks. Samuti peab isikute ring, kelle suhtes jälgimismeetmeid läbi viiakse, olema selgelt määratletud. Olukord, kus andmeid kogutakse isikute kohta, kelle kohta pole mingeid tõendeid, mille põhjal võiks arvata, et nende käitumisel oleks kasvõi kaudne või kauge seos raskete kuritegudega, ei ole Euroopa Kohtu hinnangul kooskõlas proportsionaalsuse põhimõttega. Nendele tagatistele on lisaks oluline, et riigisisene õigus sätestaks täpsed reeglid jälgimisega saadud andmete hoiustamise, kasutamise, edastamise ja hävitamise jaoks, et vähendada riski, et andmetele pääsetakse ligi ilma volituseta või avalikustatakse ilma loata.

Väga oluliseks tagatiseks isiku õiguste kaitsel on tõhusa järelevalvesüsteemi olemasolu ning isiku teavitamine tema suhtes kasutuselevõetud meetmest ehk isiku teavitamine tema põhiõiguste riivest. Järelevalvesüsteem võib hõlmata nii kohtulikku kontrolli (eelnevat või järelkontrolli) või muud sõltumatut kontrolli, näiteks parlamentaarset kontrolli. Sellistes valdkonnades, kus õiguste kuritarvitamine on üksikjuhtudel väga kergesti võimalik, on soovitatav usaldada kontroll kohtunikule. Euroopa Inimõiguste Kohtu praktikast tulenevalt peab ka kohtulik kontroll vastama teatud nõuetele. Eelkõige peab kohtul olema sisuline pädevus hinnata, kas taotletav meede on kooskõlas vajalikkuse ja proportsionaalsuse nõudega. Järelevalve süsteemi kõrval on oluline roll ka isiku teavitamisel jälgimismeetmetest, millest sõltub otseselt see, kas saab isik oma õigusi võimaliku kuritarvitamisel korral kaitsta.

Eelnevast tulenevalt leidis kinnitust töö esimene hüpotees, et inimeste privaatsusesse sekkumine selliste meetmetega, mis lubavad automaatselt paljude isikute kohta andmete kogumist, on lubatud üksnes väga rangetel ning erandlikel tingimustel. Seda kinnitavad Euroopa Inimõiguste Kohtu ja Euroopa Kohtu kohtupraktika, mis nõuavad piisavate tagatiste olemasolu riigisiseses õiguses.

Viimasena analüüsiti seda, kuidas vastab Eesti elektroonilise side andmete regulatsiooni alusel massiline sideandmete kogumine Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktika tingimustele. Eesti regulatsioon läheb oluliselt kaugemale julgeoleku ning raskete kuritegude tõkestamise ja menetlemise eesmärgist, mis oli algselt elektroonilise side andmete regulatsiooni väljatöötamise eesmärgiks. Sealhulgas kogutakse ning kasutatakse neid andmeid ka vähem tähtsate kuritegude uurimiseks, väärtegude uurimiseks, haldusmenetlustes taustakontrolli tegemiseks, riikliku järelevalve teostamiseks, tunnistajakaitse andmise menetluses ning tsiviilkohtumenetluses. Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktika kohaselt võib sellist massilist andmete kogumist kasutada üksnes raskete kuritegude avastamiseks, ärahoidmiseks ning menetlemiseks, mistõttu peab nende süütegude loetelu olema väga kitsalt

piiritletud, mille puhul võib andmeid koguda ning kasutada. Seega ei vasta Eesti regulatsioon selles osas kohtupraktikas sätestatud tingimustele ning võib kahelda selle vastavuses rangelt vajalikkuse põhimõttele.

Elektroonilise side andmeid kogutakse eranditult kõikide isikute kohta ning nendele andmetele on ligipääs väga paljudel ametiasutustel. Sealjuures ei ole kriminaalmenetluses, väärteomenetluses, tsiviilkohtumenetluses ning julgeolekuasutuste poolt läbiviidavas menetluses piiritletud, milliste isikute kohta andmepäringuid esitada tohib. Erinevate seaduste alusel on ligipääs elektroonise side andmetele Politsei- ja Piirivalveametil, Kaitsepolitseiametil, Teabeametil, Maksu- ja Tolliametil, Konkurentsiametil, Sõjaväepolitseil, Keskkonnainspektsioonil, Justiitsministeeriumi vanglate osakonnal, Andmekaitse Inspektsioonil, Finantsinspektsioonil ning vanglatel ja tsiviilkohtutel. Selline lai isikute ring ei ole kooskõlas Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikaga.

