TARTU ÜLIKOOL
ÕIGUSTEADUSKOND
Avaliku õiguse osakond

Kätlin Helena Sehver

PRIVAATSUSÕIGUSE RIIVE PROPORTSIONAALSUSE HINDAMISE KRITEERIUMID EUROOPA LIIDU ÕIGUSES ELEKTROONILISE SIDE ANDMETE KAITSE VALDKONNA NÄITEL

Magistritöö

Juhendaja:
PhD Carri Ginter

Tallinn
2017

SISUKORD

SISSEJUHATUS

Viimastel aastatel on olukord seoses aina hoogustuva rändekriisi ning konfliktidega Lähis-Idas muutunud ärevaks. Uudised terrorismijuhtumitest kuuleb murettekitavalt tihti[1] ning vajadus selliste rünnakute ennetamiseks ja muu raske kuritegevusega võitlemiseks on suur. Julgeolekuasutustel lasub kohustus tagada ühiskonnas turvalisus ning nende huvi on kasutada selle kohustuse täitmiseks kõiki võimalikke ja kättesaadavaid meetmeid. Tehnoloogia areneb pidevalt ning tänapäevased lahendused võimaldavad lihtsasti erinevaid andmeid koguda, töödelda ja säilitada. Elame nn suurandmete (ingl. k *Big Data*) ajastul, kus infot liigub internetiavarustes palju ning erinevatest kanalitest saadud teavet saab automaatselt omavahel siduda ning seeläbi vajalikke seoseid luua. Valdav enamus inimesi kasutab igapäevaselt telekommunikatsioonivahendeid, sh mobiiltelefoni, nutiseadmeid ja internetti ning omab kontot ühes või mitmes sotsiaalmeediavõrgustikus. Kõik eelnimetatud tegevused jätavad endast maha hulga andmeid ning julgeolekuasutustel on nende andmete kasutamise vastu suur huvi.

Mida rohkem andmeid ringleb, seda suurem on tõenäosus, et mingil hetkel riivatakse andmesubjektide õigusi nende andmete kaitsele. Isikuandmed [2] kuuluvad andmesubjekti eraelu puutumatuse, mida loetakse on ÜRO inimõiguste ülddeklaratsiooni[3], Euroopa inimõiguste ja põhivabaduste kaitse konventsiooni

[1] 13.11.2015 toimus mitmeid terrorirünnakuid Pratsusmaal Pariisis, 22.03.2016 toimus pommiplahvatus Belgias Brüsseli lennujaamas, 14.07.2016 rammiti veokiga rahvamassi Prantsusmaal Nizzas, 01.01.2017 tulistati Türgis Istanbulis ööklubikülastajaid, 22.03.2017 rammiti veokiga jalakäijaid Suurbritannias Londonis, 03.04.2017 toimusid pommiplahvatused Venemaal Peterburi metroos, 07.04.2017 rammiti veokiga jalakäijaid Rootsis Stockholmis. Vt ka http://maailm.postimees.ee/3952189/ajatelg-terrorirunnakud-2016-aasta-eli-riikides (22.04.2017), https://en.wikipedia.org/wiki/List_of_terrorist_incidents_in_2017 (22.04.2017)

[2] Isikuandmed on igasugune teave tuvastatud või tuvastatava füüsilise isiku ehk andmesubjekti kohta. Isikut saab otseselt või kaudselt tuvastada eelkõige sellise identifitseerimistunnuse põhjal nagu nimi, isikukood, asukohateave, võrguidentifikaator või selle füüsilise isiku ühe või mitme füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse tunnuse põhjal – Euroopa Parlamendi ja Nõukogu määrus 2016/679 (isikuandmete kaitse üldmäärus) art 4 p 1

[3] Inimõiguste Ülddeklaratsioon. Arvutivõrgus: http://www.un.org/en/universal-declaration-human-rights/ (07.04.2017)

(EIÕK)[4], Euroopa Liidu põhiõiguste harta (edaspidi "põhiõiguste harta")[5] ja reeglina ka riikide konstitutsiooniseaduste alusel inimeste põhiõiguseks, kaitse alla. Euroopa Liit on esimese isikuandmete kaitse alase direktiivi vastu võtnud juba 1995. aastal[6] ning 2016. aasta kevadel sündis pikaajalise andmekaitsereformi[7] tulemusena ka uus isikuandmete kaitse üldmäärus[8]. Euroopa Liit on oma põhjalike regulatsioonidega asunud käesoleval ajal täitma isikuandmete kaitse valdkonnas maailmas liidrirolli.[9]

Kuid mitte alati ei ole Euroopa Liit olnud isikuandmete kaitse alal musternäidiseks. 2006. aastal vastu võetud direktiiv 2006/24/EÜ[10] (edaspidi "andmete säilitamise direktiiv") kohustas liikmesriike koguma ja säilitama kõikide telekommunikatsioonivahendite kasutajate liiklus- ja asukohaandmeid (edaspidi "sideandmed") kuritegevusevastase võitluse ja avaliku korra tagamise eesmärgil. Säilitatavate andmete hulka kuulusid mh sideseansi alustamise ja lõpetamise kellaaeg, sideseansi poolteks olevate kasutajate nimi ja asukoht. Eelnimetatud direktiiv põhjustas palju pahameelt nii tavainimestes kui ka isikuandmete kaitse eest seisvatest ühendustes ja ametkondades, kuna see riivas inimeste põhiõigust eraelu puutumatusele. Samal põhjusel keeldusid mitmed liikmesriigid direktiivi sätteid üle võtmast.[11]

---

[4] Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57

[5] Euroopa Liidu põhiõiguste harta. - ELT C 326, 26.10.2012. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A12012P%2FTXT (07.04.2017)

[6] Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:31995L0046 (07.04.2017)

[7] Euroopa Komisjoni poolt 2012. aastal esitatud seadusandlik pakett Euroopa Liidu isikuandmete kaitse alaste õigusaktide ajakohastamiseks. Vt selgitavat materjali arvutivõrgus: http://www.consilium.europa.eu/et/policies/data-protection-reform/ (07.04.2017)

[8] Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). - ELT L 119, 04.05.2016. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=ET (07.04.2017)

[9] Vt ka G. Butarelli. The EU GDPR as a clarion call for a new global digital gold standard. - International Data Privacy Law, 2016/6, No 2

[10] 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, 13.4.2006. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32006L0024 (07.04.2017)

[11] Vt U. Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. - Juridica 2015/10

2013. aastal vapustas ühiskonda USA riikliku julgeolekuagentuuri (NSA) töötaja Edward Snowden, kes paljastas NSA poolt kasutatavad salajased andmekogumise ja –töötlemise meetodid ja tehnoloogiad. Programmi PRISM abil koguti internetist *Facebook*'i, *Google*'i, *Apple*'i, *Microsoft*'i jm suurte tehnoloogiafirmade abil suures hulgas tavakodanike andmeid.[12] Snowdeni paljastused tekitasid ühiskonnas palju diskussioone selle üle, kas taoline andmete kogumine ja kodanike jälgimine on ikka vajalik ega õõnesta liigselt inimeste privaatsust.

Andmete säilitamise direktiivi hukkamõistjad algatasid mitmetes liikmesriikides kohtuasju oma privaatsusõiguse kaitseks. Iirimaa ja Austria kohtutest laekus Euroopa Kohtusse (EK) kaks eelotsusetaotlust[13], milles paluti EK-l anda seisukoht andmete säilitamise direktiivi õiguspärasuse kohta, s.t hinnata, kas nimetatud direktiiv on kooskõlas EIÕK ja põhiõiguste harta nõuetega. EK liitis nimetatud eelotsusetaotlused üheks kohtuasjaks: *Digital Rights Ireland*[14]. EK seisukoht 2014. aastal tehtud *Digital Rights Ireland* lahendis oli konkreetne: andmete säilitamise direktiivis toodud meetmed kõikide kasutajate sideandmete massiliseks ja eristamatuks säilitamiseks ei ole proportsionaalsed taotletava eesmärgiga ning direktiiv on seega vastuolu tõttu EIÕK ja põhiõiguste hartaga kehtetu. Nimetatud lahendis analüüsis EK direktiivis toodud meetmete proportsionaalsust EIK varasemast praktikast tulenevate miinimumtagatiste kaudu. Nii EIK kui EK rakendavad proportsionaalsuse hindamisel miinimumtagatisi ka oma hilisemas praktikas.

Liikmesriigid reageerisid *Digital Rights Ireland* lahendile erinevalt: oli riike, kes kuulutasid nüüdseks kehtetu andmete säilitamise direktiivi alusel üle võetud siseriiklikud sätted samuti kehtetuks, oli riike, kes muutsid selliseid sätteid ning oli ka riike, kes ei pidanud vajalikuks oma siseriiklikke sideandmete säilitamist puudutavaid regulatsioone muuta.[15] Eesti oli viimati nimetatute seas – andmete säilitamise

[12] Vt G. Greenwald, E. MacAskill. NSA Prism program taps in to user data of Apple, Google and others. - The Guardian, 07.06.2013. Arvutivõrgus kättesaadav: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (10.04.2017)
[13] Esimese eelotsusetaotluse esitas *High Court of Ireland* (Iirimaa) 11. juunil 2012 (kohtuasi C-293/12) ja teise esitas *Verfassungsgerichtshof* (Austria) 19. detsembril 2012 (kohtuasi C-594/12).
[14] EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*
[15] Vt täpsemalt käesoleva töö alapunkt 2.4.2

direktiivist üle võetud elektroonilise side seaduse (ESS)[16] sätted kehtivad muutmata kujul tänaseni.

Selgust olukorrale, kus Euroopa Liidu liikmesriigid ei ole suutnud jõuda ühisele arusaamisele kehtetuks tunnistatud andmete säilitamise direktiivi alusel siseriiklikusse õigusesse üle võetud sideandmete säilitamist puudutavate sätete muutmise vajaduse osas, tõi EK 2016. aasta lahend *Tele2 Sverige*[17]: Rootsi ja Ühendkuningriigi kohtud esitasid EK-le eelotsusetaotlused [18] küsimustega selle kohta, kas siseriiklikud õigusnormid, mis sätestavad ette kõikide kasutajate sideandmete massilise ja eristamatu säilitamise kohustuse (nagu seda nägi ette kehtetuks tunnistatud andmete säilitamise direktiiv), on põhiõiguste hartaga kooskõlas. EK vastus eelnimetatud küsimustele oli eitav. Seejuures lähtus EK oma seisukoha kujundamisel taaskord *Digital Rights Ireland* lahendis käsitletud standarditest. *Tele2 Sverige* lahendiga andis EK lõplikult tauniva hinnangu kodanike nn massilisele jälgimisele riigi poolt. Tähelepanuväärne on, et lisaks EK-le on samaaegselt inimeste privaatsusõigust kaitsma asunud ka EIK: EIK ja EK viitavad oma viimastest lahendites tihedalt üksteise praktikale ning nende kohtute hinnangud riigipoolsetele massilise jälgimise meetmetele on valdavalt samad.

Euroopa Liidu seadusandjate ja ka EK poolne initsiatiiv isikuandmete ja privaatsusõiguse kaitse eestvedajana on ühiskonna hoiakutest lähtuvalt igati õigustatud: Euroopa Komisjoni sidevõrkude, sisu ja tehnoloogia peadirektoraat (ingl. k *Directorate-General for Communications Networks, Content and Technology*) tellis 2016. aastal *Eurobarometer*'i uuringu, mille eesmärgiks oli välja selgitada inimeste hoiakud seoses internetiprivaatsuse ja andmekaitsega.[19] Uuringu tulemused näitasid, et kümnest vastajast üheksa pidasid oluliseks, et nende arvutis, mobiiltelefonis vm

[16] Elektroonilise side seadus. - RT I, 23.03.2017, 5
[17] EKo 21.12.2016, liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson and Others*
[18] Eelotsusetotluse esitasid *Kammarrätten i Stockholm* (Rootsi) 4. mail 2015 (kohtuasi C-203/15) ja *Court of Appeal, England & Wales, Civil Division* (Ühendkuningriik) 28. detsembril 2015 (kohtuasi C-698/15)
[19] E-Privacy. Survey requested by the European Commission, Directorate-General for Communications Networks, Content and Technology (DG CONNECT) and co-ordinated by Directorate-General for Communication. – Flash Eurobarometer 443 - TNS Political & Social, July 2016. Uuringu tulemused ja dokumendid on kättesaadavad arvutivõrgus: http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124 (10.04.2017)

nutiseadmes olevale isiklikule infole (pildid, kontaktid jne) on võimalik ligi pääseda ainult nende endi loal ning et nende sideseansside (e-kirjad, *online*-vestlused) sisu on konfidentsiaalne.[20]

Hoolimata EK ja EIK karmidest seisukohtadest ning inimeste üldistest privaatsust soosivatest hoiakutest ei ole Eesti siiani oma siseriiklikke sideandmete massilist säilitamist lubavaid õigusnorme muutma asunud. Antud teemal ei ole Eestis isegi olnud suuremat avalikku diskussiooni. Kõige põhjalikumalt on ESS regulatsiooni seaduspärasust analüüsinud õiguskantsler Ülle Madise, kes oma 20.07.2015.a ja 22.04.2016.a seisukohtades[21] on leidnud, et sätted ei ole põhiseadusega vastuolus. Eelnimetatud seisukohtade osas on avaldanud kriitikat nii Uno Lõhmus, kes on antud teemal avaldanud kaks artiklit ajakirjas Juridica[22], kui ka Piret Schasmin, kes kaitses 2016. aasta kevadel Tartu Ülikooli õigusteaduskonnas magistritöö teemal "Privaatsusõiguse piiramise õiguslik raamistik Euroopa Inimõiguste Kohtu ning Euroopa Kohtu lahendite alusel" [23] ning avaldas vahetult enne käesoleva töö valmimist koostöös Carri Ginteriga Juridicas artikli "Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis". [24] Kõik eelnimetatud autorid on leidnud, et kehtiv ESS regulatsioon, mis võimaldab sideandmeid massiliselt säilitada ja kasutada, on EK seisukohtade valguses õigusvastane.

Autor leiab, et kuna sideandmete kaitse on seoses EK *Tele2 Sverige* lahendiga hetkel aktuaalne teema ning võrreldes eelmisel aastal kaitstud magistritööga on olukord

---

[20] *Ibid* - Briefing note, lk 2

[21] Õiguskantsleri 20.07.2015.a seisukoht elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta. Arvutivõrgus kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mitte tuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf (09.04.2017); Õiguskantsleri 22.04.2016.a analüüs elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta. Arvutivõrgus kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (09.04.2017)

[22] U. Lõhmus. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. - Juridica X/2016; U. Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. - Juridica 2015/10

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

[24] P. Schasmin ja C. Ginter. Lahendite *Tele2 Sverige* ja *Digital Rights Ireland* mõju sideandmete mugavkasutusele Eestis. – Juridica 1/2017

sama lahendi tõttu muutunud, on asjakohane sideandmete säilitamise ja kasutamise lubatavust käesolevas magistritöös põhjalikumalt käsitleda. Töö eesmärgiks on välja selgitada, millistel tingimustel on Euroopa Liidu õiguse raames võimalik sideandmeid koguda, säilitada ja kasutada kuritegevusevastases võitluses ning kas EK on oma prakikaga loonud proportsionaalsuse testi hulka kuuluvad uued kohustuslikud standardid, s.o minimaalsed nõuded, millele siseriiklik õigus peab vastama selleks, et see oleks Euroopa Liidu õiguse valguses proportsionaalne. Magistritöö hüpoteesiks on, et sideandmete säilitamise ja kasutamise regulatsioonide hindamisel ja rakendamisel tuleb kohustuslikus korras lähtuda EK poolt sätestatud kontrollskeemist. Hüpoteesi kontrollimist toetavad järgnevad probleemküsimused:

1) kas EK on hinnanud sideandmete kogumise, säilitamise ja kasutamise regulatsiooni proportsionaalsust tervikuna või etappide kaupa?

2) millised on EK poolt sätestatud proportsionaalsuse testi kohustusliku kontrollskeemi elemendid?

3) millised on Eesti õiguses esinevad puudused lähtudes eespool nimetatud kontrollskeemist?

4) kas kontrollskeem võiks peale sideandmete säilitamise ja kasutamise proportsionaalsuse hindamise kohalduda ka muudel juhtudel?

Käesolev magistritöö koosneb kolmest peatükist. Esimeses peatükis avatakse privaatsusõiguse olemus ja tähtsus (eelkõige selle roll demokraatlikus ühiskonnas), ning uuritakse, kas isikuandmete kaitset on vajalik eristada üldisest privaatsusõigusest. Teises peatükis analüüsitakse põhjalikult EK lahendit *Digital Rights Ireland*: käsitletakse lahendi olulisemaid seisukohti, tuuakse välja selle kriitika ning tuvastatakse Euroopa Liidu andmete säilitamise direktiivi proportsionaalsuse hindamisel kasutatud standardid. Kolmandas peatükis analüüsitakse EK lahendit *Tele2 Sverige* ning tuuakse välja, millised olulised seisukohad lisandusid sellega juba olemasolevasse prakikasse. Lisaks tuuakse kolmandas peatükis välja EIK ja EK prakikast tuvastatud kontrollskeemi elemendid ning käsitletakse Eesti õiguse olulisemaid puudujääke selle skeemi valguses. Lõpetuseks analüüsitakse põgusalt, kas kontrollskeemi võiks peale sideandmete kogumise ja kasutamise regulatsiooni analüüsimise rakendada ka muudel juhtudel.

Käesolevas magistritöös kasutatakse andmekogumismeetodit ja tõlgendamismeetodit, samuti analüütilist, kronoloogilist ja võrdlevat meetodit. Töö peamisteks allikateks on võõrkeelne teaduskirjandus ning EK ja EIK lahendid. Lisaks on kasutatud ka Eesti ja Euroopa Liidu õigusakte, eestikeelset õiguskirjandust, Riigikohtu praktikat ning erinevaid analüüse ja uuringuid.

1. PRIVAATSUSÕIGUSE OLEMUS JA TÄHTSUS

Eesti Vabariigi olulisimaks õigusaktiks on põhiseadus (PS)[25], mille teises peatükis on toodud isikute põhiõigused, vabadused ja kohustused. Üks neist on PS §-s 26 toodud õigus perekonna- ja eraelu puutumatusele. Tegemist on nn privaatsusõigusega. Eesti varasemad põhiseadused ei sisaldanud privaatsusõiguse klauslit, vastav säte lisandus alles Põhiseaduse Assamblee 13. detsembri 1991. aasta eelnõusse.[26] Privaatsusõiguse kui põhiõiguse alged rahvusvahelisel tasandil ulatuvad aga juba 19. sajandi lõppu: esimest korda leidis privaatsusõigus õiguskirjanduses tunnustamist 1890. aastal USA-s, kui kohtunikud D. Warren ja L. Brandeis kirjeldasid inimeste "õigust olla üksi" (ingl. k "*the right to be left alone*").[27] 20. sajandil inkorporeeriti privaatsusõigus mitmetesse rahvusvahelistesse õigusaktidesse: esmalt 1948. aastal ÜRO inimõiguste ülddeklaratsiooni artiklisse 12, seejärel 1953. aastal EIÕK artiklisse 8 ning 1966. aastal ÜRO peaassamblee kodaniku- ja poliitiliste õiguste rahvusvaheline pakti[28] artiklisse 17. Privaatsusõiguse ulatuslikule rahvusvahelisele tunnustamisele andsid tõuke eelkõige II maailmasõja koledused – holokausti tegid võimalikuks muuhulgas rahvastikuregistri andmekogud, kust sai lihtsasti leida infot juudi soost isikute kohta.[29]

Üks olulisimatest privaatsusõigust puudutavatest rahvusvahelistest õigusaktidest pärineb ka käesolevast sajandist: 2000. aastal välja kuulutatud ning 2009. aastal Lissaboni lepinguga Euroopa Liidu aluslepingute ehk esmase õiguse osaks saanud[30] põhiõiguste harta.

---

[25] Eesti Vabariigi põhiseadus. - RT I, 15.05.2015, 2
[26] K. Jaanimägi. PS § 26/1 - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012
[27] D. Warren, L. Brandeis. The Right to Privacy. - Harvard Law Review, 1890/1891/4, 193
[28] Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. - RT II 1994, 10, 11
[29] O. Diggelmann, M. N. Cleis. How the Right to Privacy Became a Human Right. - Human Rights Law Review 2014 (14) 3, lk 441 jj. Vt ka P. K. Tupay. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. - Juridica IV/2016, lk 228
[30] Põhimõte on toodud Euroopa Liidu toimimise lepingu (ELT C 326, 26.10.2012) artiklis 16. Õigusakti tekst arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.EST#C_2012326ET.01004701 (07.04.2017)

1.1. Privaatsusõiguse kui põhiõiguse olemus

Privaatsusõigusele on keeruline anda ühest definitsiooni. Privaatsusõiguse sisu on eesti keeles vast kõige selgemini suutnud lahti mõtestada Rait Maruste: privaatsusõigust ehk õigust eraelu puutumatusele saab lugeda igaühe õiguseks enesemääratlemisele, elada oma soovide ja tahtmiste kohaselt minimaalse välise sekkumisega, kontrollida enda kohta käiva informatsiooni liikumist iseenda ja avaliku võimu vahel ning olla efektiivselt kaitstud eraellu põhjendamatute sekkumiste eest.[31] Eeltoodud definitsioonist saab kokkuvõtvalt tuletada, et privaatsusõiguse olemus seisneb kontrollis oma eraelu üle ning võimaluses takistada igausugust põhjendamatut välist sekkumist oma eraellu.

Privaatsusõigus kuulub põhiõiguste hulka ning seda saab muuhulgas iseloomustada põhiõiguste üldiste tunnuste kaudu. Tuntud saksa õigusteadlase ja –filosoofi Robert Alexy käsitluse kohaselt iseloomustab põhiõiguseid a) universaalsus, s.t nad on kõigi õigused kõigi vastu, b) moraalne kehtivus, s.t nad on õigustatavad kõigi suhtes, c) fundamentaalsus, s.t nende rikkumine või rahuldamata jätmine toob endaga kaasa surma, rasked kannatused või puudutab autonoomia tuumikolemust, d) prioriteetsus, s.t nad on positiivse õiguse legitiimsuse paratamatuks tingimuseks ja e) abstraktsus, s.t nende kohaldamisala ja -ulatuse kohta pole võimalik luua konkreetset ja täielikku kataloogi.[32] Põhiõiguseid saab R. Alexy hinnangul jagada tõrjeõigusteks, mis kaitsevad elu ja vabadust, luues riigile n-ö negatiivse kohustuse sekkumisest hoiduda, ning kaitseõigusteks, mis kohustavad riiki kaitsma isikut kolmandate isikute rünnete eest luues riigile n-ö positiivse kohustuse tegutsemiseks.[33] Privaatsusõigus sisaldab endas nii negatiivset kui positiivset komponenti: ühelt poolt on riigil kohustus hoiduda sekkumast isiku eraellu (riigi negatiivne kohustus) ning teiselt poolt on riigil kohustus võtta tarvitusele meetmeid selleks, et isiku eraellu ei sekkutaks, kas siis riigi enda või teiste isikute poolt (riigi positiivne kohustus).[34]

---

[31] R. Maruste. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura 2004, lk 429
[32] M. Ernits. PS II peatükk, sissejuhatus/2.1.3 - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012
[33] *Ibid*
[34] K. Jaanimägi (viide 26). PS § 26/5.1. Vt ka M. Taylor. The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect. - International Data Privacy Law, 2015/5, no 4, lk 251

Privaatsusõigust on võimalik sisustada veel ka EIÕK artiklis 8 otsesõnu nimetatud valdkondade kaudu: eraelu, perekonnaelu ja kodu puutumatus ning sõnumisaladus.[35] Nimetatud valdkondi saab omakorda täpsamalt lahti mõtestada kohtupraktika alusel – Euroopa Inimõiguste Kohus (EIK) on EIÕK artikli 8 alusel teinud arvukalt lahendeid, mis aitavad privaatsusõiguse olemust ja ulatust mõista. Asjakohased näited EIK praktikast eraelu, perekonnaelu ja kodu puutumatuse ning sõnumisaladuse avamiseks on välja toonud P. Schasmin oma magistritöö alapunktis 1.3.

Privaatsusõigus on ühtlasi ka sotsiaalne väärtus, mis on tugevalt seotud demokraatia aluspõhimõtetega. [36] Demokraatia seisneb vabaduses teha valikuid, avaldada arvamusi, pakkuda lahendusi ja arutleda. Selleks, et demokraatia toimiks, on vaja osavõtlikke kodanikke, kes eelnimetatud vabadusi iseseisvalt ning ilma väliste mõjutusteta kasutavad. [37] Põhirõhk on just iseseisvusel, mille inimene saavutab psühhosotsiaalse arenguprotsessi käigus – elu jooksul kogetud bioloogilised, kultuurilised ja sotsiaalsed kokkupuuted kujundavad inimesel välja autonoomse isiksuse, mille kaudu omab inimene vaid temale omaseid arvamusi ja hinnanguid. [38] Eelkirjeldatud protsess vajab aga kaitset avalikkuse eest, vastasel juhul ei saa inimese isiksus vabalt areneda ega tema ideed ja arvamused autonoomselt kujuneda.

Inimene, kes teab, et teda pidevalt jälgitakse, käitub teisiti võrreldes inimesega, kes seda ei tea. See tähendab, et inimene ei ole jälgimise all enam iseseisev oma ideedes ja arvamustes. Sama mõtet illustreerib hästi G. Orwelli kuulus teos "1984", kus inimeste hirm parteijuhi ("Suur Vend") poolse jälgimise ees oli sedavõrd suur, et see muutis nii nende käitumist kui ka mõtlemist. Demokraatia, mille edu sõltub just inimeste autonoomsusest, on sellises olukorras ohus. Lihtsaim näide inimese autonoomsusest demokraatia sümbolina on valimiste salajasus – inimesed saavad valida vabalt ilma, et keegi neid valimisprotsessis jälgiks või nende valikut suunaks. Võrdluseks – totalitaarsed režiimid tihti kärbivad oma võimu kinnistamiseks esimese

[35] Vt ka P. Schasmin (viide 23), lk 13
[36] D. J. Solove. Nothing to Hide. The False Tradeoff Between Privacy and Security. Yale University Press, 2011
[37] V. Boehme-Neßler. Privacy: a matter of democracy. Why Democracy Needs Privacy and Data Protection. - International Data Privacy Law, 2016/6, no 3, lk 226-227
[38] *Ibid*, lk 227-228

asjana inimeste privaatsust, et neil ei tekiks autonoomset isiksust ega soovi avaldada oma ideid ja seisukohti. Õiguse roll privaatsuse kaitsjana on seega üldisemalt demokraatia toimimise tagamine.[39] Privaatsusõiguse piiramise negatiivsetest mõjudest saab täpsemalt lugeda P. Schasmini magistritöö alapunktist 1.4.

1.2. Isikuandmete kaitse eristamine nn klassikalisest privaatsusõigusest

Mida aeg edasi, seda enam on EIK privaatsusõiguse sisu ning EIÕK artikli 8 kohaldamisala laiendanud. Tehnoloogia arengu ja andmeside hoogustumise tõttu on EIK praktikas 20. sajandi lõpust alates privaatsusõiguse raames leidnud tunnustamist õigus isikuandmete kaitsele. Näiteks on EIK oma 1997. aasta lahendis Z v Soome[40] täheldanud, et isikuandmete kaitse on "fundamentaalse tähtsusega" osa EIÕK artikliga 8 tagatud õigusest eraelu- ja perekonna puutumatuse kaitsele.[41] Antud kohtuasjas seisnes vaidlus kriminaalmenetluse raames HIV-positiivse isiku haigusloo ja muude meditsiiniliste andmete edastamises arstidelt uurimisorganitele ja kohtule ilma isiku nõusolekuta. Isiku nimi koos tema terviseandmetega avaldati seejuures hilisemas kohtuotsuses. EIK pidas taolist olukorda EIÕK art 8 ehk eraelu puutumatuse rikkumiseks.

Lisaks kohtupraktikale on isikuandmete kaitse esile tõusnud ka Euroopa Liidu õigusloomes. 2009. aastal jõustunud põhiõiguste harta on privaatsusõiguse määratlemisel läinud EIÕK-st sammu kaugemale: põhiõiguste harta artikkel 7 sõnastus on sarnane EIÕK art 8 sõnastusega hõlmates endas era- ja perekonnaelu ja kodu puutumatuse ning sõnumisaladuse kaitset, kuid lisaks sellele on põhiõiguste hartas ka artikkel 8, mis on pühendatud eraldi just isikuandmete kaitsele. Põhiõiguste harta on ainus rahvusvaheline õigusakt, milles isikuandmete kaitse on iseseisva põhiõigusena sätestatud.[42]

Euroopa Liidu õigusruumis on veel lisaks mitmeid sekundaarseid isikuandmete kaitset puudutavaid õigusakte: direktiiv 95/46/EÜ üksikisikute kaitse kohta

[39] *Ibid*, lk 228
[40] EIKo 25.02.1997, 22009/93, Z vs Finland
[41] *Ibid*, p 95
[42] P. K. Tupay (viide 29), lk 231

isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta, määrus 45/2001 üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutusioonides ja asutustes ja selliste andmete vaba liikumise kohta[43] ja direktiiv 2002/58/EÜ isikuandmete töötlemise ja eraelu puutumatuse kaiste kohta eletroonilise side sektoris (edaspidi "e-privaatsuse direktiiv")[44]. 2016. aasta kevadel võeti andmekaitsereformi tulemusena vastu uus isikuandmete kaitse üldmäärus, mida hakatakse direktiivi 95/46/EÜ asemel kohaldama alates 25.05.2018.[45] Kõik eelnimetatud õigusaktid aitavad ellu viia aluslepingutes toodud eesmärke ning täiendada põhiõiguste hartaga sätestatud põhiõiguse sisu, luues isikuandmete töötlemisele konkreetsed reeglid ja tingimused. Lõpptulemusena aitavad need reeglid tagada isikute privaatsuse, sh eraelu puutumatuse ning sõnumisaladuse kaitse.

Nagu eespool käsitletud on isikuandmete kaitse juured nn klassikalises privaatsusõiguses – EIK on oma pikaajalises praktikas lugenud isikuandmete kaitset osaks EIÕK artiklis 8 toodud õigusest eraelu puutumatusele. Põhiõiguste hartas on aga peetud vajalikuks isikuandmete kaitsele eraldi säte (art 8) pühendada ning seega tekib küsimus, kas isikuandmete kaitse väärib Euroopa Liidu õiguse raames eraldiseisva põhiõiguse rolli. Põhiõiguste harta seletuskirjas on viidatud, et artikkel 8 põhineb direktiivil 95/46/EÜ, EIÕK artiklil 8 ja Euroopa Nõukogu konventsioonil nr 108[46] ning et isikuandmete kaitset teostatakse nimetatud direktiiviga määratud korras, mida on võimalik piirata põhiõiguste harta artiklis 52 sätestatud tingimustel. Veel on seletuskirjas nenditud, et artikliga 7 tagatud õigus era- ja perekonnaelu austamisele vastab artiklis 8 tagatud isikuandmete kaitse õigusele.[47] Eeltoodu viitab, et sisuliselt on tegemist ühe ja sama õigusega ning nende eristamine on vaid formaalne ning pole

[43] Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 45/2001, 18. detsember 2000, üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta. - ELT L 8, 12.1.2001. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1491558697563&uri=CELEX:32001R0045 (07.04.2017)

[44] Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). - ELT L 201, 31.7.2002. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32002L0058 (07.04.2017)

[45] Isikuandmete kaitse üldmääruse 2016/679 art 99 lg 2

[46] Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3

[47] Explanations Relating to the Charter of Fundamental Rights of the European Union. – ELT C 303, 14.12.2007. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF (07.04.2017). Vt ka P. K. Tupay (viide 29), lk 232.

praktikas vajalik.[48]Autor ei saa nõustuda sellega, et isikuandmete kaitset ei saa ega ole vaja üldisest privaatsusõigusest eristada. Nimetatud seisukohta põhjendatakse alljärgnevalt.

Lisaks privaatsusõigusele saab n-ö klassikaliseks õiguseks nimetada ka õigust sõnavabadusele. Privaatsusõigus on sätestatud EIÕK artiklis 8 ja põhiõiguste harta artiklis 7 ning sõnavabadus EIÕK artiklis 10 ja põhiõiguste harta artiklis 11. Nii privaatsusõigust kui sõnavabadust puudutavad EIÕK sätted sisaldavad esmalt üldist keeldu õigust riivata ning seejärel üksikuid reegleid, millal riive siiski lubatud on.[49] Mõlema nimetatud klassikalise õigusega käib kaasas teine, nn kaasaegsem õigus[50]: privaatsusõiguse puhul isikuandmete kaitse ja sõnavabaduse puhul õigus tutvuda dokumentidega (põhiõiguste harta art 42). Erinevalt klassikalitest õigustest on kaasaegsed õigused rohkem tehnilise iseloomuga ning sisaldavad endas spetsiifilisi sisutingimusi: meetmeid, nõudeid ja garantiisid õiguse realiseerimiseks. [51] Isikuandmete kaitse põhiolemus on küll toodud põhiõiguste harta artiklis 8 ja ka ELTL artiklis 16, kuid selle täpsem sisu on reguleeritud sekundaarsetes õigusaktides: direktiivis 95/46/EÜ (alates 25.05.2018 isikuandmete kaitse üldmääruses), määruses 45/2001 ja e-privaatsuse direktiivis. Sarnaselt on dokumentidega tutvumine üldiselt sõnastatud põhiõiguste harta artiklis 42 ja ka ELTL artiklis 15, kuid täpsemalt lahti kirjutatud määruses 1049/2001 üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele.[52]

Privaatsusõiguse ja sõnavabaduse puhul sekundaarsest õigusest taolisi regulatsioone täpsemate sisutingimustega ei leia, privaatsuse ja sõnavabaduse sätted seisnevad

[48] Vt ka P. K. Tupay (viide 29), lk 232 ja O. Lynskey. Deconstruction Data Protection: The „Added-Value" of a Right to Data Protection in the EU Legal Order. – International & Comparative Law Quarterly 2014 (63) 3, lk 570 jj.
[49] EIÕK art 8 lg 2 ja art 10 lg 2
[50] Nn klassikalist privaatsusõigust kaasaegsest isikuandmete kaitse õigusest eristas kohtujurist E. Sharpston: EK 09.11.2010, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR vs Land Hessen*, kohtujuristi ettepanek, p 71. Vt ka C. Docksey. Four Fundamental Rights: Finding the Balance. - International Data Privacy Law, 2016/6, no 3, lk 195
[51] C. Docksey (viide 50), lk 195
[52] Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1049/2001, 30. mai 2001, üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele. - ELT L 145, 31.5.2001. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1491560704007&uri=CELEX:32001R1049 (07.04.2017)

pigem vastava õiguse üldise olemasolu konstanteerimises ning seeläbi riigile nn negatiivse kohustuse loomises. Kaasaegsed õigused nagu isikuandmete kaitse ja dokumentidega tutvumine sisaldavad võrreldes klassikaliste õigustega nagu privaatsusõigus ja sõnavabadus endas aga rohkem positiivset komponenti, kuna seavad ette täpsed reeglid nende õiguste kaitsmiseks eeldades sellega riigilt aktiivset tegevust üldise negatiivse tõrjekohustuse asemel. [53] Täiendavates, positiivseid kohustusi loovates sisutingimustes sisaldub isikuandmete kaitse "lisandväärtus"[54] võrreldes klassikalise privaatsusõigusega: näiteks on uues isikuandmete kaitse üldmääruses toodud kaitse automaatse töötlemise eest[55] ja andmelekete eest[56], andmete ülekanne[57] ning õigus "olla unustatud"[58]. Selliseid elemente klassikalise privaatsusõiguse osana käsitleda ei saa.[59]

Isikuandmete kaitsele on omane ka põhiõiguste harta art 8 lõikes 2 toodud õiglase töötlemise põhimõte. Nimetatud põhimõte sisaldub näiteks uue isikuandmete kaitse üldmääruse artiklis 5, kusjuures üldmäärusega luuakse andmesubjektile oma õiguste kaitseks lisaks rida garantiisid[60] ning andmete töötlejatel lasub vastutus ettenähtud reeglite järgimise eest[61]. Selline konkreetne reeglistik aitab isikuandmete kaitse ulatust praktikas paremini mõista ning oma käitumist selliselt suunata, et isikuandmete kaitse oleks tagatud. Klassikalise privaatsusõiguse sisu on oluliselt raskem hoomata ning seega ei pruugi ka selle kaitse praktikas sama hästi tagatud saada.[62]

Eeltoodust saab järeldada, et isikuandmete kaitse on klassikalisest privaatsusõigusest erinevalt reglementeeritud ja formuleeritud, ta sisaldab täiendavaid sisukompomente ning võib hõlmata olukordi, mida klassikaline privaatsusõigus ei hõlma. Sellega väljub isikuandmete kaitse privaatsusõiguse tavapärasest kohaldamisalast. [63]

[53] C. Docksey (viide 50), lk 196-197. Vt ka P. K. Tupay (viide 29), lk 232
[54] Ingl. k "added-value", vt O. Lynskey (viide 48)
[55] Isikuandmete kaitse üldmääruse 2016/679 art 21-22
[56] *Ibid*, art 32-34
[57] *Ibid*, art 20
[58] *Ibid*, art 17
[59] C. Docksey (viide 50), lk 198; O. Lynskey (viide 48), lk 583
[60] Vt isikuandmete kaitse üldmääruse 2016/679 III ptk
[61] *Ibid*, IV peatükk
[62] Vt ka C. Docksey (viide 50), lk 198-199
[63] P. K. Tupay (viide 29), lk 232

Järgnevalt vaadeldakse, kas ja kuidas on kohtuprakitkas isikuandmete kaitset eristatud klassikalisest privaatsusõigusest.

Riigikohus on asunud seisukohale, et füüsiliste isikute kaitse isikuandmete töötlemisel on käsitatav eraldi põhiõigusena.[64] EIK ja EK on oma lahendites isikuandmete kaitse ja privaatsusõiguse küll välja toonud eraldi riive alustena, kui valdavalt on analüüsitud neid õiguseid siiski koostoimes. EIK puhul on see arusaadav, kuna EIÕK, mida EIK oma lahendites kohaldab, ei sätesta isikuandmete kaitset eraldiseisvat, vaid see sisaldub EIÕK art 8 üldises privaatsusõiguse klauslis. Võrreldes EIK-ga on EK-l aga võimalik käsitleda neid õiguseid ka eraldi: kuna EK saab tugineda põhiõiguste hartale, kus on isikuandmete kaitse (art 8) privaatsusõigusest eraldiseisev (art 7), ei pea EK tingimata tuvastama privaatsusõiguse riivet art 7 alusel selleks, et tuvastada isikuandmete kaitse rikkumine art 8 alusel.[65]

See võimalus on oluline, kuna mitte alati ei esine isikuandmete kaitse ja privaatsusõiguse riive koos ning igasugune isikuandmete töötlemine ei kujuta endas privaatsusõiguse riivet *per se*.[66] Selleks, et esineks privaatsusõiguse riive, peab EIK praktika kohaselt töötlemine aset leidma viisil, mis tungib liigselt isiku eraellu – nt töödeldakse delikaatseteid isikuandmeid[67], andmesubjekt on alaealine[68], töötlemine toimub avaliku julgeoleku huvides ja/või õiguskaitseorganite poolt[69], töötlemine on pikajaline[70].[71] Tõsi, kuna isikuandmete kaitse ja klassikaline privaatsusõigus on tihedalt seotud, on tihti praktikas analüüsitud neid mõlemat korraga, nt nagu EK on teinud 2014. a lahendites *Digital Rights Ireland* ja *Google Spain*[72], 2015. a lahendis *Schrems*[73] ning 2016. a lahendis *Tele2 Sverige*.

[64] RKHKo 10.06.2016, 3-3-1-84-15, p 21
[65] C. Docksey (viide 50), lk 201
[66] *Ibid*, lk 199
[67] Vt EIKo 20511/03, *I v Finland*, p 38; EIKo 36919/02, *Armonas v Lithuania*, p 40; EIKo 22009/93, *Z v Finland*, p-d 94 ja 112; EIKo 20837/92, *MS v Sweden*; EIKo 7508/02, *LL v France*
[68] EIKo 2872/02, *K.U. v Finland*; EIKo 0562/04 ja 30566/04, *S and Marper v UK*, p 102
[69] EIKo 26.03.1987, 9248/81, *Leander vs Sweden*, p 48; EIKo 28341/95, *Rotaru vs Romania*, p-d 46, 57–59, EIKo 54934/00, *Weber ja Saravia vs Germany*, p 79; EIKo 0562/04 ja 30566/04, *S and Marper vs UK*, p-d 99, 102-103; EIKo 58243/00, *Liberty vs UK*, p-d 62-63; EIKo 19522/09, *M. K. vs France*, p 35
[70] EIKo *Rotaru vs Romania*; EIKo 62332/00, *Segerstedt-Wiberg and Others v Sweden*; EIKo 24029/07, *MM v UK*
[71] C. Docksey (viide 50), lk 200-201
[72] EKo 13.05.2014, C-131/12, *Google Spain v Agencia Española de Protección de Datos (AEPD)*
[73] EKo 06.10.2016, C-362/14, *Schrems vs Data Protection Commisioner*

Kohtuasjas *Digital Rights Ireland* (lahendist on täpsemalt juttu käesoleva töö teises peatükis) hindas EK andmete säilitamise direktiivi vastavust põhiõiguste hartale ning leidis, et direktiiviga sideteenuste pakkujatele pandud kohustus säilitada isikutega seotud sideandmeid riivab põhiõiguste harta artiklis 7 sätestatud õigust eraelu puutumatusele ning direktiivi alusel isikuandmete töötlemine riivab põhiõiguste harta artiklis 8 sätestatud õigust isikuandmete kaitsele. EK tõi otsuses artiklid 7 ja 8 küll välja eraldi riive alustena, kuid oma arutluskäigus käsitles mõlemat siiski üheaegselt, luues nn hübriidõiguse.[74] Palju kriitikat põhjustanud[75] *Google Spain* otsuses, mis on tuntud "õiguse olla unustatud" tunnustamise tõttu, leidis EK, et interneti otsingumootori haldaja peab otsingumootori tulemuste hulgast kustutama isikuandmeid puudutava teabe, kui andmesubjekti õigus eraelule ja andmekaitsele kaalub üles üldsuse huvi teabe saamise vastu. Ka selles otususes ei tee kohus selget vahet isikuandmete kaitse ja üldise privaatsusõiguse vahel ning käsitleb põhiõiguste harta artiklitest 7 ja 8 tulenevaid õiguseid koos.[76] *Shrems* kohtuasjas nõudis Austria kodanikust portaali *Facebook* kasutaja M. Schrems, et USA, kuhu serveritesse *Facebook* Euroopa Komisjoni 2000. aasta otsuse 2000/520/EÜ (nn *Safe Harbour*'i programm)[77] alusel tema isikuandmeid saadab, ei taga tema andmetele piisavat kaitset.[78] Lahendis tuvastas EK põhiõiguste riive ning kuulutas eespool nimetatud komisjoni otsuse kehtetuks. EK käsitleb *Schrems* lahendis küll põhiõiguste harta art 8 ning direktiivi 95/46/EÜ nõudeid[79], kuid tuvastab riive vaid põhiõiguste harta art 7 puhul ning jätab olukorra art 8 valguses sisuliselt analüüsimata.[80]

Olgugi, et EK eelnevalt välja toodud lahendites oma analüüsis sisuliselt privaatsusõiguse ja isikuandmete kaitset üksteisest ei eristanud, oli nende juhtumite

[74] P. K. Tupay (viide 29), lk 233
[75] Kriitikute peamiseks argumendiks on see, et EK eelistas põhjendamatult privaatsusõigust sõnavabadusele ning andis võimaluse ajaloo ümberkirjutamiseks – vt EK C-131/12, kohtujurist N. Jääskineni ettepanek, 25.06.2013, p 129; lahendi põhjaliku analüüsi kohta vt S. Allen. Remembering and Forgetting - Protecting Privacy Rights in the Digital Age. - European Data Protection Law Reviev, 164/2015
[76] Vt EKo *Google Spain*, p-d 74, 81, 97, 99; P. K. Tupay (viide 29), lk 233
[77] Euroopa Komisjoni otsus 2000/520/EÜ, 26. juuli 2000. - *ELT L 215 , 25/08/2000*
[78] M. Schrems viitab mh Edward Snowdeni paljastustele USA luureteenistuste, eelkõige National Security Agency (NSA) tegevuse osas. Vt otsuse p 27 jj
[79] EKo *Schrems*, p 72
[80] EKo *Schrems*, p 94 jj

puhul nimetatud õiguste koostoimes käsitlemine sisuliselt arusaadav, kuna vaidlusalused andmed olid eraelulist laadi. Veidi vanemates lahendites nagu *Rundfunk*[81] 2003. aastast ja *Schecke*[82] 2010. aastast põhjustas isikuandmete kaitse ja privaatsusõiguse mitteeristamine aga rohkem probleeme: mõlemas kohtuasjas oli tegemist lubamatu isikuandmete töötlemisega, kuid kuna tegemist ei olnud eraelulist laadi andmetega[83], ei esinenud seetõttu ka otseselt isikute privaatsusõiguse rikkumist. EK on nendes asjades üsna vaevaliselt olukorra eraelu puutumatuse kaitsealasse subsumeerinud. Selle asemel, et olukorda EIÕK art 8 kohaldamisalasse sobitada, oleks EK-l esimeses asjas piisanud direktiivi 95/46/EÜ nõuete rikkumise tuvastamisest (põhiõiguste harta ei olnud sellel ajal veel jõustunud) ning teises asjas oleks EK saanud jätta põhiõiguste harta art 7 tähelepanuta ning analüüsida vaid art 8 rikkumist.[84]

Autor leiab, et EK ei ole senises praktikas suutnud teha sisulist vahet põhiõiguste harta art 7 ja art 8 kohaldamisaladel ning et privaatsusõiguse ja isikuandmete käsitlemine ühe nn hübriidõigusena võib praktikas takistada isikuandmete kaitse täieulatusliku potentsiaali ärakasutamist. [85] Kui analüüsida kaasust vaid privaatsusõiguse valguses, võivad tulemusena mitmed isikuandmete kaitsega seotud "lisandväärtused" (nt õiglase töötlemise põhimõte) jääda tähelepanuta, samuti on võimalik, et riive jääb üleüldse fikseerimata, kuna eraellu sekkumine ei leia tuvastamist.