Seoses ajaliste piiridega jätab Eesti regulatsioon määratlemata, millistel tingimustel võib Vabariigi Valitsus andmete säilitamise tähtaegasid pikendada ning kui pikaks perioodiks. Samuti pole määratletud, millistest tingimustest tuleb lähtuda päringu esitamisel perioodi määratlemisel. Selliselt on võimalik, et andmete säilitamise tähtaega pikendatakse ning andmeid küsitakse sellise perioodi kohta, mis ei ole rangelt vajalik, nagu nõuab Euroopa Inimõiguste Kohtu ja Euroopa Kohtu praktika.

Samuti on elektroonilise side andmete hoiustamise, kasutamise, edastamise ja hävitamise reeglid sätestatud üldiselt ning ei ole võimalik kindlaks teha, kas need reeglid välistavad kuritarvitamise ohu. Olulisemateks puudusteks on see, et regulatsioon ei selgita, kas juba kord kogutud ja kasutatud andmeid võib kasutada ka teistes kriminaal- või muudes menetlustes ning milliseid andmete säilitamise ja hävitamise nõudeid peab sellisel juhul järgima. Lisaks on murettekitav see, et asutustel on võimalik lisaks päringute esitamisele saada elektroonilise side andmetele ligipääs ka püsivalt, mille järelkontrolli võimalused ei ole selged. Seega ka selles osas ei vasta Eesti regulatsioon kohtupraktikas sätestatud tingimustele.

Järelevalvesüsteemide osas näeb Eesti õigus erinevad lahendused: andmete päring võib toimuda prokuratuuri loa alusel, kohtu loa alusel, isiku nõusolekul või asutuse juhi või tema poolt volitatud isiku loa alusel või ilma ühegi loata. Kuigi prokuratuuri ja kohtu loa näol on formaalselt järelevalvesüsteem olemas, ei taga see siiski sisulist ning tõhusat eelkontrolli, nagu nõuab kohtupraktika. Euroopa Inimõiguste Kohtu praktikaga on kõige ilmsemalt vastuolus see,

et julgeolekuasutused saavad ligipääsu andmetele ühegi eelneva loata olukorras, kus ei ole selgelt tugevat järekontrollisüsteemi ning julgeolekuasutustel on lai kaalutlusruum isikute teavitamise otsustamisel. Kohtupraktikas sätestatud tingimustega läheb vastuollu ka see, et näiteks kriminaalmenetluse ning väärteomenetluse raames ei nähta isiku teavitamise kohustust selgelt ette. Olukorras, kus ei ole tagatud kohtulikku järelkontrolli ning puudub ka teavitamiskohustus, ei anna regulatsioon üksikisikule piisavalt tagatisi õiguste kuritarvitamise vastu.

Kokkuvõtlikult kinnitas analüüs hüpoteesi, et Eestis toimuv elektroonilise side andmete lauskogumine väljub piiritletud julgeoleku eesmärkide raamidest ning see ei vasta Euroopa Kohtu ja Euroopa Inimõiguste Kohtu praktikas sätestatud rangetele ning erandlikele tingimustele.

Nii Riigikohus kui õiguskantsler on senistes analüüsides leidnud, et olemasolev elektroonilise side andmete regulatsioon ei ole vastuolus põhiseadusega. Nendel on analüüsidel mitmeid puudusi, mistõttu ei saa nõustuda nende analüüsides tehtud järeldustega. Muude puuduste hulgas jättis õiguskantsler hindamata selle, kas näiteks väärteomenetluse või riikliku järelevalve raames on üldse vajalik elektroonilise side andmetele juurdepääsu ning kas elektroonilise side andmete säilitamine ja kasutamine on selleks eesmärgiks mõõdukas meede. Põhjuseks, miks nii Riigikohus kui ka õiguskantsler põhiseadusega vastuolu ei tuvastanud, on tõenäoliselt see, et elektroonilise side andmete säilitamist ja kasutamist ei nähta niivõrd intensiivse riivena kui seda näeb näiteks Euroopa Kohus. Elektroonilise side andmete jälgimine võimaldab teha siiski väga olulisi järeldusi inimeste elu kohta, mistõttu vajaks senine seisukoht lähitulevikus ümberhindamist.

Isikuandmete kaitse elektroonilise side sektoris kuulub Euroopa Liidu pädevusse, mis tähendab ühtlasi seda, et elektroonilise side andmete säilitamise ja kasutamise meetmete proportsionaalsuse hindamisel on oluline sõnaõigus Euroopa Kohtul. Lähiajal on tulemas nii Euroopa Kohtust kui ka Euroopa Inimõiguste Kohtust olulised kohtulahendid, mis võivad oluliselt täiendada või muuta seniseid seisukohti inimeste massilise jälgimise lubatavuse tingimuste osas. Sinnamaani vajaksid lähtuvalt olemasolevast Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikast analüüsimist ka lennureisijate broneeringuinfo, hotellikülastajate andmekogu ja miks ka mitte kiiruskaamerate regulatsioon, et välistada võimalikku vastuolu Euroopa Kohtu ning Euroopa Inimõiguste Kohtu praktikaga.