Kokkuvõtvalt saab öelda, et isikuandmete kaitse juured on privaatsusõiguses, kuid täna saab siiski rääkida isikuandmete kaitsest kui eraldiseisvast põhiõigusest. Selline käsitlus on vajalik, et inimeste õiguseid tõhusamalt kaitsta, eriti tänases infoühiskonnas, kus isikuandmete töötlemine leiab interneti ja nutiseadmete kasutamisel aset sisuliselt igal sammul.

[81] EKo 22.01.2013, C-283/11, *Sky Österreich vs Österreichischer Rundfunk*
[82] EKo *Volker und Markus Schecke*
[83] Esimesel juhul oli tegemist kohaliku omavalitsuse, s.o avaliku sektori töötajate palgaandmetega ning teisel juhul riiklikku toetust saanud isikute nimede ja elukohaandmetega.
[84] C. Docksey (viide 50), lk 201-202
[85] Vt *ibid*, lk 202; P. K. Tupay (viide 29), lk 234 ja 236; O. Lynskey (viide 48), lk 573 jj

1.3. Privaatsusõiguse subjektiivsus

Põhiõiguste olemuse mõistmiseks on oluline rääkida õiguste absoluutsusest ja relatiivsusest ehk subjektiivsusest. Õiguse absoluutsus tähendab, et selle tuumikolemust ei tohi mingil juhul riivata, ka juhul kui esinevad kaalukad põhjendused riive õigustamiseks. Subjektiivseid õiguseid tuleb aga omavahel kaaluda ning lähtuda proportsionaalsusest – kui riive on proportsionaalne, on ta ka õigustatud.[86] Toon siinkohal mõned näited selle teooria illustreerimiseks. Laialdaselt on levinud arvamus, et absoluutseks õiguseks on õigus elule, tegelikkuses see nii aga ei ole – teatud juhtudel on elu võtmine siiski õigustatud.[87] Absoluutseteks õigusteks, mida ei või mingil tingimusel ära võtta ega riivata, on aga piinamise, orjuse, ebainimliku või alandava kohtlemise ja karistamise keeld. Rahvusvaheline õigus ei luba nendest keeldudest mingeid erandeid, isegi mitte sõjaolukorras ega terrorismi või organiseeritud kuritegevuse vastasel võitlemisel.[88]

Privaatsusõigus ei ole absoluutne õigus, seda võib teatud juhtudel piirata ning kaaluda vahekorras teiste põhiõigustega.[89] Privaatsusõigust võib nimetada ka kvalifitseeritud õiguseks, kuna EIÕK-s on toodud alused, millal võib seda piirata[90]: EIÕK art 8 lg 2 alusel on privaatsusõiguse riive lubatud, kui on täidetud järgmised tingimused: a) riive on "kooskõlas seadusega", s.t eksisteerib kehtiv õigusnorm, mis annab riiveks aluse; b) riive eesmärk on konventsioonis ette nähtud (riigi julgeoleku, ühiskondliku turvalisuse või riigi majanduslik heaolu huvides, korratuse või kuriteo ärahoidmiseks, tervise või kõlbluse või kaasinimeste õiguste ja vabaduste kaitseks) ning c) riive peab on demokraatlikus ühiskonnas vajalik.

[86] M. Ernits (viide 32). PS § 12/4.2
[87] EIÕK art 2 lg 1 sätestab, et igaühel on õigus elule, kuid sama artikli lg 2 toob välja olukorrad, millal on nimetatud õiguse riive lubatud - inimese kaitsmisel õigusvastase vägivalla eest (art 2 lg 2 p a), seaduslikul vahistamisel või seaduslikult kinni peetud isiku põgenemise vältimiseks (art 2 lg 2 p b) ning seaduslikel toimingutel rahutuste või mässu mahasurumiseks (art 2 lg 2 p c).
[88] EIÕK art 15 lg 2 keelab nimetatud õiguste mittejärgimise sõja ajal või muus hädaolukorras, mis ohustab rahva eluvõimet. Vt ka R. Maruste. PS § 18/1. - Ü. Madise jt (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012
[89] Vt EKo *Volker und Markus Schecke*, p 48; M. Taylor (viide 34), lk 253
[90] B. van der Sloot. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. – Information & Communications Technology Law 2015/24, lk 77

Põhiõiguste hartas nimetatud õiguste ja vabaduste teostamist võib piirata harta artiklis 52 nimetatud alustel ehk piirangu peab kehtestama seadusega, arvestades vastavate 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. PS § 11 sätestab, et õiguste ja vabaduste piirangud peavad olema demokraatlikus ühiskonnas vajalikud ega tohi moonutada piiratavate õiguste ja vabaduste olemust.

Sisuliselt on kõikides eelnimetatud õigusaktides nõutavad eeldused samasisulised ning neid võib kokku võtta ühise nimetaja alla – proportsionaalsuse test. Proportsionaalsus on üks õiguse üldprintsiipe, mille eesmärgiks on olnud kaitsta üksikisikut Euroopa Liidu institutsioonide ja liikmesriikide tegevuse eest.[91] Privaatsusõiguse riive lubatavust ning proportsioanaalsuse testi rakendamist on põhjalikult analüüsinud P. Schasmin oma magistritöö teises peatükis. Lühidalt on kuritegevusevastase võitluse kontekstis vajalik ära mainida, et olgugi et EIÕK art 8 lg 2 nimetab privaatsusõiguse piirangut õigustava eesmärgina mh riiklikku julgeolekut, ühiskondlikku turvalisust ning kuritegude ärahoidmist, tuleb riiklike julgeolekuhuvide kaitsmist ning tänapäeva teaduslike ja tehniliste vahendite kasutamisest tulenevaid kasusid tuleb kaaluda võrreldes sellega, kui tõsine on sekkumine isiku eraellu.[92]

Kokkuvõtvalt võib öelda, et privaatsusõigus ning isikuandmete kaitse kui selle moodsam haru on mõlemad suure tähtsusega põhiõigused, mis on välja toodud mitmetes rahvusvahelistes õigusaktides ning mille sisu ning kaitse ulatust on aidanud defineerida nii EIK kui EK. Nimetatud õiguste riive on küll lubatud, kuid see peab läbima nn proportsionaalsuse testi. Lisaks privaatsusõigusele on põhiõiguste hartaga kaitstud ka isikuandmete kaitse iseseisva põhiõigusena, kuid EIK ja EK ei ole senini isikuandmete kaitset privaatsusõigusest eraldiseisvalt sisuliselt analüüsitud. Privaatsusõigus ja isikuandmete kaitse leiavad kohtupraktikas käsitlemist ühise hübriidõigusena ning reeglina on see kohtuvaidluse esemest, s.o riivatava huvi ja riive iseloomust lähtuvalt olnud ka õigustatud.

[91] J. Milaj. Invalidation of the data retention directive: extending the proportionality test. – Computer Law & Security Review 2015/31, lk 610
[92] EIKo *Leander*, p 59; EIKo *S and Marper*, p 112

Järgnevates peatükkides vaadeldakse lähemalt, kuidas on EK käsitlenud riive lubatavust kuritegevusevastase võitluse eesmärgil sideandmete kogumise, säilitamise ja kasutamise puhul. Analüüsitakse, kas EK lahendite *Digital Rights Ireland* ja *Tele2 Sverige* ning sama valdkonda puudutavate EIK lahendite alusel on võimalik formuleerida konkreetsed standardid ehk nn kontrollskeem, millega privaatsusõiguse ja isikuandmete kaitse riive proportsionaalsuse hindamisel igal juhul arvestama peaks.

2. PROPORTSIONAALSUSE TESTI SISUSTAMINE SIDEANDMETE KAITSE VALDKONNA KOHTUPRAKTIKAS

Riikliku julgeoleku ja privaatsusõiguse omavaheline seos on Euroopa Liidus viimastel aastatel aina enam tähelepanu saanud. Alguse on saanud nn sideandmete säilitamise saaga[93]. Käesolevas peatükis analüüsitakse, kuidas on EIK ja EK praktikas sätestatud privaatsusõiguse riive proportsionaalsuse hindamisel rakendatavad nõuded sideandmete kaitse valdkonnas. Analüüsitakse andmete säilitamise direktiivi sätteid, EK 2014. aasta lahendit *Digital Rights Ireland*, millega eelnimetatud direktiiv kehtetuks tunnistati ning seda, mida direktiivi kehtetuks tunnistamine liikmesriikide tasandil endaga kaasa tõi.

2.1. EIK varasem praktika kodanike massilise jälgimise osas

Enne kui autor asub EK seisukohtade juurde, tutvustatakse põgusalt nendele eelnevat EIK praktikat. Nagu eespool öeldud, on EIK praktikas isikuandmete kaitset käsitletud osana EIÕK artiklis 8 nimetatud privaatsusõigusest. EIÕK art 8 lõikes 2 on toodud, et ametivõimud võivad inimeste privaatsusõigusesse sekkuda, kui see on a) kooskõlas seadusega ja b) kui see on demokraatlikus ühiskonnas vajalik. "Vajadus demokraatlikus ühiskonnas" kujutab endas proportsionaalsuse testi ning seda saab EIÕK art 8 lg 2 kohaselt põhjendada a) riigi julgeoleku, b) ühiskondliku turvalisuse, c) riigi majandusliku heaolu, d) korratuse või kuriteo ärahoidmise, e) tervise või kõlbluse või f) kaasinimeste õiguste ja vabaduste kaitsega. EIÕK art 8 lõikes 2 toodud kriteeriumite sisu ja rakendamine EIK praktikas on toodud välja Piret Schasmini magistritöö alapunktis 2.

[93] Väljendit "sideandmete säilitamise saaga" kasutab Uno Lõhmus oma Juridicas avaldatud artiklites "Elektroonilise side andmete säilitamise lõpetamata saaga" (Juridica 2015/10, lk 735-745) ja "Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte" (Juridica 2016/10, lk 698-708).

Inimeste jälgimist ja andmete kogumist riiklike organite poolt on EIK EIÕK art 8 valguses hinnanud korduvalt, olulisemate lahenditena *Digital Rights Ireland'*ile eelnevast ajast saab välja tuua nt *Klass*[94] 1978. aastast, *Weber ja Saravia*[95] 2006. aastast*, S. ja Marper*[96] 2008. aastast ning *M.K.*[97] 2013. aastast. Kõikides nimetatud lahendites on EIK leidnud, et kuritegevuse ennetamise ja tuvastamisega saab isikute eraellu sekkumist iseenesest õigustada, s.t tegemist on legitiimse eesmärgiga EIÕK art 8 lg 2 mõttes. Küll aga on EIK rõhutanud, et jälgimiseks kasutatavate meetmete proportsionaalsuse hindamisel tuleb EIÕK art 8 lõikes 2 toodud erandeid tõlgendada kitsendavalt[98] ning liikmesriikide kaalutlusruum selliste meetmete kehtestamisel on seda väiksem, mida rohkem mõjutab meede inimeste n-ö intiimsfääri kuuluvate põhiõiguste, nagu seda on EIÕK artiklist 8 tulenev eraelu puutumatus, elluviimist.[99]

Lisaks mainib EIK, et olukorras, kus kriminaalmenetlustes lubatakse piiramatult kasutada kõikvõimalikke kaasaegseid tehnilisi lahendusi, on inimestele EIÕK artikliga 8 tagatud kaitse oluliselt nõrgestatud ning taolistest lahendustest saadavat kasu tuleb hoolikalt kaaluda inimeste eraeluliste huvide ja õigustega[100] ning olukorras, kus isikuandmeid töödeldakse massliselt ja automaatselt, peavad olema seatud tõhusad tagatised põhiõiguste kaitseks, eelkõige juhul kui isikuandmeid kasutavad julgeolekuasutused.[101]

EIK on oma lahendites vajalikud tagatised ka määratlenud. Tegemist on nn miinimumtingimustega, millele isikuandmete masskogumine, säilitamine ja kasutamine riigiasutuste poolt peaks vastama, et esineks kooskõla EIÕK artikliga 8 ning inimeste põhiõigused oleks riigivõimu kuritarvitamise eest kaitstud. Niisugusteks miinimumtagatiseks peab EIK:
a) säilitamistähtaja nõuet, s.t andmete kasutamise ja säilitamise ajaline ulatus peab olema piiratud. Isikuandmete tähtajatu või pikaajaline [102] säilitamine riiklikes

[94] EIKo 06.09.1978, 5029/71, *Klass and Others v Germany*
[95] EIKo *Weber and Saravia*
[96] EIKo *S and Marper*
[97] EIKo 18.04.2013, 19522/09, *M.K. v France*
[98] EIKo *Klass and Others,* p 42
[99] EIKo *S and Marper*, p 100-103
[100] *Ibid*, p 112. Vt ka P. Schasmin (viide 23), lk 34
[101] EIKo *M.K. v France*, p 32
[102] Pikaajaliseks säilitamiseks loeti *M.K. v France* asjas 25 aastat.

andmebaasides ei ole EIK arvates vajalik ega proportsionaalne meede;
b) jälgitavate isikute eristamise nõuet, s.t kõikide inimeste andmeid ei tohiks koguda samadel alustel ja samas ulatuses. Eristada tuleks kindlasti nt alaealisi ning isikuid, kes on konkreetses süüteos kahtlustatavad. Valimatul hulgal andmete kogumine ei ole EIK arvates riive eesmärgi suhtes proportsionaalne;
c) süütegude eristamise nõue, s.t andmete kogumise ja kasutamise tingimused peaksid sõltuma sellest, millise olemuse ja raskusastmega süüteoga on tegemist;
d) konkreetsete protseduurireeglite sätestamine andmete kogumisele, kasutamisele, säilitamisele aga ka kustutamisele/hävitamisele, s.t peab olema selge, kes ja millisel juhul tohib andmetele ligi pääseda, kus ja kuidas andmeid hoitakse ning millal ja kuidas andmed hävitatakse;
e) tõhusa järelvalve tagamine andmete kogumise, säilitamise ja kasutamise osas.[103]

Nimetatud tingimustele on EK oma sideandmete kaitse alases praktikas tugevalt toetunud. Järgnevalt käsitletakse andmete säilitamise direktiivi ning selle kehtivusele hävitava hinnangu andnud EK lahendit *Digital Rights Ireland*.

2.2. Direktiiv 2006/24/EÜ

Võib öelda, et "sideandmete säilitamise saaga" ajendiks oli Euroopa Komisjoni poolt 2006. aastal vastu võetud andmete säilitamise direktiiv. Direktiivi juured ulatuvad 1996. aastasse, mil Euroopa Komisjon avaldas resolutsiooni, millega võimaldati julgeolekuasutustel sideseanssidesse sekkuda[104]. Nii siseriiklikud kui rahvusvahelised julgeolekuasutused tundsid aga, et nende kuritegevusevastase võitluse võimekuse realiseerimist takistavad puudulikud mehhanismid sideandmete säilitamise

[103] EIK nimetab miinimumtagatised *Weber and Saravia* lahendi p-s 95 ning viitab sealjuures mitmetele varasematele lahenditele. Vt samal teemal P. Schasmin (viide 23), lk 28-29; S. Schweda. UK Surveillance Under Judicial Scrutiny: GCHQ Intelligence Sharing with NSA Contravened Human Rights, But Is Now Legal. – European Data Protection Law Review, 1/2015, lk 64; F. Boehm ja M. D. Cole. Data Retention after the Judgement of the Court of Justice of the European Union. - Study for the Greens/EFA Group in the European Parliament, 30.06.2014, lk 26-27. Arvutivõrgus: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf (09.04.2017)

[104] Euroopa Nõukogu 17. jaanuari 1995 resolutsioon telekommunikatsiooniseanssidesse seadusliku sekkumise kohta. - ELT C 329, 4.11.1996. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104 (09.04.2017)

valdkonnas.[105] Direktiiv 97/66/EÜ[106], mis reguleeris isikuandmete töötlemist ja privaatsust telekommunikatsioonisektoris, lubas sideandmeid säilitada arvelduste huvides vaid piiratud aja ulatuses (kuni 3 kuud), misjärel kõik andmed hävitati.[107] 2000. aastal koostas Euroopa Liit eelnõu, mis oleks tühistanud kohustuse sideandmed peale arvelduste teostamist hävitada.[108] See eelnõu küll käiku ei läinud, kuid tööd sideandmete pikaajalise säilitamise seadustamiseks jätkati. 2006. aastal võeti vaatamata erinevate andmekaitseorganisatsioonide ja sideettevõtjate ulatuslikule vastuseisule lõpuks vastu andmete säilitamise direktiiv.[109]

Andmete säilitamise direktiiviga kohustati Euroopa Liidu liikmesriike tagama, et üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujad säilitaksid kõikide oma kasutajate kommunikatsiooni liiklus- ja asukohaandmeid, mis on vajalikud:

a) sideallika seiramiseks ja tuvastamiseks;
b) side sihtpunkti tuvastamiseks;
c) side kuupäeva, aja ja kestuse kindlaksmääramiseks;
d) sideliigi kindlaksmääramiseks;
e) kasutaja sidevahendi või oletatava sidevahendi kindlaksmääramiseks ja
f) mobiilsidevahendi asukoha kindlaksmääramiseks.[110]

Andmeid tuli säilitada minimaalselt kuus kuud ja maksimaalselt kaks aastat alates sideseansi toimumise päevast.[111] Andmete säilitamise eesmärgiks oli "liikmesriigi õiguses määratletud" raskete kuritegude uurimise, avastamise ja kohtus menetlemise võimaldamine.[112] See, millised ametiasutused saavad juurdepääsu säilitatud

[105] C. Jones. Background to the EU Data Retention Directive. - EU Law Analysis, 07.04.2014. Arvutivõrgus: http://eulawanalysis.blogspot.com/2014/04/background-to-eu-data-retention.html (09.04.2017)
[106] Euroopa Parlamendi ja Nõukogu direktiiv 97/66/EÜ, 15.12.1997, telekommunikatsioonisektoris isikuandmete töötlemise ja privaatsuse kaitse kohta. - ELT L 24, 30.1.1998. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML (09.04.17)
[107] *Ibid*, art 17
[108] C. Jones (viide 105)
[109] L. Drewry. Crimes without Culprits: Why the European Union Needs Data Retention, and How it Can Be Balanced With the Right to Privacy. - Wisconsin International Law Journal, 2016/33, no 4, lk 732-733
[110] direktiivi art 5
[111] direktiivi art 6
[112] direktiivi art 1 lg 1

andmetele, millist menetlust tuleb järgida ning millised tingimused peavad selleks olema täidetud, jäeti samuti liikmesriikide otsustada.[113]

Andmete säilitamise direktiiv põhjustas mitmetes liikmesriikides vaidlusi ning selle sätteid peeti ülemäära põhiõigusi riivavateks.[114] Osad liikmesriigid keeldusid direktiivi vastu võtmast ning Euroopa Komisjon oli liikmesriikide kohustuste rikkumise tõttu sunnitud algatama ELTL art 258 nimetatud rikkumismenetluse.[115] Rootsi ei võtnud direktiivi sätteid üle ka peale Euroopa Komisjoni etteheitvat otsust, mispeale Euroopa Komisjon esitas Rootsi vastu veel ühe hagi ning EK määras 2013. aastal Rootsile 3 miljoni euro suuruse trahvi.[116]

Direktiivi art 1 lõige 1 ning art 4 võimaldasid igal liikmesriigil ise otsustada, mida loetakse "raskeks kuriteoks" ning millistel ametiasutustel on võimalik säilitatud andmeid kasutada. Mitmed riigid laiendasid direktiivist tulenevaid sätteid ka vähemoluliste süütegude menetlemise osas ning andsid andmetele juurdepääsu mh preventiivsetel eesmärkidel tegutsevatele ametiasutustele (luureteenistused).[117] See tõi aga kodanike ning andmekaitsevaldkonna ekspertide seas kaasa suure pahameele ning viidati privaatus- ja andmekaitseõiguse rikkumistele. Andmete säilitamise direktiivi üle võtvad riigisisesed õigusaktid tunnistati põhiseadusvastaseks nt Bulgaarias, Rumeenias, Küprosel, Tšehhis ja Saksamaal.[118]

2.3. Euroopa Kohtu lahend *Digital Rights Ireland*

EK-sse jõudis direktiivi sätete õiguspärasuse teemal 2 eelotsusetaotlust, üks Iirimaalt ja teine Austriast. EK liitis nimetatud eelotsusetaotlused üheks kohtuasjaks: *Digital Rights Ireland*. Lahend avaldati 08.04.2014. a ning see oli märgilise tähtsusega.

[113] direktiivi art 4. Vt ka U. Lõhmus. Elektroonilise side andmete säilitamise lõpetamata saaga. - Juridica 2015/10, lk 736-737; M. - P. Granger ja K. Irion. The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection. - European Law Review 39/2014, no 4, lk 838
[114] Vt U. Lõhmus (viide 113), lk 737; M. - P. Granger (viide 113), lk 839
[115] Etteheiteid tehti Rumeeniale ja Saksamaale. Vt Euroopa Komisjoni 27.10.2011 pressiteadet: Commission requests Germany and Romania fully transpose EU rules. Arvutivõrgus kättesaadav: http://europa.eu/rapid/press-release_IP-11-1248_en.htm (09.04.2017)
[116] EKo 04.12.2014, C-243/13, *European Commission v Sweden*. Vt ka U. Lõhmus (viide 113), lk 737
[117] U. Lõhmus (viide 113), lk 737
[118] *Ibid*

Esiteks oli *Digital Rights Ireland* lahend märgiline seetõttu, et EK tunnistas sellega andmete säilitamise direktiivi, s.o Euroopa Komisjoni poolt välja antud raamõigusakti kehtetuks vastuolude tõttu põhiõiguste hartaga. Enne nimetatud lahendit ei ole EK reeglina Euroopa Liidu direktiive kehtetuks tunnistanud, isegi kui need on olnud inimeste põhiõiguseid riivavad.[119] Pigem jättis EK taolised direktiivid kehtima, kuid andis liikmesriikidele juhiseid, kuidas nende sätteid üle võtta selliselt, et ei esineks põhiõiguste rikkumisi.[120] Teiseks teeb lahendi märgiliseks asjaolu, et EK pani (EIK varasemale praktikale tuginedes) nn miinimumtagatise sätestamisega liikmesriikides asetleidvale kodanike jälgimisele ja andmete kogumisele piirid ette. Autor käsitleb lahendi olulisemaid pidepunkte järgnevalt ning toob välja, millised on EK poolt sätestatud miinimumtagatised ning kas neid saab lugeda standardiks, mida privaatsusõigust riivavate meetmete proportsionaalsuse hindamisel kindlasti rakendada tuleks.

2.3.1. Põhiõiguste harta artiklite 8 ja 11 eristamata ja analüüsimata jätmine

Esmalt toob autor *Digital Rights Ireland* lahendi puhul välja asjaolu, et kuigi kohtujurist P. Cruz Villalon eristab oma ettepanekus üksteisest põhiõiguste harta artiklitega 7 ja 8 tagatud õiguseid[121], EK seda ei tee. EK toob välja vaid, et "lisaks põhiõiguste harta artiklile 7 esineb antud olukorras ka artikli 8 riive, kuna andmete säilitamise direktiiv näeb ette isikuandmete töötlemise"[122] ning "põhiõiguste harta artiklis 8 nimetatud isikuandmete kaitse on tähtis osa artiklis 7 ette nähtud privaatsusõigusest".[123] EK loob isikuandmete kaitsest ja privaatsusõigusest sisuliselt ühe nn hübriidõiguse ning analüüsib olukorda mõlema õiguse riivena paralleelselt.[124] Kohtujurist P. Cruz Villalon on aga oma arutluskäigus põhirõhu asetanud põhiõiguste

[119] EK on kokku nelja kohtuasja raames Euroopa Liidu institutsioonide poolt välja antud õigustloovaid akte vastuolu tõttu põhiõigustega privaatsusele ja isikuandmete kaitsele kehtetuks tunnistanud. Vt EKo 30.05.2006, liidetud kohtuasjad C-317/04 ja C-318/ 04, *European Parliament v Council of the European Union and European Parliament v European Commission*; EKo 09.11.2010, liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke GbR, Hartmut Eifert v Land Hessen*; EKo 08.04.2014, liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*; EKo 06.10.2015, C-362/14, *Maximillian Schrems v Data Protection Commissioner*

[120] M. - P. Granger (viide 113), lk 845

[121] EK *Digital Rights Ireland,* kohtujuristi ettepanek*,* p 60 jj

[122] EKo *Digital Rights Ireland*, p 36

[123] *Ibid*, p 53

[124] Põhiõiguste harta art 7 ja art 8 käsitlemisest ühe hübriidõigusena vt täpsemalt käesoleva töö p 1.2

harta artiklile 7 leides, et see tagab antud olukorras isikute õigustele parema kaitse ning probleem ei esine niiväga selles, kuidas kogutud andmeid hiljem töödeldakse, vaid hoopis andmete kogumises kui sellises.[125]

Autor nõustub kohtujuristi seisukohaga selles osas, et antud küsimuses on põhirõhk inimeste privaatsusõiguse kaitsel, kuid samas ei pea põhjendatuks arvamust, mille kohaselt põhiõiguste harta art 7 tagab inimeste õigustele parema kaitse kui art 8. Eespool on analüüsitud põhiõiguste harta art 7 ja 8 erisusi ning jõutud järeldusele, et art 8 pakub tegelikkuses ulatuslikumat kaitset kui art 7. Kui EK ei oleks sideandmete kogumist ja säilitamist iseenesest piisavalt kaalukaks riiveks pidanud, oleks meetmete proportsionaalsuse hindamisel raskuskese langenud hoopis sideandmete hilisemale kasutamisele ja töötlemisele – sel juhul oleks olnud kindlasti vajalik analüüsida kasutamise ja töötlemise meetmeid põhiõiguste harta art 8 riive valguses.

Põhiõiguste harta artikliga 11 kaitsavat õigust ehk sõnavabadust mainib EK *Digital Rights Ireland* lahendis samuti väga põgusalt, olgugi et eelotsuse küsimustes konkreetselt selle õiguse riivele viidati. EK toob välja, et sideandmed võimaldavad teha väga täpseid järeldusi isikute eraelu kohta ning hoolimata asjaolust, et side sisule juurdepääs puudub, võib selliste andmete säilitamine mõjutada sidevahendite kasutamist ning põhiõiguste harta artikliga 11 tagatud sõnavabaduse teostamist,[126] kuid rohkem EK olukorda artikli 11 seisukohast vaadatuna ei käsitle.[127] Kohtujurist P. Cruz Villalon märgib oma ettepanekus seevastu aga ära, et pidev sideandmete kogumine ja kasutamine ilma isikuid teavitamat võib tekitada isikutes tunde, et nende eraelu pidevalt jälgitakse, mis omakorda võib tugevalt mõjutada seda, kuidas isikud kasutavad oma õigust sõnavabadusele.[128] Olgugi, et EK art 11 puutumust sideandmete kogumise süsteemi suhtes ei analüüsi, annab kohtujuristi mõttekäik aluse eeldada, et tegelikkuses esinevad taolistel juhtudel ka mõjud sõnavabadusele. Jääb üle oodata, kas tulevases kohtupraktikas leiab aset ka selle põhiõiguse täpsem analüüsimine andmete kogumise teema valguses.

[125] F. Boehm (viide 103), lk 30
[126] EKo *Digital Rights Ireland*, p 27-28
[127] Kuna EK tunnistab direktiivi kehtetuks põhiõiguste harta artiklite 7 ja 8 rikkumiste tõttu, ei pea ta vajalikuks analüüsida juhtumist harta artikli 11 valguses. Vt ka *ibid*, p 70
[128] EK *Digital Rights Ireland,* kohtujuristi ettepanek, p-d 52 ja 72. Vt ka F. Boehm (viide 103), lk 28-29

2.3.2. Sideandmed kuuluvad inimese privaatsfääri, kuid riive ei kahjusta õiguste põhiolemust

EK juhtis tähelepanu sideandmete tähendusele inimeste eraellu sekkumisel: andmete säilitamise direktiivi artiklite 3 ja 5 alusel säilitatavad andmed võimaldavad muu hulgas teha kindlaks, kellega ja millise sidevahendi kaudu ning kui sageli kasutaja suhtles ning side toimumise aja ja koha, samuti võimaldavad need teha väga täpseid järeldusi jälgitavate 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.[129] EK tõi selgesõnaliselt välja, et ei ole oluline, kas edastatud isikuandmed on delikaatsed või mitte või kas asjaomased isikud on selle riive tõttu pidanud taluma mingeid ebamugavusi.[130] Tegemist on väga olulise seisukohaga kuna sellega laiendas EK eraelu ja privaatsuse sfääri ka sideandmetele.

EK leiab *Digital Rights Ireland* lahendis, et nii sideandmete kogumine kui ka siseriiklike ametiasutuste juurdepääs nendele andmetele kujutavad endas privaatsusõiguse riivet.[131] Lahendis on toodud: "Kuna nii andmete säilitamine kui ka hilisem kasutamine toimub kasutajat teavitamata, võib see tekitada isikutes tunde, et nende eraelu pidevalt jälgitakse."[132] Samal arvamusel oli ka kohtujurist P. Cruz Villalon, kes märkis ära, et andmete säilitamise direktiivi rakendamisega tekitatakse inimestes tunne, et nad on kogu aeg pideva jälgimise all ning olgugi et kogutud andmete pinnalt saab jälgimine toimuda tagantjärele, ohustab see siiski kodanike õigust oma eraelu saladusele kogu andmete säilitamise aja vältel.[133]

---

[129] EKo *Digital Rights Irelend*, p 26-27.
[130] *Ibid*, p 34
[131] *Ibid*, p 33
[132] *Ibid*, p 37.
[133] EK *Digital Rights Ireland*, kohtujuristi ettepanek, p-d 52 ja 72. Vt ka E. Guild ja S. Carrera. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. - CEPS Papers in Liberty and Security in Europe, no 65/May 2014, lk 6. Arvutivõrgus kättesaadav: https://www.ceps.eu/system/files/EG%20and%20SC%20Data%20retention.pdf (09.04.2017)

EK ei pea eelnimetatud riivet siiski põhiõiguste harta artiklites 7 ja 8 toodud põhiõiguste olemust kahjustavaks, kuna andmete säilitamise direktiivi art 1 lõikest 2 nähtuvalt ei ole elektroonilise side sisuga tutvumine lubatud ning andmete kogumisel ja säilitamisel peab järgima direktiividega 95/46/EÜ ja 2002/58/EÜ sätestatud andmekaitsepõhimõtteid.[134] Sideandmete kogumise riivava iseloomu alahindamist võrreldes kommunikatsiooni sisuga võib aga kritiseerida – praktikas võib kasvõi ühe sideseansi meta-andmete põhjal teha isiku eraelu kohta põhjapanevaid järeldusi ja seda ilma sideseansi sisuga tutvumata – nt koduvägivalla tugiliinile helistamine. Kuna sideandmete kogumine toimub pikema ajaperioodi jooksul (minimaalselt 6 kuud), saab neid koos analüüsides anda hinnangu isiku harjumustele ja käitmismustrile – kellega ja kui tihti isik suhtleb, kuidas ta liigub jne. Nagu EK ise ütleb: "sõnumi sisule ligipääsu puudumine ei mõjuta asjaolu, et sideandmete kogumine ja kasutamine iseenesest on põhiõiguste harta art 7 sätestatud isiku privaatsusõiguse riivamine."[135] Sideandmete säilitamise, kasutamise ja kuritarvitamisega võib privaatsusõiguse põhiolemust kahjustada samaväärselt, kui seda saab teha sõnumisaladusse sekkumisega.[136]

2.3.3. Proportsionaalsuse testi esimene etapp: julgeoleku kaitse eesmärk kooskõlas liidu üldiste huvidega

Leides, et sideandmete kogumine ja kasutamine ei kujuta endas sellist riivet, mis kahjustaks põhiõiguste harta art 7 ja 8 põhiolemust, annab EK mõista, et andmete säilitamise direktiivi kehtivuse hindamiseks tuleb riive osas rakendada nn proportsionaalsuse testi ehk tuvastada, kas riive on õigustatud ja vajalik.[137]

Proportsionaalsuse testi esimeses etapis arutleb EK, et andmete säilitamise direktiivi art 1 lõikest 1 nähtuvalt on selle peamiseks eesmärgiks tagada kogutud andmete abil raskete kuritegude uurimine, avastamine ja kohtus menetlemine, s.t tagada avalik

[134] EKo *Digital Rights Irelend*, p 39-40
[135] *Ibid*, p 34. Vt ka E. Guild (viide 133), lk 5-6
[136] M. - P. Granger (viide 113), lk 847
[137] E. Guild (viide 133), lk 6

julgeolek, ning selline eesmärk on kooskõlas liidu üldiste huvidega.[138] Võrdluseks: *Digital Rights Ireland* ei ole tegelikult esimene kohtuasi, kus EK on pidanud lahendama andmete säilitamise direktiivi õiguspärasuse küsimust – 2006. aasta juulis taotles Iirimaa (keda toetas ka Slovakkia) andmete säilitamise direktiivi tühistamist väitega, et seda ei ole vastu võetud sobival õiguslikul alusel.[139] Tookord leidis EK, et direktiiv on õigustatud siseturu toimimise argumendiga ning julgeoleku tagamine ei olnudki selle peamiseks eesmärgiks.[140] Küsimust, kas direktiiv rikub inimeste eraelu puutumatust, EK selles lahendis ei puudutanud.

2014. aasta *Digital Right Ireland* lahendis peab EK aga just julgeoleku faktorit direktiivi peamiseks eesmärgiks ja õigustuseks. Selline seisukoha muutmine on huvitav, eelkõige kuna Euroopa Komisjon ei suutnud oma 2011. aasta raportis[141] välja tuua tõsiseltvõetavaid tõendeid selle kohta, et sideandmete säilitamine oleks kuritegevusega võitlemisse midagi oluliselt juurde andnud. Ka Euroopa andmekaitseinspektor on oma 2011. aasta raportis kirjutanud, et ei ole veendunud sellisel kujul andmete säilitamise vajaduses ning kasuteguris kuritegevusega võitlemisel. [142] Võimalik, et surve andmete säilitamise direktiivi hindamisele põhiõiguste harta kontekstis oli sedavõrd suur, et EK pidi oma varasemat seisukohta muutma selleks, et teostada analüüsi isikute privaatsusõiguse rolli osas kuritegevuse vastu võitlemises ning luua antud teemal pretsedent.[143]

---

[138] EKo *Digital Rights Ireland*, p 41-44. Vt ka EKo 3.09.2008, liidetud kohtuasjad C-402/05 P ja C-415/05 P, *Kadi and Al Barakaat International Foundation v Council and Commission*

[139] EKo 10.02.2009, C-301/06, *Iirimaa v Euroopa Parlament ja Euroopa Liidu Nõukogu*

[140] S.t direktiivi eesmärgiks oli ühtlustada liikmesriikide sätteid, mis käsitlevad üldkasutatavate elektrooniliste sideteenuste või üldkasutatavate sidevõrkude pakkujate kohustust säilitada teatavaid nende loodud või töödeldud andmeid - EKo C-301/06, p 58 jj. Vt ka U. Lõhmus (viide 113), lk 738

[141] Euroopa Komisjoni 18.04.2011 raport andmete säilitamise direktiivi kohta. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF (09.04.2017)

[142] Euroopa andmekaitseinspektori arvamus Komisjoni 18.04.2011 raporti kohta. - ELT C 279, 23.9.2011. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011XX0923(01) (09.04.2017). Vt ka E. Guild (viide 133), lk 7

[143] Mitmed liikmesriigid olid direktiivist üle võetud siseriiklikud normid tühistanud, EK-le ja EIK-le laekus privaatsusõiguse rikkumise teemalisi kaebusi ning kriitikat esitasid ka erinevad andmekaitsega tegelevad institutsioonid, eeskätt Euroopa Andmekaitseinspektor. Lisaks oli hiljutine Snowdeni skandaal tõstnud privaatsuse küsimuse avalikkuse huviorbiiti ning kodanike jälgimine riigiasutuste poolt leidis ühiskonnas üldiselt hukkamõistmist. Vt ka M. - P. Granger (viide 113), lk 845; F. Boehm (viide 103), lk 9

2.3.4. Proportsionaalsuse testi teine etapp: riivava meetme valikuks on piiratud kaalutlusruum

Proportsionaalsuse testi teise etapi, milleks on kasutatava meetme sobivuse ja vajalikkuse hindamine, raames viitab EK esmalt EIK praktikale märkides, et juhul kui tegemist on põhiõiguse riivega, on liidu seadusandja kaalutlusõigus piiratud sõltuvalt reast teguritest – nt asjassepuutuv valdkond, põhiõiguste hartaga tagatud õiguse olemus, riive laad ja raskus ning riive eesmärk. Võttes arvesse, et andmete säilitamise direktiiv riivab ulatuslikult õigust isikuandmete kaitsele ja eraelu puutumatusele, on seadusandjal vähem kaalutlusõigust ning kontroll kõikide nõuete täitmise üle peab olema range.[144] Selle seisukoha valguses jääb aga lahtiseks küsimus põhiõiguste olemusest: kas piiratud kaalutlusõigus kohaldub kõikide põhiõiguste riive korral või ainult teatud, n-ö olulisemate puhul; ning ka riive laadist ja raskusest: kui tõsine peab riive olema ning kuidas seda hinnata. Samuti jääb lahtiseks, kuidas täpsemalt mõjutab kaalutlusõiguse piiramist kaalukausi teine pool ehk piirangu eesmärk – kas mõni üldise huvi alla kuuluv valdkond (nt rahvatervise kaitse, riiklik julgeolek, majanduslik heaolu vm) nõuab teistest rangemat piirangut.[145] Nendele küsimustele saab vastused tõenäoliselt alles tulevikus, kui EK on oma praktikas selliseid teemasid käsitlenud.

Andmete säilitamist peab EK iseenesest kuritegevuse vastu võitlemise ja julgeoleku tagamise seisukohast sobivaks meetmeks, kuna elektroonilise side vahendite suurenevat tähtsust arvestades pakuvad kogutavad sideandmed siseriiklikele õiguskaitseasutustele täiendavaid võimalusi raskete kuritegude lahendamiseks.[146] Meetme vajalikkuse osas märgib EK, et ükskõik kui oluline antud juhul üldist huvi pakkuv eesmärk (raske kuritegevuse, eeskätt organiseeritud kuritegevuse ja terrorismi vastane võitlus) ka ei ole, ei saa see siiski üksinda õigustada niisuguse sideandmete säilitamise meetme vajalikkust. Eraelu puutumatuse kaitse erandite ja piirangute puhul tuleb piirduda vaid rangelt vajalikuga.[147]

Digital Rights Ireland lahendiga paneb EK liidu seadusandjatele otsese kohustuse ja

[144] EKo *Digital Rights Ireland, p* 47-48
[145] M. - P. Granger (viide 113), lk 846
[146] EKo *Digital Rights Ireland*, p 49
[147] *Ibid*, p 51-52

ka vastutuse inimeste põhiõiguste kaitse tagamise osas. Tuues välja nn miinimumnõuded, millele õigusakt peaks vastama selleks, et see oleks põhiõiguste riive seisukohast vaadatuna põhjendatud ja vajalik (vt järgmist alapunkti), annab EK lisaks range kontrolli nõude kehtestamisele seadusandjatele ka selged suunised selle kohta, kuidas sarnaseid õigusakte tulevikus koostada ning kuidas üleliiduline andmete säilitamise süsteem, mis ei sekku liigselt inimeste privaatsusõigusesse, võiks olla üles ehitatud.[148] Suuniseid saavad EK seisukohtadest kahtlemata ka siseriiklikud kohtud, kes teostavad kontrolli siseriiklikes õigusaktides piisavate tagatiste olemasolu üle, et need vastaks põhiõiguste harta reeglitele.

Piiratud diskretsiooni ja range kontrolli sätestamine tähendavad praktikas veel ka seda, et Euroopa Liidu institutsioonid peavad tulevikus õigusaktide väljatöötamisel plaanitavaid meetmeid veelgi põhjalikumalt analüüsima, tuvastama meetmete vajalikkuse ja sobivuse ning hindama neid põhiõiguste harta valguses. Üldjoontes peaks selline tegevusviis liidu õigusloomes inimeste põhiõigustega arvestamist rohkem esile tõsma ning lõpptulemusena kaasa tooma seadusandja vähesemat sekkumist inimeste põhiõigustesse.[149]

2.3.5. Minimaalsed tagatised meetmete rakendamisel

EK viitab EIK varasemale praktikale, kui toob välja, et liidu õigusaktid peavad sätestama selged ja täpsed reeglid meetme ulatuse ja kohaldamise kohta ning kehtestama miinimumnõuded, nii et isikutel, kelle andmeid säilitatakse, oleksid piisavad tagatised, mis võimaldavad tõhusalt kaitsta nende isikuandmeid kuritarvitamise ohu ning ebaseadusliku juurdepääsu ja kasutamise eest. Tagatiste olemasolu on veel vajalikum siis, kui isikuandmeid töödeldakse automaatselt ja kui esineb suur oht, et neile andmetele pääsetakse juurde ebaseaduslikult.[150] Taolisteks miinimumnõueteks on EK hinnangul[151]:

[148] M. - P. Granger (viide 113), lk 844
[149] Vt ka *ibid*, lk 845-846
[150] EKo *Digital Rights Ireland*, p 54-55. Vt ka U. Lõhmus (viide 113), lk 739; E. Guild (viide 133), lk 7
[151] Vt ka U. Lõhmus (viide 113), lk 739-740; F. Boehm (viide 103), lk 40-45

a) kogutavate andmete ulatuse piiritlemine:

Andmete säilitamise direktiiv hõlmab üldistatult kõiki isikuid ning kõiki elektroonilise side vahendeid ja liiklusandmeid, ilma et raskete kuritegude vastu võitlemise eesmärki arvestades oleks ette nähtud mingit eristamist, piirangut või erandit. Kuna elektroonilise side seadmete kasutamine on inimeste igapäevaelus väga levinud, riivab direktiiv seega peaaegu kogu Euroopa elanikkonna põhiõigusi.[152] See tähendab, et direktiiv kohaldub ka isikutele, kelle kohta pole mingeid tõendeid, et nad oleks kasvõi kaudselt seotud raskete kuritegudega. Direktiiv ei näe ette ka ühtegi erandit, mistõttu see kohaldub ka isikutele, kelle sideseansid kuuluvad siseriikliku õiguse kohaselt ametisaladuse alla.[153]

EK peab vajalikuks, et säilitatavate andmete puhul esineks seos ohuga avalikule julgeolekule, säilitataks vaid andmeid kindlal ajavahemikul ja/või kindlas geograafilises piirkonnas ning vaid nende isikute osas, kes võivad olla mingil viisil seotud raske kuriteoga või kelle andmete säilitamine võib muul põhjusel kaasa aidata raskete kuritegude ennetamisele, avastamisele või menetlemisele.[154] Masskogumise puhul kogutakse ka selliste inimeste andmeid, kelle seotuse kohta mõne raske kuriteoga suhtes ei esinegi kahtlusi. Valdav osa ühiskonnast ei pane kunagi toime rasket kuritegu[155] ning nende puhul ei tohiks ka andmete kogumise meetmeid rakendada. Andmete kogumist ja säilitamist puudutavate regulatsioonide puhul on oluliseks diskrimineerimine, s.t üldisele masskogumisele tuleks eelistada sihtmärgistatud (ingl. k *targeted*) kogumise meetodeid.[156]

b) raskete kuritegude määratlemine:

Lisaks eelnevalt nimetatud üldiste piirangute puudumisele ei näe andmete säilitamise direktiiv ette ka ühtegi objektiivset kriteeriumit, mis võimaldaks tagada, et andmeid kasutatakse üksnes põhiõiguste harta artiklites 7 ja 8 ette nähtud põhiõiguste riive