SUMMARY

The legal framework for the interference with privacy according the European Court of Human Rights and European Court of Justice

During the recent decade national governments have been under constant pressure to address terrorism threats putting privacy under serious pressure. The aim of this thesis was to establish what the current framework for limiting the right to privacy is and which aspects should be considered when applying state surveillance measures. Therefore the focus was laid on the question how to assess the proportionality of the interference with privacy of the state surveillance. In this thesis two hypothesis were set: 1) interference with privacy, with measures that automatically allow gathering large amount of data, is allowed only on very strict and limited circumstances; 2) mass surveillance of telecommunication data in Estonia goes further from strict security reasons and is not in conformity with the strict and limited circumstances as prescribed by the European Court of Justice (ECJ) and European Court of Human Rights (ECHR).

In order to verify the hypothesis the meaning of the privacy and the consequences of excessive interference to privacy was analysed. There is no unified definition for the right to privacy but in general it can be described as person`s private sphere where autonomous decision can be made, concerning how much of it is shared with other individuals, general public or the state. The essence of privacy can be better understood by the elements which are subject to the protection of privacy. Most important of these are freedom from interference with physical and psychological integrity, which include the right to be protected from physical assaults and exposure, unwanted surveillance, intrusion into home and workplace of the individual. In the same way privacy protects personal data which means that individuals have right to control the collection, use and disclosure of the data related to that specific person.

Privacy, being inseparably linked with both individual freedom and human dignity, is the foundation of a democratic and liberal society. It is important to note that privacy is not only in the interest of the individual but also in the interest of the public as it is beneficial to the society as a whole. For the society privacy is important because it allows individuals to realize themselves and to be free from the intervention of others which in return helps to secure the compliance of the rules of conduct in the society. It is important for individuals to have personal

space and opportunity to associate with others in a free and sincere way. Privacy is important also in a political and economic sense as it allows people to be innovative and free in their thoughts, argumentation and decision-making.

Every individual has the right to privacy irrespective of the individual has something to hide or whether the individual seeks for privacy. Mass surveillance can have several negative consequences. For example people are afraid to form new ideas or to do something that differs from the mainstream thoughts or behaviour. It is because individuals, knowing that they are being observed, take into account the perspective of the observer and this will lead to self-censorship. In addition, observation influences the balance of power between the observer and the subject giving the observer more power to influence or direct the observed subject.

Secondly, the thesis focused on the legitimate aims for interfering privacy and on the terms interference to privacy is allowed. According to the European Human Rights Convention there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others. According to EU law, any limitation on the exercise of the rights and freedoms must be provided for by law and respect the essence of those rights and freedoms. Subject to the principle of proportionality, limitations may be made only if they are necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.

The thesis focused on how ECJ and ECHR have assessed the proportionality of the limitations to privacy from the point of view of secret surveillance, mass surveillance and automatic data retention. According to the court practice, the interference to privacy should first have sufficient legal basis. In case the implementation of the law consists of secret measures, which is not open to scrutiny by the individuals concerned or by the public at large, the law itself must indicate the scope of any discretion conferred on the competent authority with sufficient clarity to give the individual adequate protection against arbitrary interference. In cases where the executive power is exercised in secret, the risks of arbitrariness are evident. Therefore, the ECHR has developed several minimum safeguards that should be set out in law in order to avoid abuses of power. These safeguards are usually assessed together with the necessity assessment as in

the court's opinion, safeguards are directly related to the questions whether interference is necessary in democratic society.

An interference will be considered necessary in a democratic society for a legitimate aim if it conforms with a pressing social need and if it is proportionate to the legitimate aim pursued and if the reasons adduced by the national authorities to justify it are relevant and sufficient. The ECHR has recognised that the national authorities enjoy a fairly wide margin of appreciation in choosing the means for achieving the legitimate aim of protecting national security. However, this does not mean that the states enjoy an unlimited discretion to subject persons within their jurisdiction to secret surveillance.

The need for safeguards is all the greater where the protection of personal data undergoing automatic processing is concerned and where the secret services and the police have direct access to all communications. According to ECJ, automatic data retention must be considered to be particularly serious. The fact that data are retained and subsequently used without the user being informed is likely to generate in the minds of the persons concerned the feeling that their private lives are the subject to constant surveillance. Therefore, both ECHR and ECJ have required that that the limitations in relation to the protection of personal data must apply only in so far as is strictly necessary.

The first safeguard to be prescribed by law is that the law must define the scope of application of secret surveillance measures by giving citizens an adequate indication as to the circumstances in which public authorities are empowered to resort to such measures – in particular by clearly setting out the nature of the offences which may give rise to interference. The use of mass surveillance or secret surveillance measures should be limited only to investigation of serious crimes.

Secondly, a definition of the categories of people and the limit on the duration of the interference, should be defined. The duration of interference affects directly the seriousness of the interference. Therefore, the law should prescribe the time limits or define the limits of discretion of the authorities. The situation where all persons and all means of electronic communication as well as all traffic data without any differentiation, limitation or exception is being collected cannot be in accordance with the principle of proportionality. In addition, the law must provide specific procedures to be followed for examining, using, storing and

destroying the data obtained, together with precautions to be taken when communicating the data to other parties.

In addition, it is very important to have sufficient and effective supervision and review system for monitoring the use of surveillance measures. The judicial decisions authorising interception should contain reasons and refer to specific grounds for suspecting that a criminal offence has been committed. In addition to supervision system, subsequent notification of surveillance measures is inextricably linked to the effectiveness of remedies before the courts and therefore very important safeguard against the abuse of monitoring powers.

Previously outlined showed that the first hypothesis was proven right – the interference with privacy with measures that automatically allow gathering large amount of data is allowed only on very strict and limited circumstances.

In the last part of the thesis, Estonian electronic data retention regulation was analysed compared to the court practice of ECJ and ECHR. It was discovered that Estonian electronic data retention regulation is used for various purposes which goes significantly further from the original purpose of the regulation – the protection of security and fighting serious crimes. Electronic data is used for small crimes, misdemeanours and it is also used in the course of state supervision, administrative procedure and civil court procedure. Therefore, the Estonian law seems not to comply with the principle of strictly necessary.

As the electronic data is used for different purposes, the list of authorities who can access this data is very wide. In several cases, the law does not prescribe the circle of persons concerning who the electronic data might be used. Therefore this does not comply with the ECJ and ECHR court practice which obliges to define exactly the categories of people being concerned and persons who have access to this data. In relation to time limits the law does not give precise circumstances when and how to extend the time limits. In addition, it is possible that more electronic data might be used than strictly necessary in specific case.

Concerning the review system and subsequent notification, there are several deficiencies and gaps in the current legislation. The most problematic is the fact the secret service has access to electronic data without prior authorisation and the review system does not ensure efficient protection. In addition the secret service holds a wide discretion on deciding on the subsequent notification. Therefore, the second hypothesis was also proven right - mass surveillance of

telecommunication data in Estonia goes further from strict security reasons and is not in conformity with the strict and limited circumstances as prescribed by ECJ and ECHR.

Chancellor of Justice and the Supreme Court have previously analysed the data retention regulation in Estonian law, but so far they have not reached the conclusion that data retention regulation is not in conformity with the principle of proportionality. The main reason for it is probably the fact that the Chancellor of Justice and the Supreme Court have not seen the interference with private life as serious as it has been considered by the ECJ and ECHR. As there is new court practice coming concerning data retention and mass surveillance from both ECJ and ECHR, there is hope that the positions of the Chancellor of Justice, the Supreme Court and the government of Estonia will change already in the nearest future.

KASUTATUD ALLIKATE LOETELU

Teaduskirjandus

1. R. Alexy. Põhiõigused Eesti põhiseaduses. – Juridica eriväljaanne 2001.
2. Y. Arai-Takahashi. The Margin of Appreciation Doctrine and the Principle of Proportionality in the Jurisprudence of the ECHR. Antwerpen: Intersentia 2002.
3. J. C. Buitelaar. Privacy: Back to the Roots. − German Law Journal 2012/13.
4. J. Cohen. Examined lives: Informational Privacy and the Subject as Object. – Stanford Law Review 2000/52.
5. O. Diggelmann and M. N. Cleis. How the Right to Privacy Became a Human Right. – Human Rights Law Review, 2014/14.
6. J. Griffin. The Human Right to Privacy. - San Diego Law Review 2007/44.
7. J. Holvast. History of Privacy. Berlin: Springer Heidelberg, 2008.
8. K. Lachmayer, N. Witzleb. The challenge to privacy from ever increasing state surveillance: a comparative perspective. - UNSW Law Journal. 2014/37.
9. K. Lenaerts. Exploring the Limits of the EU Charter of Fundaments Rights. – European Constitutional Law Review 2012/8.
10. G. Letsas. The ECHR as a living instrument: its meaning and legitimacy. In Constituting Europe. The European Court of Human Rights in a National, European and Global Context. Edited by A. Follesdal, B. Peters, G. Ulfstein. Cambridge University Press: Cambridge 2013.
11. U. Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. – Juridica 2015/X.
12. U. Lõhmus. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. – Juridica 2008/VII.
13. D. Lyon. Surveillance Studies. Cambridge: Polity Press 2007.
14. J. McBride. Proportionality and the European Court of Human Rights. In The Principle of Proportionality in the Laws of Europe, edited by E. Ellis, 23–36. Oxford: Hart Publishing 1999.
15. J. Milaj. Invalidation of the data retention directive: extending the proportionality test. – Computer Law & Security Review 2015/31.
16. Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012.
17. R. Maruste. Konstitutsionalism ning põhiõiguste ja –vabaduste kaitse. Tallinn: Juura 2004.