[152] EKo *Digital Rights Ireland*, p 56-67
[153] *Ibid*, p 58
[154] *Ibid*, p 59
[155] P. Schasmin ja C. Ginter (viide 24), lk 47
[156] M. – P. Granger (viide 113), lk 848

ulatust ja raskust arvestades piisavalt "raskete" kuritegude ennetamise, avastamise või kohtus menetlemise eesmärgil. Direktiiv on jätnud "raske kuriteo" mõiste iga liikmesriigi otsustada.[157]

c) tingimuste sätestamine andmetele juurdepääsuks, vajadus eelkontrolliks:

Andmete säilitamise direktiiv ei sõnasta objektiivseid kriteeriumeid ka andmetele juurdepääsu ja nende hilisema kasutamise lubamiseks, eelkõige ei ole piiratud ligipääsuluba omavate isikute arv ning juurdepääs ei sõltu kohtu vm sõltumatu asutuse poolsest eelkontrollist.[158] Kohtulik kontroll on vajalik eelkõige selleks, et tagada kodanike usaldust õigusriigi vastu ning heastada võimalikke kuritarvitusi, selle väärtust ei saa ülehinnata, kuna ametiasutustel on võimalik sisuliselt kõikide isikute andmeid saada ja neid töödelda.[159]

Andmetele juurdepääsule ja nende hilisemale kasutamisele tuleb seega seada materiaal- ja menetlusõiguslikud tingimused selliselt, et juurdepääs ja kasutamine oleks rangelt piiratud eesmärgiga ennetada ja avastada (täpselt piiritletud) raskeid kuritegusid või viia läbi nendega seotud menetlusi.[160]

d) säilitamisperioodide eristamine:

Direktiiv sätestab, et andmete säilitamise miinimumaeg on kuus kuud ja maksimumaeg 24 kuud, kuid ei erista erinevaid tüüpi andmeid (vt eespool) ning jätab täpsustamata, mille alusel tuleks määrata konkreetne säilitamise aeg, et tagada selle piirdumine vältimatult vajalikuga.[161] Andmete säilitamise perioodi peab määrama nende andmete potentsiaalse kasutusvõimaluse järgi ning see peaks olema nii lühike kui vähegi võimalik.[162]

[157] EKo *Digital Rights Ireland,* p 60
[158] *Ibid,* p 62
[159] EIKo 12.01.2016, 37138/14, *Szabo and Vissy vs Hungary*, p 79
[160] EKo *Digital Rights Ireland,* p 61
[161] *Ibid,* p 64
[162] M. – P. Granger (viide 113), lk 848

e) säilitatavate andmete kaitse tagamine ning andmete hävitamine:

Põhiõiguste harta artikkel 8 näeb ette vajaduse sätestada garantiid, mis võimaldaksid tagada säilitatavate andmete tõhusa kaitsmise kuritarvituste ohu eest ning ebaseadusliku juurdepääsu ja kasutamise eest. Andmete säilitamise direktiiv selliseid garantiisid aga ette ei näe. Vajalik on säilitatavate andmete suurest hulgast ja delikaatsusest lähtuvalt paika panna selged ja ranged reeglid tagamaks säilitatud andmete täielik terviklikkus ja konfidentsiaalsus.[163] Samuti on vaja tagada, et sideteenuste või -võrkude pakkujad rakendaksid tehniliste ja korralduslike meetmetega eriti kõrge kaitse- ja turbetaseme, mille valiku puhul ei tohiks lähtuda vaid majanduslikest kaalutlustest. Ilma nimetatud tagatisteta on oht, et säilitatavad andmed saavad avalikuks – kas teadlikult või kogemata sideettevõtja töötajate või häkkerite käe läbi.[164]

Andmeid tuleks EK hinnangul kindlasti säilitada liidu territoorumil, et oleks tagatud andmekaitse ja andmeturbega seotud nõuete täitmise kontrollimise võimalus põhiõiguste harta art 8 lõikega 3 sätestatud liidu sõltumatu asutuse poolt, ning pärast säilitamistähtaja lõppu on vajalik andmed pöördumatult hävitada.[165] Andmete hävitamine on seejuures sideandmete kaitse protsessi väga oluline lüli, kuna sellest, kas ja kuidas andmeid hävitatakse, sõltub suures osas ka andmete kogumise ja kasutamise õiguspärasus.[166]

Eelnimetatud standardeid kasutas EK andmete säilitamise direktiivi proportsionaalsuse hindamisel. Täpsemalt sõltus direktiivis toodud meetmete "vältimatu vajalikkus" ja seega ka kogu direktiivi kehtivus sellest, kas direktiiv sisaldab endas eespool toodud miinimumnõudeid. Kuna andmete säilitamise direktiiv neid miinimumnõudeid ei täitnud, ei piirdunud selles sätestatud meetmed ka "vältimatult vajalikuga", s.t EK hinnangul oli direktiiv ebaproportsionaalne oma eesmärgi suhtes ning seega vastuolus põhiõiguste harta artiklitega 7 ja 8.[167] Sellest

[163] EKo *Digital Rights Ireland*, p 66
[164] L. Drewry (viide 109), lk 737
[165] EKo *Digital Rights Ireland,* p 67-68
[166] Vt ka P. Schasmin ja Ginter (viide 24), lk 46
[167] EKo *Digital Rights Ireland,* p 69

tulenevalt leidis EK, et direktiiv on kehtetu. EK kasutas kõiki eespool toodud miinimumtagatisi direktiivi kehtetuse argumenteerimisel, s.o selle proportsionaalsuse hindamisel, kusjuures EK analüüsis direktiivi vastavust iga nõude osas eraldi. Selline lähenemine viitab, et neid nõuded saab käsitleda ühtse nn kontrollskeemina, mida taoliste riivete proportsionaalsuse hindamise korral peaks läbima.

2.3.6. Etapiviisilisele analüüsile tervikliku lähenemise eelistamine

Väga oluline on *Digital Rights Ireland* lahendist tähele panna ka seda, et EK käsitles sideandmete kogumist, säilitamist ja kasutamist (lisades juurde veel ka direktiivis kajastust mitteleidnud hävitamise etapi) ühtse tervikuna ega pidanud vajalikuks analüüsida proportsionaalsust erinevate etappide kaupa. EK on lähtunud põhimõttest, et ranged reeglid ühes etapis võivad teatud ulatuses kompenseerda puudujääke mõnes teises etapis ja vastupidi. Sisuliselt tähendab see seda, et mida vabam on ligipääs juba kogutud andmetele, seda rangemalt tuleb suhtuda andmete kogumisse ning mida väiksemad on tagatised, et andmed kindlasti hävitatakse, seda piiratum peaks olema andmete kogumine ja nendele ligipääs.[168]

Selline lähenemine aga vastandub Eesti õiguskantsleri lähenemisele, kes analüüsis Eestis andmete säilitamise direktiivi alusel kehtestatud sideandmete kogumise, säilitamise ja kasutamise režiimi etapiliselt, s.t esmalt andmete kogumise ja säilitamise norme ja seejärel nende töötlemist puudutavaid norme. Lähenemise erinevus on antud juhul kaasa toonud ka erinevuse lõplikes seisukohtades – kui EK, kes hindas olukorda tervikuna, leidis, et meetmed on ei ole õigustatud, siis õiguskantsler, kes hindas reeglistikku osade kaupa, leidis, et meetmed ikkagi on õigustatud. Käsitlus, kus hinnatakse üksnes andmete säilitamist, jättes andmete kasutamise ning kuritarvituste vältimiseks piisavate tagatiste puudumise kõrvale, on vägagi vaieldav. Kui lähtuda jätkuvalt Eesti õiguskorrale omasest proportsionaalsuse testist, peaks andmete kogumine, säilitamine, kasutamine ning hävitamine moodustama ühe terviku.[169]

[168] P. Schasmin ja Ginter (viide 24), lk 46
[169] *Ibid*, lk 50

2.4. Olukord peale direktiivi kehtetuks tunnistamist

Peale eespool mainitud põhiõiguste harta art 11 riive analüüsimata jätmise jättis EK veel mõningatele *Digital Rights Ireland* kohtuasja raames esitatud eelotsuse küsimustele vastamata. Kuna EK tunnistas direktiivi kehtetuks, ei pidanud ta vajalikuks analüüsida, kas ja millises ulatuses peaksid siseriiklikud kohtud hindama andmete säilitamise direktiivist üle võetud siseriiklike meetmete kooskõla põhiõiguste harta ja selles ette nähtud tagatistega.[170] Kohtujurist P. Cruz Villalon on oma ettepanekutes seda küsimust käsitlenud ning leidis, et siseriiklikud kohtud on tõepoolest kohustatud analüüsima ja hindama direktiivi üle võtvate riigisiseste õigusaktide kooskõla põhiõiguste hartas ettenähtud tagatistega.[171] Sellel küsimusel on kogu "sideandmete säilitamise saagas" tegelikult keskne roll. EK otsusest jäi selgusetuks, kas selles toodud miinimumstandardit peaks käsitlema kui siseriiklike normide proportsionaalsuse hindamise kohustuslikku kontrollskeemi. Mitmed liikmesriikid ei osanud *Digital Rights Ireland* otsuse järgselt otsustada, mida direktiivist alles jäänud riigisiseste meetmetega edasi peale hakata.

Järgnevalt on käsitletud seda, milline õigus Euroopa Liidu tasandil peale andmete säilitamise direktiivi kehtetuks tunnistamist sideandmete säilitamise osas kohaldub ning kuidas liikmesriigid *Digital Rights Ireland* otsusele reageerisid. Veidi pikemalt käsitletakse Eesti reaktsiooni ning õiguskantsler Ülle Madise seisukohti kehtetu direktiivi alusel Eesti õigusesse ülevõetud ESS-i sätete kehtivuse ning õiguspärasuse osas.

2.4.1. E-privaatsuse direktiiv ja rahvusvahelised inimõiguste kaitset hõlmavad õigusaktid

Andmete säilitamise direktiivi kehtetuks tunnistamine tähendab seda, et Euroopa Liidu tasemel puudub nüüdsest õigusakt, mis kohustaks liikmesriike sideandmeid

[170] EKo *Digital Rights Ireland,* p 72.
[171] EK *Digital Rights Ireland,* kohtujuristi ettepanek, p 51. Vt ka U. Lõhmus (viide 113), lk 740

säilitama.[172] Liikmesriigid peavad sideandmete säilitamise süsteemide rakendamisel järgima e-privaatsuse direktiivis sätestatud nõudeid: mh nõuab nimetatud direktiiv sideandmete konfidentsiaalsuse tagamist ning keelab nende jälgimise, salvestamise ja säilitamise ilma kasutaja nõusolekuta (art 5), samuti kohustab sideteenuse pakkujat andmeid kustutama või anonüümseks muutma, kui need ei ole enam side edastamiseks või arvete esitamiseks vajalikud (art 6).

Kuid loomulikult on üldreeglitest ka erandid: e-privaatsuse direktiivi art 15 lg 1 ütleb, et liikmesriigid võivad riikliku julgeoleku, avaliku korra ning kuritegude ennetamise, uurimise, avastamise ning kohtus menetlemise kaitseks rakendada direktiivi üldistest nõuetest piiranguid, mh võtta tarvitusele meetmeid eelnimetatud eesmärkidel andmete säilitamiseks piiratud aja jooksul. Kõik sellised piirangud peavad aga olema vajalikud, otstarbekad ja proportsionaalsed ning olema kooskõlas Euroopa Liidu õiguse üldpõhimõtetega, sh põhiõiguste hartaga. E-privaatsuse direktiivi preambula punkt 11 täpsustab liikmesriikide kohustust veelgi: direktiivi artikli 15 lõikes 1 nimetatud meetmed peavad olema kooskõlas EIÕK-ga nii nagu seda on tõlgendanud EIK. Liikmesriigid peavad seega oma siseriiklike andmekogumissüsteemide puhul järgima liidu õiguses, eelkõige põhiõiguste hartas, aga ka EIÕK-s ettenähtud sätteid ning arvestama nii EK kui ka EIK poolt antud seisukohtade ja tõlgendustega.[173]

2.4.2. Vastukaja liikmesriikide õiguses

Andmete säilitamise direktiivi kehtetuks tunnistamine ei muuda automaatselt kehtetuks liikmesriikides selle direktiivi alusel kehtestatud siseriiklikke õigusnorme. See, et vastavas valdkonnas puudub nüüdsest Euroopa Liidu raamseadus, ei tähenda, et liikmesriigid ei võiks sideandmete säilitamise kohta luua ise uut siseriiklikku reeglistikku või oma seniseid norme säilitada. Oluline on vaid, et reeglid oleksid kooskõlas Euroopa Liidu õigusega, eelkõige e-privaatsuse direktiivis sätestatuga.[174] Järgnevalt vaadeldakse lähemalt, kuidas liikmesriigid *Digital Rights Ireland* lahendile

[172] Euroopa Komisjon andis oma 16. septembri 2015. a pressiteates teada, et uusi ettepanekuid sideandmete säilitamise reguleerimiseks ei esitata - vt U. Lõhmus (viide 113), lk 740
[173] Vt ka M. - P. Granger (viide 113), lk 848; U. Lõhmus (viide 113), lk 742; F. Boehm (viide 103), lk 46-47
[174] U. Lõhmus (viide 113), lk 740

reageerisid ning milliseid muudatusi tehti siseriiklikes õigusaktides.

2015. aaste oktoobrikuu seisuga (umbes poolteist aastat peale andmete säilitamise direktiivi kehtuks tunnistamist EK poolt) olid vähemalt 11 liikmesriiki andmete säilitamise direktiivi ülevõtvad siseriiklikud sätted kehtetuks tunnistanud (enne *Digital Rights Ireland* lahendit olid seda juba teinud Bulgaaria, Rumeenia, Saksamaa, Küpros ja Tšehhi, kellele peale Digital Right Ireland lahendit lisandusid Austria, Belgia, Leedu, Holland, Poola, Sloveenia, Slovakkia ja Ühendkuningriik[175]) ning 14 liikmesriigis olid vastavad sätted endiselt jõus (Taani, Eesti, Hispaania, Soome, Prantsusmaa, Horvaatia, Ungari, Iirimaa, Luksemburg, Läti, Malta, Portugal ja Rootsi).[176]

Õigusteadlaste hinnangul võimaldas *Digital Rights Ireland* lahend liikmesriikides kahte sorti tõlgendusi: esiteks nn range tõlgendus, mille kohaselt massiline kõikide kasutajate (s.t konkreetse kuriteo või terrorismiohuga seostamata) sideandmete säilitamine on põhiõigustega vastuolus ega ole seetõttu lubatud, ning teiseks nn lubav tõlgendus, mille kohaselt selline sideandmete säilitamine iseenesest ei ole põhiõigustega vastuolus, kui vastavas reeglistikus on olemas piisavad tagatised kasutajate põhiõiguste kaitseks.[177] Liikmesriigid, kus konstitutsioonikohtud on andmete säilitamise direktiivi ülevõtvad siseriiklikud sätted kehtetuks tunnistanud, on lähtunud eelkõige rangest tõlgendusest ning liikmesriigid, kus siseriiklikud sätted on püsima jäänud, on lähtunud eelkõige lubavast tõlgendusest. Rangest tõlgedusest lähtunud kohtute huvi on ilmselgelt olnud rakendada põhiõigustele laiemat kaitset samas kui lubavast tõlgendusest lähtunud liikmesriikide parlamentide ja valitsuste huvi on olnud tagata riiklikele ametiasutustele võimalikult laiad volitused ning kasutada riikliku julgeoleku tagamise huvides kõiki vähegi kättesaadavaid meetmeid.[178]

[175] Ühendkuningriik tühistas küll direktiivi ülevõtva õigusakti, kuid võttis koheselt kiirkorras vastu uue, sisult väga sarnase õigusakti (DRIPA)
[176] Eurojust's analysis of EU Member States' legal framework and current challenges on data retention, 26.10.2015. Arvutivõrgus kättesaadav: http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf (09.04.2017)
[177] N. Vainio ja S. Miettinen. Telecommunications data retention after *Digital Rights Ireland*: legislative and judicial reactions in the Member States. - International Journal of Law and Information Technology, 2015/23, lk 299-300
[178] *Ibid*, lk-d 300 ja 303

Hea näide lubava tõlgenduse rakendamisest on Ühendkuningriik ja Rootsi. Rootsis oli tugev vastuseis andmete säilitamise diretkiivi sätete ülevõtmisele ning vastavad siseriiklikud normid võeti lõpuks vastu alles 2012. aastal. Peale andmete säilitamise direktiivi kehtetuks tunnistamist jäid aga ülevõtvad sätted jõusse, kuna Rootsi valitsus oli seiskohal, et nende sätted vastavad kõikidele EK poolt *Digital Rights Ireland* lahendis väljatoodud tingimustele ega riku seega inimeste põhiõiguseid. Mitmed suuremad telekomiettevõtted, sh Rootsis tegutsev Tele2 Sverige lõpetasid aga sellest hoolimata *Digital Rights Ireland* otsuse valguses päevapealt oma kasutajate sideandmete säilitamise ning kustutasid ka ära kõik seni säilitatud andmed. Kohalik posti- ja telekommunikatsiooni järelevalveasutus tegi seepeale telekomiettevõtetele ettekirjutused, milles kohustas neid siseriiklike õigusnorme järgima ning andmete säilitamisega jätkama.[179]

Ühendkuningriigis võttis valitus peale andmete säilitamise direktiivi kehtetuks tunnistamist kiirkorras vastu uue, nn hädaolukorra seaduse - *Data Retention and Investigatory Powers Act* (DRIPA)[180]. Ühendkuningriigi toonane peaminister David Cameron väljendas seisukohta, et taoline tegevusviis oli vajalik selleks, et telekomifirmad ei lõpetaks andmete säilitamist ega kustutaks juba säilitatud andmeid, kuna vastasel juhul kaoks julgeolekuasutustel võimalus andmeid kasutada ning sellisel juhul "oleksid tagajärjed sünged".[181] Ühendkuningriigi valitsuse hinnangul tegeles EK *Digital Right Ireland* lahendis vaid konkreetselt andmete säilitamise direktiivi analüüsimisega ega andnud hinnangut liikmesriikide, sh Ühendkuningriigi siseriiklikele regulatsioonidele lisades, et nende õigusnormid vastavad nagunii igati EK poolt seatud nõuetele.[182] Tegelikkuses oli uus seadus eelmisele, direktiivist ülevõetud seadusele sisu poolest üsna sarnane, väidetavalt uus seadus isegi laiendas andmete kogumise ja kasutamise võimalusi.[183] Olgugi, et uue seaduse järgi toimus sideandmete kogumine ja säilitamine riigisekretäri (ingl. k *Secretary of State*) vastava

[179] *Ibid*, lk 303-304
[180] Arvutivõrgus kättesaadav: http://www.legislation.gov.uk/ukpga/2014/27/pdfs/ukpga_20140027_en.pdf (09.04.2017)
[181] N. Vainio (viide 177), lk 304
[182] *Ibid*, lk 304-305; vt ka L. M. Woods. High Court Strikes Down Data Retention Laws in Ruling on DRIPA. - European Data Protection Law Review, 3/2015, lk 237
[183] N. Vainio (viide 177), lk 304; L. M. Woods (viide 182), lk 236

korralduse (ingl. k *retention notice*) alusel, ei pidanud selline korraldus tuginema vajadusele uurida, ära hoida või menetleda tõsiseid kuritegusid ega allunud kohtulikule eelkontrollile.[184] Andmetele juurdepääsu ja nende kasutamise osas ei olnud loodud ka sõltumatu järelvalve mehhanismi ning säilitamisperioodidele ei olnud seatud konkreetseid ajalisi piiranguid.[185]

Nii Rootsis kui Ühendkuningriigis algatati andmete säilitamise režiimi vastased kohtuvaidlused – Rootsis vaidlustas kasutajate sideandmete kogumisest loobunud telekomifirma Tele2 Sverige talle riikliku järelvalveasutuse poolt "seaduserikkumise" tõttu tehtud ettekirjutuse ning Ühendkuningriigis taotlesid parlamendiliikmed DRIPA kuulutamist Euroopa Liidu õigusega vastuolus olevaks, kuna see rikub põhiõiguste harta artiklitega 7 ja 8 tagatud kodanike põhiõigusi.[186] Nii Rootsi kui Ühendkuningriigi kohtud esitasid EK-le eelotsusetaotluse. EK liitis need taotlused üheks kohtuasjaks, millest on täpsemalt juttu käesoleva töö 3. peatükis.

Ka Eesti on näide lubavast tõlgendusest. Andmete säilitamise direktiivist võeti siseriiklikusse õigusesse üle ESS § 111^1. Nimetatud säte kohustab kõiki sideettevõtjaid säilitama oma kasutajate sideandmeid vähemalt üks aasta (lg 4), kuid Vabariigi Valitsus võib avaliku korra ja riigi julgeoleku huvides tähtaega ka "piiratud ajavahemikuks" pikendada (lg 6). Andmeid tuleb säilitada Euroopa Liidu territooriumil (lg 5) ning sideettevõtja peab mh tagama andmete turvalisuse ja kaitse ning piirama neile juurdepääsuvõimalusi (lg 9). Sideandmeid peab edastama mh uurimisasutusele, jälitusasutusele, prokuratuurile, kohtule (sh tsiviilkohtule), julgeolekuasutusele, Andmekaitse Inspektsioonile, Finantsinspektsioonile, Keskkonnainspektsioonile, Politsei- ja Piirivalveametile, Kaitsepolitseiametile, Maksu- ja Tolliametile (ESS § 111^1 lg 11). Sätted, mis puudutavad andmetele ligipääsu ning nende kasutamist asuvad reeglina eriseadustes – nt kriminaalmenetluse seadustik (KrMS)[187], julgeolekuasutuste seadus (JAS)[188], väärteomenetluse seadustik (VtMS)[189], maksukorralduse seadus (MKS)[190], politsei ja piirivalve seadus (PPVS)[191],

[184] L. M. Woods (viide 182), lk 237
[185] N. Vainio (viide 177), lk 305
[186] *Ibid*
[187] RT I, 31.12.2016, 46
[188] RT I, 17.12.2015, 39
[189] RT I, 01.03.2017, 5

korrakaitseseadus (KorS)[192] jne. ESS § 111[1] ja seda täiendavate eriseaduste sätete sisu kohta saab täpsemalt lugeda Piret Schasmini magistritöö alapunktist 3.