18. M. Männiko. Õigus privaatsusele ja andmekaitse. Tallinn: Juura 2011.
19. N. A. Moreham. The right to respect for private life in the European convention on human rights: a re-examination. – European Human Rights Law Review 2008/1.
20. R. C. Post. The Social Foundations of Privacy: Community and Self in the Common Law Tort. – California Law Review 1989/77.
21. W. H. Rehnquist. Is an expanded right of privacy consistent with fair and effective law enforcement? Or: Privacy, You´ve Come a Long Way Baby. – Kansas Law Review 1974/23.
22. J. Reiman. Driving to the Panopticon: A Philosophical Exploration of the Risks to Privacy Posed by the Highway Technology of the Future. – Santa Clara Computer ja High Technology Law Journal. 1995/11. viidatud C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal 2002/72.
23. M. N. Richards. The Dangers of Surveillance. – Harvard Law Review, 2013.
24. C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal 2002/72.
25. B. Sloot. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for o fourth one. – Information & Communications Technology Law 2015/24.
26. D. J. Solove. „I've Got Nothing to Hide" and Other Misunderstandings of Privacy. – San Diego Law Review 2007/44.
27. D. J. Solove. Conceptualisation privacy. – California Law Review 2002/90.
28. D. J. Solove. Data Mining and the Security-Liberty Debate. – The University of Chicago Law Review 2008/75.
29. S. Stalla-Bourdillon, J. Phillips, M. D. Ryan. Privacy vs. Security. Springer London 2014.
30. N. Taylor. Policing, Privacy and Proportionality. – European Human Rights Law Review 2003.
31. T. Tridimas. Proportionality in European Community Law: Searching for the Appropriate Standard of Scrutiny. In The Principle of Proportionality in the Laws of Europe, edited by E. Ellis, 65–84. Oxford: Hart Publishing 1999.
32. D. Warren, L. Brandeis. The right to privacy. – Harvard Law Review, 1890/4.
33. R. Wasserstrom. Privacy: Some Arguments and Assumptions, in Philosophical Dimension of Privacy. Ed. F. D. Schoeman. Cambridge University Press 1984. viidatud

C. Slobogin. Public privacy: camera surveillance of public places and the right to anonymity. – Mississippi Law Review Journal 2002/72.

34. L. Wildhaber, O. Diggelmann. Euroopa inimõiguste konventsioon ja eraelu kaitse. Uuemad arengusuunad. – Juridica 2007/I.
35. N. Witzleb, D. Lindsay, M. Paterson, S. Rodrick. Emerging Challenges in Privacy Law. Comparative perspectives. Cambridge: University Press 2014.

Euroopa Inimõiguste Kohtu kohtulahendid

36. EIKo 07.12.1976, 5493/72, *Handyside v. the United Kingdom.*
37. EIKo 06.09.1978, 5029/71, *Klass and Others vs Germany.*
38. EIKo 26.04.1979, 6538/74, *Sunday Times vs the United Kingdom*.
39. EIKo 13.06.1979, 6833/74, *Marckx vs Belgium.*
40. EIKo 13.12.1979, 8278/78, *X vs Austria*.
41. EIKo 22.10.1981, 7525/76, *Dudgeon vs United Kingdom*.
42. EIKo 25.03.1983, 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75, *Silver and Others vs the United Kingdom.*
43. EIKo 02.08.1984, 8691/79, *Malone vs the United Kingdom.*
44. EIKo 26.03.1985, 8978/80, *X and Y vs Netherlands.*
45. EIKo 24.11.1986, 9063/80, *Gillow vs United Kingdom*.
46. EIKo 18.12.1986, 9697/82, *Johnston vs Ireland.*
47. EIKo 26.03.1987, 9248/81, *Leander vs Sweden*.
48. EIKo 24.04.1990, 11105/84, *Huvig vs France.*
49. EIKo 16.12.1992, 13710/88, *Niemietz vs Germany.*
50. EIKo 09.02.1994, 16798/90, *Lopez Ostra vs Spain*.
51. EIKo 31.01.1995, 15225/89, *Friedl vs Austria.*
52. EIKo 25.02.1997, 22009/93, *Z vs Finland*.
53. EIKo 19.02.1998, 14967/89, *Guerra vs Italy.*
54. EIKo 25.03.1998, 23224/94, *Kopp vs Switzerland.*
55. EIKo 5.07.1999, 31534/96, *Matter vs Slovakia*.
56. EIKo 27.09.1999, 33985/96 33986/96, *Smith and Grady vs United Kingdom*.
57. EIKo 16.02.2000, 27798/95, *Amann vs Swtizerland.*
58. EIKo 04.05.2000, 28341/95, *Rotaru vs Romania.*
59. EIKo 29.04.2002, 2346/02, *Pretty vs United Kingdom.*
60. EIKo 11.07.2002, 28957/95, *Goodwin vs United Kingdom.*
61. EIKo 16.07.2002, 37971/97 *Societe Colas Est and others vs France.*

62. EIKo 22.10.2002, 47114/99, *Taylor-Sabori vs United Kingdom.*
63. EIKo 05.11.2002, 48539/99, *Allan vs United Kingdom.*
64. EIKo 28.01.2003, 44647/98 *Peck vs United Kingdom*.
65. EIKo 13.02.2003, 42326/98, *Odievre vs Prantsusmaa*.
66. EIKo 12.06.2003, 35968/97, *Van Kück vs Germany.*
67. EIKo 08.07.2003, 36022/97 *Hatton and others vs United Kingdom*.
68. EIKo 17.07.2003, 63737/00, *Perry vs United Kingdom.*
69. EIKo 17.07.2003, 25337/94, *Craxi vs Italy.*
70. EIKo 22.07.2003, 24209/94, *Y.F. vs Turkey.*
71. EIKo 04.12.2003, 39272/98, *MC vs Bulgaria*.
72. EIKo 09.03.2004, 61827/00, *Glass vs United Kingdom*.
73. EIKo 27.10.2004, 39647/98 40461/98, *Lewis vs United Kingdom.*
74. EIKo 16.11.2004, 4143/02, *Gomez vs Spain.*
75. EIKo 11.01.2005, 50774/99, *Sciacca vs Italy*.
76. EIKo 16.06.2005, 61603/00, *Storck vs Germany.*
77. EIKo 29.06.2006, 54934/00, *Weber and Saravia vs Germany.*
78. EIKo 26.09.2006, 12350/04, *Wainwright vs United Kingdom*.
79. EIKo 03.04.2007, 62617/00, *Copland vs United Kingdom.*
80. EIKo 10.04.2007, 6339/05, *Evans vs the United Kingdom*.
81. EIKo 04.12.2007, 44362/04, *Dickson vs the United Kingdom.*
82. EIKo 01.07.2008, 58243/00, *Liberty vs United Kingdom.*
83. EIKo 04.12.2008, 30562/04, 30566/04, *S and Marper vs United Kingdom*.
84. EIKo 03.12.2009, 22028/04, *Zaunegger vs Germany*.
85. EIKo 24.06.2010, 30141/04, *Schalk and Kopf vs Austria*.
86. EIKo 18.10.2011, 16188/07, *Kheili vs Switzerland.*
87. EIKo 07.02.2012, 40660/08, *Von Hannover vs Germany.*
88. EIKo 12.01.2016, 37138/14, *Szab and Vissy vs Hungary.*
89. EIKo 21.02.1986, 8793/79, *James and Others vs The United Kingdom.*
90. EIKo 17.10.1986, 9532/81, *Rees vs The United Kingdom.*
91. EIKo 04.12.2015, 47143/06, *Roman Zakharov vs Russia.*
92. EIKo 18.04.2013, 19522/09, *M.K. vs France.*
93. EIKo 18.05.2010, 26839/05, *Kennedy vs United Kingdom.*
94. EIKo 22.11.2012, 39315/06, *Telegraaf Media Nederland Landelijke Media B.V. and Others v. the Netherlands.*
95. EIKo 24.09.2009, 25198/02, *Iordachi and Others v. Moldova.*