Seadusandja ja valitsuse tasandil ei ole Eestis sideandmete säilitamise teemal suuremat diskussiooni olnud. Riigikohtu kriminaalkolleegium on 23.02.2015.a lahendis 3-1-1-51-14 põgusalt käsitlenud sideandmete säilitamist ja nende politseile kättesaadavaks tegemise põhiseaduspärasust seoses tõendi lubatavuse küsimusega ning leidnud, et ESS regulatsioon ei ole vastuolus põhiseadusega ulatuses, mis võimaldab taotleda ja kasutada sideettevõtja andmeid kriminaalmenetluses. [193] Teemat on kõige põhjalikumalt käsitlenud õiguskantsler Ülle Madise, kes on oma 20.07.2015 seisukohas elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta leidnud, et andmete ennetava kogumise ja säilitamise regulatsioon, nagu see on ette nähtud ESS §-s 111[1] ei ole selgelt ebamõõdukas ega ole põhiseadusega vastuolus. Õiguskantsler möönis siiski sama seisukoha raames, et andmete kogumise ja säilitamise normistik ei ole täiuslik ning et täitevvõim peaks analüüsima olemasolevate menetluslike garantiide piisavust, sh sideteenuse osutajate senist praktikat oma kohustuste täitmisel, võimalikke toimunud kuritarvitusi jne. Õiguskantsleri hinnangul tuleks vajadusel kaaluda andmete säilitamise nõuete (eelkõige turvalisusnõuete) ning nende hävitamise korra täpsustamist, samuti andmetele ligipääsu omavate isikute ringi täpsemat määratlemist ning eraldi järelevalvemehhanismi sätestamist.

Nagu eespool öeldud, vaatles õiguskantsler oma 2015. a seisukohas andmete kogumist ja säilitamist nende hilisemast kasutamisest ja töötlemisest eraldiseisvalt. Kogutud andmete töötlemise osas esitas õiguskantsler 2016. a täiendava hinnangu, kus leidis taaskord, et ESS § 111[1] ja muude normidega ette nähtud sideandmete säilitamise ning edasise töötlemise süsteem ei ole vastuolus põhiseadusega. Õiguskantlser pidas siiski vajalikuks rõhutada, et täitevvõimul ja seadusandjal tuleb üle vaadata olemasolevad menetluslikud garantiid: mh tuleks ühtlustada andmete töötlemisele esitatavaid nõudeid erinevates menetlustes; kaaluda kohtu või muu

[190] RT I, 31.03.2017, 3
[191] RT I, 15.12.2016, 7
[192] RT I, 02.12.2016, 6
[193] RKKKo 3-1-1-51-14, p 22.4. Vt ka U. Lõhmus (viide 113), lk 741; P. Schasmin (viide 23), lk 70

sõltumatu organi poolt antava eelneva loa nõude üldist rakendamist sideandmetele ligipääsu saamiseks ja andmesubjekti teavitamist tema õiguste piiramisest; andmesubjektide ringi piiritlemist nii kitsalt kui võimalik; hinnata andmete nõudmise aluste ulatust ning vältida andmete nõudmise võimaldamist põhjendamatult laiadel või õigusselgusetutel alustel. Muuhulgas viitab õiguskantsler oma 2016. aasta seisukoha lõpus, et sideandmete töötlemise õiguspärasuse hindamisel tuleb arvestada arenguid Euroopa Liidu ja rahvusvahelisel tasandil ning kui EIK või EK praktikast peaks tulevikus "selgelt nähtuma, et Eestis olemasolevad alused või menetlusnõuded ei vasta kohustuslikule minimaalsele põhiõiguste kaitse standardile", on riigisisese õiguse muutmine vältimatu.

Õiguskantsleri nn "õigeksmõistvat" otsust ESS §-le 111[1] on Eesti õiguskirjanduses kritiseeritud. Uno Lõhmus, kes on tegutsenud nii EIK kui EK kohtunikuna, on leidnud, et õiguskantsleri argumendid ei ole veenvad ning et Eestis ei tohiks privaatsusõigus nõuda vähemat tähelepanu kui teistes Euroopa Liidu liikmesriikides.[194] Piret Schasmin on oma magisritöös kirjutanud, et õiguskantsleri analüüsis puudub sisuline riive vajalikkuse kui ka mõõdukuse hindamine ning formaalselt ühe või kahe menetlusliku garantii olemasolu ei tähenda veel seda, et rakendatavad meetmed on piisavad ja tõhusad.[195] Autorile jääb arusaamatuks, miks on õiguskantsler valinud sellise tee, et on tunnistanud kehtivad sätted põhiseadusega kooskõlas olevateks kuid juhtinud samaaegselt seadusandja tähelepanu seaduse mitmetele puudujääkidele viidates ka EK praktikas toodud samasisulistele nõuetele. Võimalik, et sellise seisukohani on õiguskantsleri viinud andmete kogumise ja säilitamise käsitlemine nende hilisemast kasutamisest ja töötlemisest eraldi – kui vaadata kogu regulatsiooni tervikuna, tuleks liita igas etapis, s.o andmete kogumise, säilitamise, töötlemise ja hävitamise etapis esinevad puudujäägid ning puudujääkide osakaal muutub seeläbi suuremaks. See võib omakorda mõjutada kogu regulatsiooni kehtivust ja põhiseaduspärasust.[196] U. Lõhmuse hinnangul on õiguskantsler tahtnud oma argumentatsiooniga öelda, et seadusandja kehtestatud õigusnormid on kõll põhiseaduspärased, kuid nende kohaldamispraktika võib olla põhiseadusvastane.[197]

[194] U. Lõhmus (viide 113), lk 741
[195] P. Schasmin (viide 23), lk 70-72
[196] Vt ka *ibid*, lk 70
[197] U. Lõhmus. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. -

Autor nõustub P. Schasmini ja U. Lõhmuse seisukohtadega selles osas, et õiguskantsler ei näe ekslikult sideandmete säilitamist ja kasutamist piisavalt intensiivse riivena, kuna ta ei pea seda sõnumi saladuse kaitsealas olevaks. Õiguskantsleriga vastupidist leiavad aga nii EIK ja EK, kelle hinnangul võivad sideandmed sideseansi kohta öelda väga palju ning on seega sama tundliku loomuga kui sideseansi sisu.[198] Autor nõustub eelnimetatud autorite seisukohtadega ka selles osas, et õiguskantsler oleks pidanud analüüsima probleemi tervikuna, mitte jagama seda etappideks, s.o käsitlema andmete kogumist ja säilitamist nende hilisemast kasutamisest ja töötlemisest eraldi.

Tõenäoliselt tõstatavad hiljutised arengud EK praktikas (analüüs järgmises peatükis) Eestis antud diskussiooni lähiajal ka laialdasemalt ning seadusandja peab kehtivat regulatsiooni muutma sõltumata õiguskantsleri senistest hinnangutest.

Juridica X/2016, lk 699

[198] Vt P. Schasmin (viide 23), lk 72-74; U. Lõhmus (viide 197), lk 700

3. SIDEANDMETE KAITSE LAIENDAMINE JA KRITEERIUMITE KINNISTAMINE

Peale EK otsust asjas *Digital Rights Ireland* on rahvusvahelisel tasandil nn digitaalajastu privaatsusõiguse kaitsele aina enam tähelepanu pööratud. EK-lt on vahemikus 2014-2016 tulnud 3 antud valdkonnas olulise tähtsusega lahendit: a) *Schrems*, milles EK tunnistas kehtetuks Edward Snowdeni avalduste järgselt "kurikuulsaks" saanud Euroopa Liidu ja USA vahelise andmeedastuskokkuleppe *Safe Harbour*, b) *Google Spain*, milles EK tunnustas inimeste õigust "olla unustatud" ning koos sellega tähtsustas privaatsusõigust sõna- ja väljendusvabadusest enam, ja c) *Tele2 Sverige*, millega EK pani selged piirid liikmesriikidesiseste sideandmete säilitamise alaste õigusaktide sisule ja kehtivusele. EIK-lt on samal ajal paralleelselt tulnud olulised lahendid kohtuasjades *Szabó ja Vissy* ning *Zakharov*[199], kus EIK annab omapoolse hinnangu andmete masskogumist jm viisil kodanike jälgimist võimaldavatele õiguslikele režiimidele.

Käesolevas peatükis analüüsib autor eelkõige EK lahendit *Tele2 Sverige* ning uurib, kas EK järgib *Digital Rights Ireland* lahendis toodud proportsionaalususe hindamise nn kontrollskeemi ning kas EK lisab sinna veel mõningaid elemente. Autor tuvastab käesolevas peatükis ka puudujäägid Eestis kehtivas sideandmete regulatsioonis, lähtudes eelnimetatud kontrollskeemist.

3.1. Hiljutised Euroopa Inimõiguste Kohtu seisukohad

Enne kui autor asub *Tele2 Sverige* lahendit analüüsima, käsitletakse põgusalt EIK praktikat samas valdkonnas. Peale EK otsust asjas *Digital Rights Ireland* on ka EIK teinud riigipoolset andmetekogumist ning kodanike massilist jälgimist puudutavad lahendid kohtuasjades *Szabó ja Vissy* 2016. a jaanuaris ning *Zakharov* 2015. a detsembris. *Szabó ja Vissy* lahendis oli analüüsimisel Ungaris kehtinud

[199] EIKo 04.12.2015, 47143/06 *Roman Zakharov vs Russia*

terrorismivastane seadus, mis võimaldas ametivõimudel koguda infot salajaste läbiotsimiste, pealtkuulamiste vm jälgimisviiside teel, sh pääseda ligi sideteenuste kasutajate sideandmetele ning ka sideseansi sisule. EIK pidas inimeste sideseansside ulatuslikku jälgimist terrorismivastase võitluse õigustusel iseenesest aktsepteeritavaks, kuid lisas, et oluline on jälgida, kas arengud inimeste andmete kogumiseks kasutatavates tehnoloogilistes lahendustes käivad käsikäes arengutega samaaegselt inimestele kaitset võimaldavates õiguslikes tagatistes.[200]

Ungari seaduses EIK hinnangul vajalikud tagatised puudusid: a) jälgimise objektiks võis olla valimatult igaüks, s.t isikute ringi ei olnud piiratud nendega, kes olid terrorismijuhtumis kahtlusalused või juhtumiga muul moel seotud,[201] b) jälgimise meetme rakendamise üle otsustas täitevvõim, s.t puudus sõltumatu (kohtulik) eelkontroll, mille raames oleks meetme rakendamise vajalikkust ja põhjendatust kontrollitud ning selle jaoks tõendeid esitatud,[202] c) isikuid, kelle suhtes oli seaduses toodud meetmeid rakendatud, sellest asjaolust ei teavitatud ning neil puudus seega reaalne võimalus oma õiguseid kaitsta[203] ning d) ebaselge oli tähtaegade pikkus, s.t puudus konkreetne ajaline piirang meetmete rakendamise ning andmete säilitamise puhuks.[204] Sellises olukorras olid Ungari valitsusel sisuliselt piiramatud võimalused inimeste eraellu sekkumiseks ning saadud informatsiooni kuritarvitamiseks.[205] Vajalike tagatiste puudumise tõttu rikkus Ungari seadus EIK hinnangul EIÕK artiklis 8 nimetatud privaatsusõigust.

Zakharov lahendis oli olukord analoogne – Venemaa seadused võimaldasid julgeoleku huvides salaja jälgida inimeste sideseansse, kuid õiguslike tagatistega ei olnud välistatud võimalikud kuritarvitused ja volituste ületamised. Probleemid esinesid taaskord selles, et a) isikute ja juhtumite ring, mille puhul meetmeid võis rakendada, ei olnud piisavalt selged ja määratletud[206] ning b) meetme rakendamiseks ning andmete säilitamiseks polnud selgeid ajalisi ja menetluslikke piiranguid, mistõttu

[200] EIKo *Szabo and Vissy*, p 66
[201] *Ibid*, 66-67
[202] *Ibid*, p-d 67, 71-73, 75 jj
[203] *Ibid*, p 82 jj
[204] *Ibid*, p 74
[205] Kohtuliku kontrolli vajalikkuse ning vastavate EIK seisukohtade kohta vt ka P. Schasmin (viide 23), lk 45
[206] EIKo *Zakharov*, p 243 jj

ametivõimudel oli jälgimise teostamiseks väga suur kaalutlusõigus.[207] Samuti olid probleemkohad c) eelkontrolli ja järelvalve ebapiisavuses ja läbipaistmatuses[208] ja d) isikute nende jälgimisest teavitamata jätmises, mistõttu oli neil praktiliselt võimatu oma õiguseid kaitsta.[209] Kohtuliku kontrolli ja järelevalve olulisusele on EIK *Zakharov* lahendis seejuures pühendanud pikki lõike – olgugi et Venemaa õiguses oli formaalselt kohtuliku kontrolli aspekt sisse kirjutatud, ei toiminud see EIK hinnangul praktikas selliselt, et oleks võimaldanud analüüsida jälgimismeetme põhjendatust ning "vältimatut vajalikkust" ning seetõttu ei olnud praktikas kohtuliku kontrolli tagatis tegelikult esindatud.[210]

Lahendid *Zakharov* ja *Szabo* kinnistasid EIK varasemas praktikas väljaöeldud seisukohti. Nii *Zakharovi* kui *Szabo* lahendi ning ka EIK varasema praktika najalt saab järeldada, et EIK nõuab olukorras, kus inimeste põhiõigustesse sekkutakse küll õigustatud alusel (julgeolek, võitlus kuritegevuse või terrorismi vastu), kasutatavate meetmete proportsionaalsuse ranget hindamist ning kohtupraktikas korduvalt välja toodud tagatiste olemasolu. EIK märgib, et "riikidele on küll tagatud kaalutlusõigus rakendamaks isikute privaatsust riivavaid meetmeid selleks, et kaitsta riiklikku julgeolekut, kuid EIK roll on tagada, et kasutatavad meetmed ei õõnestaks teenitavat eesmärki, s.t lõhuks samal ajal demokraatlikke väärtuseid, mille kaitseks nad algselt on loodud; sellise olukorra välistamiseks peavad õiguses olema sisseseatud meetmete kuritarvitamist välistavad tagatised."[211]

On väidetud, et EIK on pelgalt EIÕK art 8 kaitsmisele lisaks võtnud missiooniks avaldada arvamust tänapäeval eri riikides laialdaselt kasutuses olevate massjälgimise ja –andmekogumise režiimide osas.[212] *Szabo* ja *Zakharovi* pinnalt saab järeldada, et EIK mõistab aina konkreetsemalt hukka meetodeid, mille raames kogutakse valimatult kõikide inimeste andmeid: jälgimise ning andmetekogumise ja säilitamise

[207] *Ibid*, p 250 jj
[208] *Ibid*, p 257 jj
[209] *Ibid*, p 286 jj
[210] *Ibid*, p 257-263. Vt ka P. Schasmin (viide 23), lk 46
[211] EIKo *Szabo and Vissy*, lk p 57; EIKo *Zakharov*, p 232
[212] P. de Hert ja P. C. Bocos. Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment. – Strasbourg Observers, 23.12.2015. Arvutivõrgus kättesaadav: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ (09.04.2017)

meetmeid tohib rakendada vaid õigusaktis kindlaksmääratud isikute suhtes kindlaksmääratud juhtumite raames ja kindlaksmääratud alustel. Näiteks Szabo lahendi punktides 53 ja 73 märgib EIK muuhulgas, et meetme "vältimatut vajalikkust" tuleb lisaks üldisele plaanile hinnata ka konkreetse juhtumi/menetluse ning kindla isiku sideühenduse raames. Kõiki eelnimetatud asjaolusid on EIK arvates seejuures pädev hindama eelkõige kohus, ja seda mitte pelgalt formaalselt, vaid sisuliselt ja sõltumatult.[213]

Samal ajal, kui EIK on massjälgimise iseenesest hukka mõistnud, on ta aga ka möönnud, et tänapäevaseid terroristlikke rünnakuid saab ennetada vaid moodsate tehnoloogiliste vahenditega, sh sellistega, mis võimaldavad massilist kommunikatsioonivahendite jälgimist ja sideandmete kogumist.[214] Jääb selgusetuks, kuidas seda EIK seisukohta tuleks tõlgendada – kas tegemist on muutustega leppimise ning tõdemisega, et privaatsust jääb inimestele aja möödudes vältimatult aina vähemaks.[215]

3.2. Euroopa Kohtu lahend *Tele2 Sverige*

EIK kõrval on ka EK seisukohtadel suur tähtsus sideandmete kogumise jm massjälgimise režiimide hindamise kontekstis. Tundub, et EIK ja EK on ühendanud jõud, et asuda kaitsma inimeste põhiõiguseid. Tähelepanu väärib, et EIK tsiteerib oma lahendites EK seisukohti ja vastupidi.[216] Viimased arengud EIK praktikas said välja toodud eelmises alapunktis ning järgnevalt käsitleb autor värskeid arenguid EK praktikas lahendi *Tele2 Sverige* valguses.

Nagu eespool öeldud oli EK eelmisel samateemalisel lahendil *Digital Rights Ireland* Euroopa Liidu liikmesriigiti erinev vastukaja. Osad liikmesriigid lähtusid nn rangest tõlgendusest, s.t leidsid, et igasugune sideandmete masskogumine ja –säilitamine on

[213] EIKo *Zakharov*, p 232
[214] EIKo *Szabo and Vissy*, p 68
[215] Vt ka Ambiguous judgment of the European Court of human rights on surveillance issues. - Association Européenne pour la défense des Droits de l'Homme (AEDH). Arvutivõrgus kättesaadav: http://www.aedh.eu/Ambiguous-judgment-of-the-European.html (09.04.2017)
[216] Vt EK lahendid *Digital Rights Ireland* ja *Tele2 Sverige* ning EIK lahendid *Zakharov* ja *Szabo and Vissy*

põhiõigustega vastuolus ning tühistasid riigisisesed sideandmete säilitamist reguleerivad õigusaktid, ning teised liikmesriigid lähtusid hoopis nn lubavast tõlgendusest, s.t leidsid, et sideandmete massiline säilitamine ei ole probleem, kui õigusaktides sisalduvad vajalikud tagatised põhiõiguste kaitseks. Mainitud sai ka, et Rootsi ja Ühendkuningriik esindasid mõlemad lubava tõlgenduse leeri ning nimetatud riikide kohtutesse jõudsid vaidlused, kus tugineti siseriikliku õiguse vastuolule Euroopa Liidu õigusega.

Rootsi ja Ühendkuningriikide kohtud esitasid EK-le eelotsusetaotlused selle kohta, kuidas tõlgendada e-privaatsuse direktiivi koostoimes põhiõiguste hartaga. Täpsemalt olid eelotsusetaotluse olulisimateks küsimusteks a) kas üldine kohustus säilitada kuritegevuse vastu võitlemise eesmärgil sideandmeid, mis hõlmab eranditult ja ilma igasuguste piiranguteta kõiki isikuid, kõiki seadmeid ja kõiki andmeid, on lubatud[217] ning b) kas lahendis *Digital Rights Ireland* nimetatud tagatised on liikmesriigi õiguse suhtes imperatiivsed nõuded.[218] Ümbersõnastatult on tegemist küsimustega, kas massjälgimine on lubatud ning kas eespool käsitlemist leidnud nn kontrollskeemi on siseriiklike regulatsioonide proportsionaalsuse hindamisel kohustuslik järgida.

EK liitis Rootsi ja Ühendkuningriigi eelotsusetaotlused üheks kohtuasjaks: *Tele2 Sverige*. Lahendis EK poolt esitatud olulisemad seisukohad on välja toodud alljärgnevalt.

3.2.1. Sideandmete säilitamine ja töötlemine on üks tervik ning langeb Euroopa Liidu õiguse kohaldamisalasse

Esimese olulise punktina *Tele2 Sverige* lahendis saab välja tuua seisukoha, et nii sideandmete kogumine kui ka andmetele hilisem juurdepääs ja nende töötlemine siseriiklike ametiasutuste poolt kuuluvad e-privaatsuse direktiivi, s.t liidu õiguse kohaldamisalasse. Olgugi, et e-privaatususe direktiivi art 1 lõike 3 kohaselt ei hõlma see direktiiv riikide tegevust karistusõiguse, avaliku korra, riigikaitse ja julgeoleku valdkondades, s.t art 15 lõikes 1 nimetatud meetmeid, mille alla siseriiklikud

[217] EKo *Tele2 Sverige*, p 51
[218] *Ibid*, p 59

sideandmete kogumise ja säilitamise reeglistikud kuuluvad, selgitab EK, et kuna direktiivi artikliga 15 on riigi julgeoleku huvides üleüldse võimaldatud erimeetmeid rakendada, siis peavad need meetmed – nii andmete kogumine ja säilitamine kui ka andmetele juurdepääs ja nende töötlemine ametiasutuste poolt kuuluma direktiivi kohaldamisalasse.[219]

Seega on kogu sideandmete kogumist, säilitamist ja kasutamist puudutav tegevus Euroopa Liidu õiguse kohaldamisalas ning vastava valdkonna riigisisese õiguse tõlgendamisel ja rakendamisel tuleb lähtuda Euroopa Liidu õigusaktidest, sh põhiõiguste hartast ning EK praktikast. Liikmesriigid, kes lootsid, et kehtetuks tunnistatud andmete säilitamise direktiivi alusel vastu võetud normid muutusid puhtalt riigisiseseks õiguseks ning seega õnnestub neil vältida EK lahendis *Digital Rights Ireland* väljendatud seisukohtade rakendamist,[220] peavad nüüd oma seisukohta igal juhul muutma. Üheks selliseks riigiks on kahtlemata Eesti – õiguskantsler on hinnanud ESS regulatsiooni kehtivust lähtuvalt PS-st, kuid tegelikkuses on vaja seda hinnata hoopis e-privaatsuse direktiivi ja põhiõiguste harta valguses.

Märkimisväärne on ka asjaolu, et EK vaatleb taaskord andmete kogumist ja säilitamist ühtse tervikuna koos andmetele hilisema juurdepääsu ja töötlemisega (jõudes seejuures ka seisukohale, et mõlemad režiimi osad langevad Euroopa Liidu õiguse ja e-privaatsuse direktiivi kohaldamisalasse). See tähendab, et tagatised peavad olema seatud kogu režiimi ulatuses ning rakendatava meetme proportsionaalsuse hindamisel arvestatakse nii andmete kogumise ja säilitamise raames seatud tagatiste kui ka hilisema juurdepääsu ja töötlemise raames seatud tagatiste olemasolu ja sisuga. Ka kohtujurist Henrik Saugmandsgaard Øe (kes leidis oma ettepanekus küll, et andmetele juurdepääs ei kuulu direktiivi kohaldamisalasse) hinnangul ei saa andmete säilitamise ja juurdepääsu probleeme täielikult üksteisest lahutada: juurdepääsu reguleerivatel õigusnormidel on määrav tähtsus selle üle otsustamisel, kas sätted, millega kehtestatakse üldine andmete säilitamise kohustus, on põhiõiguste hartaga kooskõlas, s.t andmete säilitamise kohustuse vajalikkuse ja proportsionaalsuse

[219] *Ibid*, p 69-81. Vt ka U. Lõhmus (viide 197), lk 704-705
[220] P. Shasmin ja C. Ginter (viide 24), lk 43

hindamisel tuleb juurdepääsu reguleerivaid õigusnorme arvesse võtta.[221]

Selline hinnang erineb kardinaalselt õiguskantsler Ülle Madise lähenemisest ESS põhiseaduspärasuse hindamisel – õiguskantsler vaatles andmete säilitamist eraldi nende hilisemast kasutamisest ning hindas ka sätete proportsionaalsust vaid konkreetse etapi kontekstis, s.t ei arvestanud andmete säilitamist võimaldavate meetmete sobivuse ja vajalikkuse hindamisel seda, millistel tingimustel on neid andmeid hiljem võimalik erinevatel ametiasutsutel kasutada. Nagu eespool toodud, leiab autor, et see oli suuresti põhjuseks, miks õiguskantsler tunnistas EK varasema tõlgendusega *Digital Rights Ireland* kohtuasjas selges konfliktis olevad Eesti seadusesätted põhiseadusega kooskõlas olevateks. Sideandmete kogumine, säilitamine ning kasutamine ja töötlemine on tervikuna Euroopa Liidu õiguse kohaldamisalas, samuti on EK selle proportsionaalsust hinnanud tevikuna. Puudub alus Eesti vastava regulatsiooni puhul lähtuda teistsugusest lähenemisest, s.t ESS-st jm eriseadustest tulenevat sideandmete regulatsiooni tuleb hinnata tervikuna ning lähtuvalt e-privaatuse direktiivist ja põhiõiguste hartast, mitte põhiseadusest.

3.2.2. E-privaatsuse direktiivi art 15 lg 1 kitsas tõlgendamine ning sideandmete masskogumise keelustamine

Väga oluline on EK seisukoht e-privaatsuse direktiivi art 15 lõike 1 alusel rakendatavate meetmete hindamise osas: EK hinnangul tuleb seda sätet tõlgendada kitsalt arvestades seejuures direktiivi artiklis 5 nimetatud sideandmete konfidentsiaalsuse tagamise kohustuse ulatust. Konfidentsiaalsuse tagamise kohustus seisneb eelnimetatud sätte kohaselt selles, et liikmesriik peab oma õigusega tagama üldkasutatava sidevõrgu ja üldkasutatavate elektrooniliste sideteenuste kaudu toimuva side ja sellega seotud liiklusandmete konfidentsiaalsuse sellselt, et kõrvalistel isikutel oleks keelatud pealt kuulata, salvestada või muul viisil jälgida sideseanssi ja sellega seotud liiklusandmeid ilma asjaomaste kasutajate loata.

Kitsas tõlgendus tähendab esmalt seda, et art 15 lõike 1 esimeses lauses nimetatud aluste (riiklik julgeolek, riigikaitse, avalik kord, kriminaalkuritegude või

[221] EK *Tele2 Sverige*, kohtujuristi ettepanek, p 125

elektroonilise sidesüsteemi volitamata kasutamise ennetamine, uurimine, avastamine ja kohtus menetlemine või direktiivi 95/46/EÜ art 13 lõikes 1 nimetatud muu eesmärk) loetelu on ammendav, s.t liikmesriigid ei või rakendada meetmeid ühelgi muul alusel. Teisalt tähendab kitsas tõlgendus seda, et kõik art 15 lõike 1 alusel rakendatavad meetmed peavad olema kooskõlas liidu õiguse üldpõhimõtetega, sh põhiõiguste hartaga tagatud põhiõigustega.[222]

EK kordab *Digital Rights Ireland* lahendis toodud seisukohta, et sideandmed võimaldavad teha täpseid järeldusi isiku eraelu kohta lisades, et nende abil on võimalik lihtsasti koostada isiku profiili. Sideandmed on EK hinanngul sama tundliku iseloomuga kui sideseansi sisu ning õigusnormid, mis lubavad sideandmeid koguda, säilitada ja kasutada, kujutavad endas põhiõiguste harta artiklites 7 ja 8 nimetatud põhiõiguste eriti ulatuslikku ja rasket riivet. Riive raskuse tõttu saab selliseid meetmeid põhjendada ainult võitlusega raskete kuritegude vastu.[223]

Nimetatud seisukoht on oluline, kuna sellega piiratakse konkreetselt liikmesriikide võimalusi allutada nimetatud sättes toodud erandi alla ka muid eesmärke teenivaid meetmeid. Eesti õigusest saab siinkohal välja tuua näite sideandmete muul kui e-privaatsuse direktiivi art 15 lõikes 1 nimetatud eesmärgil kasutamise kohta: kindlustustegevuse seaduse (KindlTS)[224] § 219 lõikega 1 on kindlustusandjatele antud võimalus kasutada sideandmeid kindlustusjuhtumi lahendamiseks. Julgen väita, et kindlustusjuhtumite lahendamine ei kuulu eespool välja toodud e-privaatsuse direktiivi art 15 lõikes 1 nimetatud eesmärkide hulka, samuti ei tohiks olla vaidlust teemal, et kindlustuskelmuste puhul ei ole tegemist raskete kuritegudega.[225]

Kitsa tõlgenduse vajaduse osas rõhutab EK, et artikliga 15 lubatud erandid artiklis 5 ette nähtud põhimõttest ei saa olla reegliks, kuna vastasel juhul jääks artikkel 5 suuresti sisutühjaks.[226] Kui liikmesriik rakendab artikliga 15 lubatud meetmeid üldiselt ja eristamatult kõikide isikute, kõikide sidevahendite ja –andmete suhtes, siis

[222] EKo *Tele2 Sverige*, p 90-91. Vt ka U. Lõhmus (viide 197), lk 705
[223] *Ibid*, p 99-102. Vt ka U. Lõhmus (viide 197), lk 705
[224] RT I, 31.12.2016, 26
[225] Vt ka P. Schasmin ja C. Ginter (viide 24), lk 45
[226] EKo *Tele2 Sverige*, p 89

ei ole tegemist enam erandiga vaid juba reegliga.[227] Sellega mõistab EK hukka nii Rootsi kui Ühendkuningriigi õigusnormid ning ühtlasi ka kõikid teised sideandmete massilist kogumist ja säilitamist võimaldavad reeglistikud: õigusnormid, mida kohaldatakse ka isikutele, kelle puhul puudub igasugune seos raskete kuritegudega, väljuvad rangelt vajaliku piiridest ning neid ei saa põhiõiguste harta artiklites 7 ja 8 toodud põhimõtteid arvestades lugeda e-privaatsuse direktiivi art 15 lõike 1 alusel põhjendatuks.[228]

Eelnimetatud seisukoht on ülimalt tähelepanuväärne, kuna sellega ütleb EK, et sideandmete üldine ja eristamatu masskogumine ei ole õiguspärane. Kodanike ulatusliku riigipoolse jälgimise vastastes ringkondades, mida olid 2013. aastal vapustanud Edward Snowdeni avaldused meeletutest andmekogudest USA riikliku julgeolekuasutuse NSA valduses, saadi *Tele2 Sverige* lahendi üle kindlasti rõõmustada, kuna sellega keelustas EK sisuliselt ära kõik Euroopa Liidu liikmesriikide üldised ennetavad andmekogumise režiimid. Sama rõõmsalt ei suhtunud lahendisse tõenäoliselt riikliku julgeoleku tagamise ning kuritegevuse ja terrorismi vastase võitluse eest seisvad ringkonnad, kuna andmete massilise kogumise ja säilitamise keeluga võetakse õiguskaitse- ja luureasutustelt ära lihtne võimalus tõendite jm menetlusliku teabe kogumiseks.

Oluline on eristada seda, et EK ei pea kõiki julgeoleku huvides sideandmete kogumise ja säilitamise meetmeid otseselt lubamatuteks – nn sihtmärgistatud, s.t konkreetse juhtumi ja vajaduse alusel piiritletud andmete kogumine on lahendis mainitud tagatiste olemasolu korral igati adekvaatne tegevus. Üldine ennetav andmete kogumine ja säilitamine ei saa EK hinnangul aga kuidagi olla proportsionaalne meede ja seda ka terrorismivastase võitluse kontekstis. EK on üldise säilitamiskohustuse taunimisega asunud teisele seisukohale kui kohtujurist Henrik Saugmandsgaard Øe, kes oma 19.06.2016.a ettepanekus leidis, et *Digital Rights Ireland* lahendiga ei tahtnud EK öelda, et (andmete, andmesubjektide, eesmärkide) eristamise puudumine andmete kogumise ja säilitamise reeglites ei tähenda, et niisugune meede ületab

[227] *Ibid*, p 104
[228] *Ibid*, p-d 105-107, 112

vältimatu vajalikkuse piire;[229] ning üldine andmete säilitamise kohustus ei ületa iseenesest vältimatu vajalikkuse piire, kui sellega kaasnevad andmetele juurdepääsu, nende säilitamise kestuse ning kaitse ja turve alased tagatised.[230]

Üldise masskogumise keelule on avaldatud ka kriitikat. Iga inimene võib potentsiaalselt olla kurjategija ning tihti ei ole õiguskaitseorganitel ilma juba nn eelkogutud sideandmeteta võimalik kuriteole üldse jälile saada – nt küberkuritegude puhul on reeglina ainus juhtlõng toimepanija IP-aadress ning olukorras, kus IP-aadresse eelnevalt säilitatud ei ole ning õiguskaitseorganid alustavad uurimist peale sellise kuriteo toimepanemist, ei ole neil võimalik toimepanija kohta enam kuidagi tõendeid saada. [231] Üldise masskogumise alternatiivina välja pakutud nn sihtmärgistatud andmete kogumine ei saa omada sarnaseid tulemusi, kuna on oma ulatuse poolest oluliselt piiratum. Andmeid hakatakse sel juhul koguma alles hetkest, mil on tekkinud põhjendatud kahtlus, et isik on seotud raske kuriteoga (ingl k *quick-freeze*), sellele hetkele eelnevast ajast andmeid aga võtta ei ole. Masskogutud andmed tagavad seega õiguskaitseorganitele vajalikud eeldused raskete kuritegude uurimiseks, avastamiseks ja menetlemiseks.[232]

EK argumentatsioonist nähtub aga hoiak, et andmete kogumise eelduseks peab olema põhjendatud kahtluse olemasolu ning vastupidist olukorda, kus andmete kogumine on eelduseks põhjendatud kahtluse olemasolu tekkele, ei saa olla.[233] See on väga oluline seisukoht, kuna kaasaegsete tehniliste võimaluste arenedes tekib õiguskaitseasutustel aina enam soovi neid võimalusi kasutada ning teha sellega oma tööd lihtsamaks – selle asemel, et koguda kahtlustuse kinnitamiseks kuude kaupa materjale, küsitleda tunnistajaid, uurida asitõendeid jne soovitakse reeglina minna lihtsama vastupanu teed ning formuleerida kahtlustus isiku viimase aasta sideandmete (mis, nagu eespool korduvalt mainitud, võivad anda isiku kohta välja tundlikku eraelulist teavet) väljavõtte põhjal. Autori arvates ei saa mugavus aga kuidagi üles kaaluda inimeste

[229] EK *Tele2 Sverige*, kohtujuristi ettepanek, p 199
[230] *Ibid*, p 205
[231] L. Drewry (viide 109), lk 752
[232] *Ibid*, lk 753
[233] L. M. Woods. Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson. – EU Law Analysis, 21.12.2016. Arvutivõrgus kättesaadav: http://eulawanalysis.blogspot.com.ee/2016/12/data-retention-and-national-law-ecj.html (09.04.2017)

põhiõiguseid ning seetõttu ei saa ka nõustuda kriitikaga, et andmete masskogumine on kuritegude uurimiseks ja avastamiseks ainus võimalik lahendus, millele pole mõistlikke ja tõhusaid alternatiive.

Masskogumise keelustamise kriitikud on toonud ka välja, et selle mõjul on vaid sümboolne iseloom:[234] kuna e-privaatsuse direktiivi art 6 lõigete 2 ja 3 kohaselt võivad sideettevõtjad kasutajate sideandmeid säilitada ja töödelda nii kaua kui on vajalik arvelduste eesmärgil ning kasutaja nõusolekul ka turunduse jm lisateenuste osutamise eesmärgil. See tähendab, et sideettevõtjad säilitavad kasutajate andmeid ka ilma vastava seadusest tuleneva kohustuseta.[235]

Tele2 Sverige lahendist nähtub lisaks, et EK siiski eristab terrorismiohtu kui teistest erandlikumat ja kaalukamat olukorda. Seisukohale, et kuritegevuse vastu võitlemise eesmärgil tohib tagada juurdepääsu ainult nende isikute andmetele, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või eelnevas toimepanemises või niisuguse kuriteoga ühel või teisel viisil seotud olemises, lisab EK, et teatavatel erijuhtudel, näiteks terroriohu korral, võib juurdepääsu anda ka muude isikute andmetele, kui esineb objektiivseid asjaolusid, mis võimaldavad järeldada, et need andmed võimaldavad konkreetsel juhul tulemuslikult kaasa terrorismivastasele võitlusele.[236] Seega ei pea terrorismivastase võitluse korral isikute ring, kelle andmetele juurdepääs on lubatud, olema piiratud vaid konkreetses kuriteos kahtlustatavate isikutega nagu see peab olema muude raskete kuritegude puhul.[237]

3.2.3. Digital Rights Ireland lahendis toodud nõuete imperatiivsus siseriiklike regulatsioonide suhtes

EK jätkab *Tele2 Sverige* lahendis oma argumentatsiooni tuues välja, et igasugune sideandmete kogumine ja säilitamine on õiguspärane vaid juhul, kui liikmesriigid näevad ette piirangud säilitatavate andmete liigile, asjassepuutuvatele sidevahenditele ja isikutele ning säilitamise kestusele. Liikmesriigi õigusnormid peavad selgelt ja

[234] M. – P. Granger (viide 113), lk 849
[235] *Ibid*
[236] EKo *Tele2 Sverige*, p 112
[237] U. Lõhmus (viide 197), lk 707

täpselt ette nägema, millistel asjaoludel ja tingimustel võib säilitamise meetmeid rakendada, et isikutel, kelle andmeid säilitatakse, oleksid oma õiguste kaitseks ja andmete kuritarvitamiste vastu piisavad tagatised. Tingimused peavad võimaldama meetme ulatust ja puudutatud isikute ringi tõhusalt piirata ning seos säilitatavate andmete ja taotletava eesmärgi, s.o raske kuriteo ennetamine, uurimine, avastamine ja/või menetlemine, peab rajanema objektiivsetel kriteeriumitel - nt geograafiline piirkond, mille puhul on objektiivsete asjaolude pinnalt tõendatud, et esineb kõrgendatud oht teatud raskete kuritegude ettevalmistamiseks või toimepanemiseks.[238]

Seega andis EK eitava vastuse eespool välja toodud esimesele olulisele eelotsusetaotluse küsimusele (kas üldine kohustus säilitada kuritegevuse vastu võitlemise eesmärgil sideandmeid, mis hõlmab eranditult ja ilma igasuguste piiranguteta kõiki isikuid, kõiki seadmeid ja kõiki andmeid, on lubatud) ning samal ajal vastas teatud ulatuses ka teisele küsimusele (kas lahendis *Digital Rights Ireland* nimetatud tagatised on liikmesriigi õiguse suhtes imperatiivsed nõuded). Nimelt on üks *Digital Rights Ireland* lahendis toodud nn miinimumtagatistest kogutavate andmete ulatuse piiritlemise nõue – väites, et kõikide sideandmete üldine ja piiritlemata kogumise ja säilitamise kohustus ei ole lubatud, ütleb EK, et eelnimetatud miinimumtagatis on tõepoolest liikmesriikide õiguse suhtes imperatiivne nõue.

EK andis *Tele2 Sverige* lahendi viimases osas seisukoha ka teiste *Digital Rights Ireland* lahendis toodud nn miinimumtagatiste imperatiivsuse osas. Säilitatud andmetele juurdepääsu osas rõhutab EK vajadust õigusnormidega ette näha materiaal- ja menetlusõiguslikud tingimused, mille esinemisel saavad pädevad ametiasutused säilitatud sideandmetele ligipääsu. Andmetele juurdepääs tohib samuti toimuda vaid rangelt e-privaatsuse direktiivi art 15 lõikes 1 toodud eesmärkidel, s.t andmesubjekt peab objektiivsetel asjaoludel olema seotud raske kuritegevusega. Eelnimetatud tingimuste täitmist praktikas saab EK hinnangul järgida vaid juhul, kui andmetele juurdepääs on allutatud kohtu vm sõltumatu haldusasutuse eelkontrollile.[239] Sellega loeb EK imperatiivseks veel kaks *Digital Rights Ireland* lahendis toodud

[238] EKo *Tele2 Sverige*, p 108-111. Vt ka U. Lõhmus (viide 197), lk 705-706
[239] *Ibid*, p 115-120

miinimumtagatist: tingimuste sätestamine andmetele juurdepääsuks ja vajadus eelkontrolliks.

Digital Rights Ireland lahendis toodud nõude säilitatavate andmete kaitse tagamise ning andmete hävitamise osas viitab EK küll vajadusele võtta säilitatud andmete kuritarvitamise ohu vältimiseks tarvitusele vajalikud tehnilised ja korralduslikud meetmed ning peale säilitamistähtaja lõppu hävitada andmed pöördumatult, kuid imperatiivseks peab EK selgesõnaliselt eelkõige vaid kohustust säilitada andmeid Euroopa Liidu territooriumil.[240] Lisaks turvalisuse ja hävitamisnõuetele mainib EK ilma selle imperatiivsusele rõhumata ära ka nõude andmesubjekti andmetele juurdepääsust teavitamise kohta (teavitamine võimaldab puudutatud isikutel oma õiguste rikkumise korral kasutada e-privaatsuse direktiivi art 15 lõikes 2 nimetatud õiguskaitsevahendeid) ning nõude tagada sõltumatu järelvalveasutuse kontroll isikuandmete töötlemise üle (nagu seda nõuab põhiõiguste harta art 8 lõige 3).[241]

Tegelikkuses ei andnud EK *Tele2 Sverige* lahendis siiski selget vastust küsimusele, kas lahendis *Digital Rights Ireland* on sedastatud imperatiivsed nõuded, mida liikmesriikide õigus peab järgima. Nagu eespool mainitud, saab *Tele2 Sverige* lahendis välja lugeda, et EK peab imperatiivseteks a) nõuet piirata kogutavate andmete ulatust, b) nõuet seada andmetele juurdepääsu eelduseks kohtulik eelkontroll ning c) nõuet säilitada andmeid liidu territooriumil. Muude *Digital Rights Ireland* lahendis toodud tagatiste imperatiivsuse osas EK selget hinnangut ei anna. Näiteks ei käsitleta *Tele2 Sverige* lahendis üldse andmete säilitamisperioodi ajalist kestvust ning vajadust sisustada konkreetselt "raske kuriteo" mõiste. Nõudeid andmete kaitse ja turbe ning pöördumatult hävitamise, samuti andmesubjekti andmete kasutamisest teavitamise ning andmete töötlemise üle sõltumatu järelvalveasutuse kontrolli tagamise osas EK küll mainib, kuid mitte kontekstis, et nende tingimuste puudumisel tuleb õigusnormid lugeda e-privaatsususe direktiivi ning põhiõiguste hartaga automaatselt vastuolus olevateks. Autor aga leiab, et olgugi et EK osade nõuete imperatiivsust selgelt ei rõhuta, tähendab nende praktikas korduv käsitlemine siiski seda, et tegemist on proportsionaalsuse testi oluliste komponentidega, mis kuuluvad

[240] *Ibid*, p-d 122, 125
[241] *Ibid*, p-d 121, 123

meetmete hindamise nn kontrollskeemi.

3.2.4. *Digital Rights Ireland* lahendi kitsaskohad jäävad

Tele2 Sverige lahendis jääb EK eelnevalt *Digital Rights Ireland* lahendis toodud seisukoha juurde, mille kohaselt sideandmete kogumine ja kasutamine julgeoleku huvides ei kahjusta põhiõiguste harta artiklites 7 ja 8 nimetatud põhiõiguste peamist olemust.[242] See seisukoht jääb autorile jätkuvalt arusaamatuks, eriti kuna EK peab sideandmeid sama tundlikuks kui sideseansi sisu ning nende säilitamiseks ja kasutamiseks rakendatavaid meetmeid põhiõiguste harta artiklites 7 ja 8 nimetatud õigusi ulatuslikult ja raskelt riivavateks.[243]

EK ei täpsusta ei *Digital Rights Ireland* ega *Tele2 Sverige* lahendis, miks ta sellisele arvamusele on jõudnud.[244] Loogika, kus EK ühelt poolt hindab privaatsusõigust kõrgelt ning on asunud seda sideandmete kaitse saaga raames järjepidevalt tunnustama ja teiselt poolt väidab, et sideandmete kogumine ja kasutamine ei kahjusta privaatsusõiguse ja isikuandmete kaitse põhiiseloomu, jääb autorile arusaamatuks ega tundu kuigi veenev.

Lisaks vastandlikele arutluskäikudele õiguste peamise olemuse üle, jätab EK *Tele2 Sverige* lahendis jällegi eraldi käsitlemata põhiõiguste harta artiklid 7 ja 8. Taaskord on EK analüüsinud nimetatud õiguseid sisuliselt ühe nn hübriidõigusena ilma nende sisu ja ulatuse selge eristamiseta. Ka põhiõiguste harta artiklis 11 nimetatud sõnavabaduse puhul piirdus EK pelgalt nimetatud õiguse käesolevas kontekstis äramainimisega.[245] Huvitav oleks olnud lugeda EK argumentatsiooni teemal, kuidas sideandmete säilitamise režiimid omavad mõju sellise olulise põhiõiguse, nagu seda on sõnavabadus, elluviimisele ning kuidas tuleks kaaluda omavahel sõnavabadust ja üldist huvi riikliku julgeoleku tagamise vastu.

---

[242] EKo *Tele2 Sverige,* p 101; EKo *Digital Rights Ireland*, p 39-40
[243] EKo *Tele2 Sverige,* p 99-100
[244] Vt ka M. White. A Threat to Human Rights? The new e-Privacy Regulation and some thoughts on Tele2 and Watson. – EU Law Analysis, 10.01.2017. Arvutivõrgus kättesaadav: http://eulawanalysis.blogspot.com.ee/2017/01/a-threat-to-human-rights-new-e-privacy.html (09.04.2017)
[245] EKo *Tele2 Sverige*, p 92-93, 101. Vt ka L. M. Woods (viide 233)

Kokkuvõtvalt seisneb *Tele2 Sverige* lahendi olulisus käesoleva töö kontekstis *Digital Rights Ireland* lahendi seisukohtade siduvuse kinnitamises – *Digital Rights Ireland* lahendis kasutatud proportsionaalsuse hindamise nn kontrollskeemi rakendab EK ka *Tele2 Sverige* lahendis (viidates seejuures ka asjakohasele EIK prakikale) – ning seisukohas, et sideandmete kogumine ja kasutamine moodustavad komplekti, mis langeb täielikult Euroopa Liidu õiguse kohaldamisalasse ning mida tuleb kontrollskeemi järgi analüüsida tervikuna.