96. EIK taotlus nr 58170/13, *Big Brother Watch and Others v. The United Kingdom*.

97. EIKo 03.04.2007, 62617/00, *Copland vs the United Kingdom.*

Euroopa Kohtu kohtulahendid

98. EK C-203/15, *Tele2 Sverige AB versus Post- och telestyrelsen*, eelotsuse taotlus.

99. EK C-698/15, *Davis jt*, eelotsuse taotlus.

100. EKo C-11/70, *Internationale Handelsgesellschaft v. Einfuhr- und Vorratsstelle Getreide*.

101. EKo, 29.04.1999, C-293/97, *The Queen vs. Minister of Agriculture, Fisheries and Food, ex parte Standley jt.*

102. EKo 12.07.2001, C-189/01, *Jippes jt.*

103. EKo 3.09.2008, C-402/05 P ja C-415/05 P, *Kadi ja Al Barakaat International Foundation vs. nõukogu ja komisjon.*

104. EKo 08.07.2010, C-343/09, *Afton Chemical Limited vs Secretary of State for Transport*.

105. EKo 09.11.2010, C-92/09 ja C-93/09, *Volker und Markus Schecke ja Hartmut Eifert vs Land Hessen*.

106. EKo 23.11.2010, C-145/09, *Land Baden-Württemberg vs Panagiotis Tsakouridis.*

107. EKo 16.10.2012, C-614/10 *European Commission vs Austria.*

108. EKo 23.10.2012, C-581/10 ja C-629/10, *Nelson jt* vs *Deutsche Lufthansa AG*

109. EKo 15.11.2012, C-539/10 P ja C-550/10 P, *Al-Aqsa vs. Nõukogu.*

110. EKo 22.01.2013, C-283/11, *Sky Österreich vs Österreichischer Rundfunk.*

111. EKo 07.11.2013, C-473/12, *IPI vs Geoffrey Englebert, Immo 9 SPRL, Gregory Francotte.*

112. EKo 12.12.2013, C-293/12 ja C-594, *Digital Rights Ireland*, kohtujurist P. C. Villalon ettepanek.

113. EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vs Ireland*.

114. EKo 06.10.2016, C-362/14, *Schrems vs Data Protection Commisioner.*

Eesti kohtulahendid

115. RKKKo 3-1-1-80-97

116. RKKKo 3-1-1-51-14

117. RKPSJKo 3-4-1-42-13

118. RKKKKo 3-1-1-51-14, Riigikohtunike Saale Laose ja Eerik Kergandbergi eriarvamus
119. RKPJKo 3-4-1-6-00
120. RKPJKo 3-4-1-6-08

Õigusaktid

121. Euroopa Liidu põhiõiguste harta. – ELT C 326, 26.10.2012. – http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A12012P%2FTXT (09.04.2016)
122. Euroopa Liidu toimimise leping. http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.EST#C_2012326ET.01004701 (29.04.2016).
123. Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv) (ELT 2002 L 201, lk 37; ELT eriväljaanne 13/29, lk 514).
124. Euroopa Parlamendi ja nõukogu direktiiv 2006/24/EÜ, 15. märts 2006, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse direktiivi 2002/58/EÜ. – ELT L 105, 13.04.2006, lk 54–63.
125. Inimõiguste ja põhivabaduste kaitse konventsioon. – RT II 2010, 14, 54.
126. Inimõiguste ülddeklaratsioon. Eestikeelne tõlge. – http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/est.pdf (16.04.2016).
127. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3. – https://www.riigiteataja.ee/akt/78300 (14.04.2016).
128. Isikuandmete kaitse seaduses. - RT I, 06.01.2016, 10.
129. Jälitustegevuse seadus. – RT I, 29.06.2012, 38.
130. Julgeoleku asutuste seadus. - RT I, 17.12.2015, 38.
131. Kaitseväe korralduse seaduses - RT I, 12.03.2015, 19.
132. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt (mitteametlik tõlge). – https://www.riigiteataja.ee/akt/23982 (27.03.2016).
133. Komisjoni ettepanek: Euroopa Parlamendi ja nõukogu direktiiv, mis käsitleb üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate tegevusega kaasnevate või nende töödeldud andmete säilitamist ja millega muudetakse

direktiivi 2002/58/EÜ. – http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=CELEX:52005PC0438&from=ET (16.04.2016).

134. Korrakaitseseaduses - RT I, 23.03.2015, 207.
135. Kriminaalmenetluse seadustik RT I, 06.01.2016, 19.
136. Maksukorralduse seaduses - RT I, 09.02.2016, 3.
137. Õiguskantsleri seadus. - RT I, 30.12.2015, 105.
138. Politsei ja piirivalve seaduses - RT I, 31.12.2015, 28.
139. Relvaseaduses - RT I, 19.03.2015, 19.
140. Riigipiiri seadus. – RT I, 31.12.2015, 27.
141. Strateegilise kauba seaduses - RT I, 12.03.2015, 48.
142. Tolliseaduses - RT I, 10.11.2015, 4.
143. Tunnistajakaitse seaduses - RT I, 29.06.2012, 46.
144. Turvaseaduses - RT I, 30.12.2015, 53.
145. Väärteomenetluse seadustikus - RT I, 19.03.2015, 37.
146. Väärtpaberituru seaduses - RT I, 14.11.2015, 2.
147. Välismaalaste seaduses - RT I, 17.12.2015, 14.
148. Vangistusseaduses - RT I, 23.03.2015, 141.

Analüüsid

149. A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. Riigikohus: Tartu 2015. – http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf (14.04.2016).
150. M. Kruusamäe, T. Reinthal. Jälitustegevuse kohtulik eelkontroll Eestis: kohtupraktika analüüs. Tartu 2013. – http://www.nc.ee/?id=1252 (29.04.2016).
151. Õiguskantsleri seisukoht elektroonilise side seaduse § 1111 põhiseaduspärasuse kohta, 20.07.2015. – http://oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotte_poolt.pdf (15.04.2016).
152. Õiguskantsleri seisukoht: Elektroonilise side seaduse § 1111 alusel sideandmete töötlemise põhiseaduspärasus. 22.04.2016. – http://oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (29.04.2016).

Muud allikad

153. 2013 Annual Report of the Interception of Communications Commissioner. – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302597/InterceptionCommunicationsCommissionerPrint.pdf (27.04.2016).
154. Aruanne jälitusstatistikast 2013. aastal. Justiitsministeerium. – http://www.kriminaalpoliitika.ee/sites/www.kriminaalpoliitika.ee/files/elfinder/dokumendid/jalitusstatistika_aruanne_2013_14022014.pdf (15.04.2016).
155. G. Greenwald, E. MacAskill. NSA Prism program taps in to user data of Apple, Google and others. The Guardian. – http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (09.04.2016).
156. G. Orwell. 1984. Tallinn: Perioodika 1990.
157. J. Vasagar. Germany 'not a surveillance state', says Angela Merkel. The Telegraph. 19.07.2013. – http://www.telegraph.co.uk/news/worldnews/europe/germany/10190946/Germany-not-a-surveillance-state-says-Angela-Merkel.html (09.04.2016).
158. Keskmise kiiruse mõõtmisel põhineva automaatse liiklusjärelevalve kasutamise uuring. 2013. – http://www.mnt.ee/public/ASSC_lopparuanne_v_final.pdf (09.04.2016).
159. KrMS muutmise seaduse muutmise eelnõus. Kriminaalmenetluse seadustiku muutmise ja sellega seonduvalt teiste seaduste muutmise seaduse eelnõu seletuskiri. – http://www.riigikogu.ee/?op=ems&page=eelnou&eid=86dde8ff-c50e-48ba-a39ea325fe15a3f0& (14.04.2016).
160. N. C. Burbules, Privacy, Surveillance, and Classroom Communication on the Internet. –http://faculty.education.illinois.edu/burbules/papers/privacy.html (25.03.2016).
161. P. Luts. Koort: Euroopa peab üle vaatama tabud andmekogumise osas. ERR. 22.03.2016. – http://uudised.err.ee/v/eesti/a145d905-c876-4f4c-bff1-ac99aecd8a65/koort-euroopa-peab-ule-vaatama-tabud-andmekogumise-osas (09.04.2016).
162. P. Sprenger. Sun On Privacy: 'Get Over It'. Wired Magazine. 26.01.1999. – http://archive.wired.com/politics/law/news/1999/01/17538 (27.03.2016).
163. Politsei hakkab ilmselt saama reaalajas kõigi hotellikülastajate andmeid. ERR. – http://uudised.err.ee/v/f1e44719-8eeb-4dc6-9972-6df87419c230/politsei-hakkab-ilmselt-saama-reaalajas-koigi-hotellikulastajate-andmeid (09.04.2016).

164. R. A. Posner. Our Domestic Intelligence Crisis. – Washington Post, 21.12.2005. –http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html (25.03.2016).

165. R. Clarke. What's 'Privacy? 2006. – http://www.rogerclarke.com/DV/Privacy.html (24.03.2016).

166. S. Greer. The Exceptions to Articles 8 to 11 of the European Convention on Human Rights. Council of Europe 1997 – http://www.echr.coe.int/LibraryDocs/DG2/HRFILES/DG2-EN-HRFILES-15(1997).pdf (25.03.2016).

167. Seletuskiri elektroonilise side seaduse ja rahvatervise seaduse muutmise seaduse eelnõu juurde. – http://www.riigikogu.ee/download/2b4f9436-7aa3-4cac-b731-f21c4b3de535 (15.04.2016).

168. T. Bardley. Zuckerberg Comments Underscore Conflict Between Social Networking And Privacy. PCWorld. 11.01.2010. – http://www.pcworld.com/article/186651/zuckerberg_comments_underscore_conflict_between_social_networking_and_privacy.html (27.03.2016).

169. Ülevaade Riigikogu julgeolekuasutuste järelevalve erikomisjoni tegevusest. 13.01.2014–16.02.2015 Kättesaadav: Riigikogu dokumendiregister.

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina Piret Schasmin (sünnikuupäev: 02.02.1987)

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose „Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel“, mille juhendaja on Carri Ginter,

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

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

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

Tallinnas, 02.05.2016