3.3. Uute seisukohtadega kaasnevad muutused

Nagu eespool kirjutatust saab järeldada on *Tele2 Sverige* lahend oluline edasiarendus *Digital Rights Ireland* lahendist, kuna annab selge tauniva hinnangu liikmesriikidesisestele õigusnormidele, mis kohustavad üldiselt kõikide kasutajate sideandmeid säilitada ning lubavad neid andmeid ametiasutustel kasutada peale raske kuritegevuse vastu võitlemise ka muudeks eesmärkideks. Sisuliselt peaksid liikmesriigid, kus taolised reeglid kasutusel on, need kiiremas korras üle vaatama ning vajadusel Euroopa Liidu õigusega kooskõlla viima.

Rootsi ja Ühendkuningriigi kohtud saavad siseriiklike normide õiguspärasuse osas oma seisukohad anda üsna ruttu, kuna *Tele2 Sverige* lahend oli neis riikides juba pooleliolevate kohtumentluste raames esitatud eelotsusetaotluste tulem. Ühendkuningriik on antud juhul muidugi võrreldes teiste Euroopa Liidu liikmesriikidega erinevas olukorras, kuna eesootav väljaastumine Euroopa Liidust (*Brexit*) tähendab suure tõenäosusega lahtiütlemist Euroopa Liidu õiguse ning EK alluvusest. See tähendab, et tulevikus ei pruugi EK praktika ning liidu õiguse muudatused Ühendkuningriigile ja selle kodanikele enam midagi tähendada. Põhiõiguste kaitsmiseks jääb Ühendkuningriigi kodanikele siiski võimalus EIÕK-le tuginedes pöörduda EIK-sse. Nn "sideandmete säilitamise saaga" kontekstis tunduvad EIK ja EK olevat aga sarnastel arusaamadel.

Tele2 Sverige lahend on väga oluline ka Eestile. Olgu öeldud, et Rootsi vastavasisulised õigusnormid, mille EK tunnistas sisuliselt Euroopa Liidu õigusega

vastuolus olevateks, on Eestis kehtivatest normidest oluliselt rangemad: Rootsis kohustuvad sideettevõtjad sideandmeid säilitama kuus kuud (võrdluseks: Eestis on see periood ESS § 111[1] lg 4 kohaselt üks aasta) ning ka juurdepääs neile andmetele on Rootsis piiratum.[246] Eesti kehtiva õiguse kohaselt teostatakse sideandmete säilitamist üldiselt kõikide kasutajate ja kõikide andmeliikide osas ning säilitatud andmetele juurdepääs ei ole piiratud vaid raskete kuritegude ennetamise, uurimise, avastamise ja menetlemisega. Eesti õigus läheb suisa EK seatud tingimustest nii kaugele, et peale kuritegevuse vastase võitluse võib meil sideandmeid kasutada ka nt tsiviilkohtumenetluses[247], keskkonnaalastes väärteomenetlustes[248], eespool kirjeldatud kindlustusjuhtumite lahendamises ning turvateenuse osutamiseks vajaliku tegevusloa taotlemisel.[249]

Õiguskantsler, kes *Digital Rights Ireland* lahendi järgselt asus seisukohale, et Eestis kehtivad õigusnormid on põhiseaduspärased, peaks nüüd *Tele2 Sverige* lahendi valguses oma seisukohad üle vaatama ning teostama uue analüüsi Euroopa Liidu õiguse ning sellest tuleneva proportsionaalsuse testi valguses. EK on selgelt öelnud, et nii andmete säilitamine kui nende hilisem kasutamine langevad liidu õiguse kohaldamisalasse.[250] See tähendab, et nii andmete säilitamist kui nendele juurdepääsu võimaldavad riigisiseseid norme tuleb vaadelda ühe tervikuna ning nende vastavust tuleb hinnata Euroopa Liidu õiguse, mitte riigi põhiseaduse suhtes.[251] Õiguskantsleri seletused, mille kohaselt võib meie normide rakendamises küll esineda probleeme, kuid normid ise on igati Eesti ja Euroopa Liidu õigusruumi sobivad, ei ole piisavad: EK on *Tele2 Sverige* lahendiga öelnud põhjapanevalt, et siseriiklikud õigusnormid, mis näevad kuritegevusega võitlemise eesmärgil ette üldise ja vahet tegemata kohustuse kõikide kasutajate sideandmete säilitamiseks, s.t sellised normid nagu kehtivad Eestis, on e-privaatsuse direktiivi ja põhiõiguste hartaga vastuolus. Euroopa

[246] U. Lõhmus (viide 197), lk 703-704
[247] ESS § 111[1] lg 11 p 5
[248] ESS § 111[1] lg 11 p 3
[249] ESS § 111[1] lg 11 p 6, TurvaS § 46[1]
[250] Vt EKo *Tele2 Sverige*, p 68-81
[251] U. Lõhmus (viide 197), lk 704

Liidu õiguse ülimuslikkuse põhimõtte[252] kohaselt ei ole Eestil võimalik sellest tõlgendusest mööda vaadata.

Järgnevas alapunktis on toodud EK ja EIK poolt kehtestatud kontrollskeemi elemendid ning nende valguses on käsitletud puudujääke Eesti õiguses.

3.4. Kontrollskeemi elemendid ning puudujäägid Eesti õiguses

Järgnevalt toob autor eespool käsitletud kohtupraktikast tuletatava proportsionaalsuse hindamise kontrollskeemi elemendid ning Eesti õiguses esinevad puudujäägid, millele tuleks kontrollskeemi valguses enim tähelepanu pöörata.

a) andmete eristamine ja piiritlemine

Eespool analüüsitud kohtupraktikas on viidatud, et oluline on eristada säilitatavate andmete liike ning piirata nende kogumise ulatust. Seejuures tuleb piiritlemisel lähtuda objektiivsetest kriteeriumitest, et inimestel oleks võimalik aru saada, millises olukorras nende sideandmete säilitamise meetmeid rakendada on lubatud. Vajadust andmete ulatust ning subjektide ringi võimalikult kitsalt piiritleda on seejuures rõhutanud ka õiguskantsler.[253]

Hetkel kehtib Eestis säilitamiskohustus eranditult kõikide sideandmete ja kasutajate osas.[254] Autori arvates oleks mõistlik jagada andmed nn tundlikkuse astme järgi erinevatesse gruppidesse, nt eristada üksteisest 1) kõneandmeid (helistaja ja vastuvõtja number, kõne kuupäev ja kellaaeg ning ajaline kestus), 2) asukohaandmeid (helistaja ja vastuvõtja geograafiline asukoht) ning 3) IP-aadresse. Ilmselgelt on kõne- ja asukohainfo privaatsusõiguse seisukohalt vaadatuna oluliselt tundlikuma sisuga kui

[252] Euroopa Liidu õiguse ülimuslikkuse põhimõte tuleneb EK praktikast (EKo 15.07.1964, C-6/64, *Costa v ENEL*) ning selle kohaselt tuleb Euroopa Liidu õigusega vastuolu korral siseriiklik õigusnorm kohaldamata jätta. Euroopa Liidu õiguse ülimuslikkuse põhimõtet on korduvalt tunnustanud ka Riigikohus, vt RKHKo 19.04.2005, 3-4-1-1-05; RKHKo 5.10.2006, 3-3-1-33-06; RKHKo 7.05.2008, 3-3-1-85-07; RKHKo 26.06.2008, 3-4-1-5-08
[253] Õiguskantsleri 22.04.2016 seisukoht (viide 21)
[254] ESS § 111^1 lg 1-3

IP-aadress[255] – seega saab erinevate andmegruppide suhtes rakendada ka erineva rangusega säilitamise ja juurdepääsu tingimusi.

Kogutavaid andmeid saab piiritleda ka isikuliselt – eristada tuleks andmesubjekte, kes 1) on raske kuriteoga seotud otseselt (nt kahtlustatav), 2) on raske kuriteoga seotud kaudselt (nt kaasaaitaja, kahtlustatava lähikondlane) või 3) võivad muul viisil kaasa aidata kuritegude vastu võitlemisele. Taaskord saab erinevate gruppide suhtes rakendada erineva rangusega tingimusi – nt peaks isiku, kes pole raske kuritegevusega otseselt või kaudselt seotud, kuid kes võib kuritegevuse vastu võitlemisele kaasa aidata "muul põhjusel", andmete säilitamise või kasutamise vajaduse hindamisel rakendama suuremat põhjendamiskohustust kui isiku puhul, kes on juba raske kuriteo toimepanemises kahtlustatav. Lisaks isikulisele piirangule on seadusandjal võimalik andmete kogumist piirata ka geograafiliste, ajaliste vm tunnuste abil – nt kogutakse andmeid kindlast ajavahemikust ja/või geograafilisest piirkonnast, kus esineb kõrgendatud oht raskete kuritegude ettevalmistamiseks või toimepanemiseks.[256]

b) seos raskete kuritegudega

EK on pidanud eriti oluliseks, et selline ulatuslik põhiõiguste riive nagu seda on sideandmete säilitamine ja kasutamine oleks põhjendatud vaid raskete kuritegude uurimise, avastamise ja menetlemisega. "Raske kuriteo" mõiste sisu EK sideandmete kaitse teemalistes lahendites aga ei eriti täpsusta. *Digital Rights Ireland* lahendis nimetab EK rasketeks kuritegudeks eeskätt organiseeritud kuritegevuse ja terrorismi.[257] Lisaks on EK oma varasemas praktikas toonud välja, et põhiõiguste harta art 52 lõikes 1 nimetatud "üldist huvi" pakkuvate eesmärkide hulka kuulub mh rahvusvaheline terrorismivastane võitlus rahvusvahelise rahu ja julgeoleku säilitamiseks.[258]

[255] EK hiljutine lahend C-582/14, *Breyer* käsitleb IP-aadresse samuti isikuandmetena. Vt ka M. Kotula. IP addresses as personal data - the CJEU's judgment in C-582/14 Breyer. – EU Law Analysis, 04.01.2017. Arvutivõrgus kättesaadav: http://eulawanalysis.blogspot.com.ee/2017/01/ip-addresses-as-personal-data-cjeus.html (09.04.2017)
[256] EKo *Tele2 Sverige*, p-d 106 ja 111
[257] EKo *Digital Rights Ireland*, p 51
[258] Vt EKo 3.09.2008, C-402/05 P ja C-415/05 P, *Kadi ja Al Barakaat International Foundation vs.*

EIK on seevastu oma lahendites *Kennedy* v Ühendkuningriik[259] ja *Zakharov* avaldanud seisukohta, et võitlusel selliste kuritegude vastu, mille puhul on inimeste privaatsusesse sekkumine EIÕK art 8 alusel õigustatud, ei pea õigusaktis tooma välja ammendavat nimekirja konkreetsetest kuritegudest, mille puhul privaatsust riivavaid meetmeid kasutada võib. Piisab, kui õigusaktis on kuritegude olemust ja iseloomu avatud selliselt, et inimestel on võimalik aru saada, millises olukorras on alust nende suhtes erinevaid meetmeid rakendada.[260] Lahendis *Klass* käsitles EIK taolist laadi kuriteogudena näiteks spionaaži ja terrorismi.[261]

Kirjanduses on "raske kuriteona" käsitletud eelkõige terrorismi, organiseeritud kuritegevust, narkokaubandust ning ulatuslikku finants- vm majandusalast kelmust (ingl. k *serious fraud*). [262] Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsiooni[263] artiklis 2 on raske kuriteona defineeritud kuritegu, mille eest on karistuseks ette nähtud vähemalt neli aastat vangistust või muu range karistus.

Autori hinnangul ei saa "raske kuriteo" mõiste alla kuidagi kvalifitseeruda Eesti õiguse järgi väärteoks ja teise astme kuriteoks lahterduvad süüteod[264] ja kohe kindlasti mitte eraõiguslikud vaidlused, kindlustusjuhtumid või riikliku järelvalve- ja taustakontrollimeetmed.[265] Vaieldav on, kas "raskeks kuriteoks" saab nimetada kõiki esimese astme kuritegusidki. Seadusandja peaks siinkohal kriitiliselt hindama, milliseid esimese astme kuritegusid EK poolt väljaöeldud "raske kuriteo" mõiste alla

---

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*

[259] EIKo 18.05.2010, 26839/05*, Kennedy vs United Kingdom*

[260] *Ibid*, p 159; EIKo *Zakharov*, p 244. Kennedy kohtuasjas aktsepteeris EIK Ühendkuningriigi õiguses toodud "raske kuriteo" defineeritsiooni – süütegu, mille eest vähemalt 21-aastast inimest, kellel puuduvad eelnevad karistused, võiks süüdimõistmise korral oodata vähemalt 3 aasta pikkune vanglakaristus.

[261] EIKo *Klass and Others*, p 48

[262] Vt A. Ashworth. Human Rights, Serious Crime and Criminal Procedure. – The Hamlin Lectures. London: Sweet and Maxwell, 2002. Arvutivõrgus kättesaadav: https://socialsciences.exeter.ac.uk/media/universityofexeter/schoolofhumanitiesandsocialsciences/law/pdfs/Human_Rights_Serious_Crime_and_Criminal_Procedure.pdf (22.04.2017)

[263] Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsioon. - RT II 2003, 1, 1

[264] Süütegude liigid ja raskusastmed on toodud KarS §§ 3-4

[265] Vt ka P. Schasmin (viide 23), alapunkt 3.1

paigutada. Mõistlik oleks lähtuda sellest, et mida suuremat ohtu kujutab kuritegu riiklikule julgeolekule, seda rohkem on põhiõiguseid riivavate meetmete rakendamine õigustatud. Autori seisukoht on, et varavastane esimese astme kuritegu (nt röövimine[266]) ei ole inimeste põhiõiguste riive õigustusena sama kaalukas kui inimsuse- või riigivastased esimese astme kuriteod (nt genotsiid,[267] terrorism[268]).

c) säilitamisperioodi eristamine ja piiritlemine

Kohtupraktikas rõhutakse järjepidevalt vajadusele piiritleda andmete säilitamist selliselt, et andmeid säilitataks vaid niikaua, kuni see on eesmärgist lähtuvalt vältimatult vajalik. Eestis kehtiv regulatsioon kohustab sideandmeid säilitama ühe aasta ning valitsusel on õigus "avaliku korra ja riigi julgeoleku huvides" seda tähtaega "piiratud ajavahemikuks" pikendada.[269]

Üheaastane kohustuslik säilitamisperiood on autori hinnangul ebaproportsionaalselt pikk.[270] Andmete säilitamise on õigustatud vaid nii kaua, kuni see on eesmärgi, milleks on raskete kuritegude avastamine, uurimine ja menetlemine, puhuks vajalik. See tähendab, et iga juhtumi puhul tuleks säilitamisperioodi üle eraldi otsustada. Ka tähtaja pikendamise võimalused ja ulatus peaks olema võimalikult piiritletud – nt võiks pikendamise aluseks olevad objektiivsed asjaolud olla kõrgendatud terrorioht, massirahutused, organiseeritud kuritegevuse uurimise pikaajalisus, kuritegevuse laine teatud piirkonnas jne.

Võimalus on ka eristada säilitamisperioode andmete liikide kaupa – näiteks on IP-aadresside, mis on teatud kuritegude (küberkuritegevus) puhul väga olulise tähtsusega tõendiks, kuid ei ole seejuures oma olemuselt sama tundliku eraelulise loomuga kui asukohaandmed, puhul põhjendatud pikem säilitamisperiood kui asukohaandmete puhul.[271]

[266] KarS § 200
[267] KarS § 90
[268] KarS § 237
[269] ESS § 111^1 lõiked 4 ja 6
[270] Võrdluseks - Riigikohus nii ei arva, vt RKKKo 3-1-1-51-14, p 22.3.
[271] L. Drewry (viide 109), lk 749

Oluline on ka täpsustada nende andmete, millele on juba juurdepääs taotletud, säilitamisperioodi kestust. Ametiasutus, kes on sideettevõtjalt andmed välja nõudnud, võib kehtiva korra alusel neid andmeid omakorda säilitada veel 2 aastat.[272] Taaskord on selline üldistus ebamõistlik ega piirdu vältimatult vajalikuga. Kaheaastane tähtaeg võib olla põhjendatud vaid olukorras, kus kriminaalmenetluse läbiviimine võtab aega mitu aastat.[273]

d) säilitatud andmete kaitse kuritarvitamiste eest

Selleks, et andmesubjektide põhiõigused oleks säilitamisperioodi jooksul tõhusalt tagatud, tuleks EK hinnangul rakendada tehnilisi ja korralduslikke meetmeid, mis võimaldaks tagada säilitatavate andmete tõhusa kaitsmise kuritarvituste ohu eest ning ebaseadusliku juurdepääsu eest.

Kõige lihtsam on andmete turvalisuse tagamist alustada hoopis nn füüsiliste abinõude kaudu – serverid, kus säilitatud andmeid hoitakse, peaksid olema kaitstud väliskeskkonna mõjude (nt tulekahju, veeuputus, lõhkumine) ning õigustamatu ligipääsu eest. Teiseks saab rakendada EK poolt viidatud tehnilisi abinõusid – nt teha süsteemid nn häkkimiskindlaks, tagada juurdepääs vaid kindlatele parooli ja/või ID-tunnuse abil identifitseeritavatele kasutajatele, säilitatatavad andmed krüpteerida. Korralduslike abinõudena tuleks rakendada eeskirjad, mida sideettevõtjad ja nende töötajad peavad silmas pidama – nt kellel ja millistel tingimustel on andmetele ligipääs, millised on volituste ületamise tagajärjed, kuidas kuritarvitamisega seotud riske juhtida jne.[274] ESS § 111^1 lg 9 küll seab sideettevõtjatele üldise kohustuse andmete turvalisuse tagamiseks, kuid selguse huvides oleks neid nõudeid õigusaktides siiski täpsustada, et kõik sideettevõtjad saaksid reeglitest ühtemoodi aru.

Lisaks sideettevõtjatele peaksid neidsamu nõudeid järgima ka õiguskaitseorganid, kelle valdusesse nimetatud andmed on jõudnud. Kehtivas õiguses ei ole õiguskaitseorganitele andmete turvalisuse tagamise osas ühtegi kohustust seatud. Kuna eespool mainitud nõuete olemasolu peaks aitama tagada andmesubjektide

[272] ESS § 111^1 lõiked 4 ja 6
[273] P. Schasmin (viide 23), lk 58
[274] Vt ka L. Drewry (viide 109), lk 745-748

õiguste kaitse ning ära hoida andmete kuritarvitamisi, siis on nõuete seadmine õiguskaitseorganitele, kes on riikliku sunnivõimu esindajad ning omavad oma ametist tulenevalt väga laialdasi õigusi, eriti olulise tähtsusega.

Andmete säilitamise puhul on veel oluline jälgida EK poolt seatud nõuet säilitada andmeid Euroopa Liidu territooriumil. Selline nõue tagab, et andmete töötlemisele kohalduvad Euroopa Liidu poolt kehtestatud andmekaitsereeglid ning see allub Euroopa Liidu poolsele järelevalvele. Eesti kehtivas õiguses on see nõue täidetud.[275]

e) kohtulik eelkontroll

Selleks, et tagada andmete kogumine ning juba säilitatud andmete kasutamine tõepoolest vaid raskete kuritegude uurimiseks, avastamiseks ja/või menetlemisest, on kohtupraktika kohaselt esmavajalik, et see saaks toimuda vaid kohtu vm sõltumatu haldusasutuse eelneval loal. Andmete kogumist teostatakse või juurdepääs tagatakse vaid juhul, kui see on vältimatult vajalik.

Autori hinnangul ei ole peale kohtu Eestis praegusel hetkel muid "sõltumatuid halduasutusi", mis suudaksid adekvaatselt hinnata andmete kogumise või neile juurdepääsu vältimatut vajalikkust, s.t kaaluda ühelt poolt andmesubjekti õigust privaatsusele ja andmete kaitsele teiselt poolt kuritegevusevastase võitluse ja riikliku julgeoleku huvidega. Siiski ei ole välistatud ka uue sõltumatu haldusinstantsi loomine – nt võiks AKI, Riigikontrolli või õiguskantsleri juures tegutseda eraldi põhiõiguste riive ja kaitse hindamisega tegelev komisjon.

EIK on toonud välja, et eelnev (*ex ante*) luba ei ole ilmtingimata vajalik, kui on olemas tugev kohtulik järelkontroll, mis võib heastada algse loa puudumise puudujääke.[276] Samas on meetme rakendamisele eelnev huvide kaalumine ning meetme vajalikkuse hindamine inimeste õiguste kaitse seisukohast vaadatuna tõenäoliselt kõige tõhusam tagatis. Nagu eespool öeldud, on taolise hindamise teostamiseks pädevaks asutuseks eelkõige kohus. Prokuratuur kui menetluses asjast

[275] ESS § 111[1] lg 5
[276] EIKo *Szabo and Vissy*, p 77; EIKo *Kennedy*, p 167. Vt ka P. Schasmin ja C. Ginter (viide 24), lk 48

huvitatud osapool (juhib kuriteo uurimist ning on eelkõige huvitatud võimalikult suurest hulgast informatsioonist) ei saa kuidagi loa andmisel olla sõltumatu ning seetõttu ei ole ka prokuratuuri luba tõhus meede inimeste õiguste kaitsmisel.[277]

Andmete kogumist või neile juurdepääasu taotlev asutus (eelkõige prokuratuur) peab kohtule esitama kindlatele vorminõuetele vastava taotluse, sh tõendid ja põhjendused, milliste konkreetsete isikute, andmeteliikide ja ajaliste perioodide osas andmete kogumist või juurdepääsu soovitakse. Kui kohus leiab, et kogumine või juurdepääs on õigustatud, s.t see on raske kuritegevuse vastases võitluses välitmatult vajalik, annab ta kindlatele vorminõuetele vastava määrusega kas ametiasutusele loa andmetele juurdepääsuks või paneb sideettevõtjale kohustuse andmete säilitamiseks. Määrus peaks olema kohtu poolt põhistatud ning sisaldama konkreetseid viiteid andmesubjektile, andmete liigile ning ajalisele perioodile, mille osas kogumine või juurdepääs võimaldatakse. Vorminõuete olemasolu, s.t kindlate elementide käsitlemine taotluse esitamisel ja loa andmisel, aitab muu hulgas tagada seda, et järgitakse põhjendamiskohustust – see paneb esmalt taotluse esitaja ja/või loa andja põhjalikumalt läbi mõtlema päringu ja/või loa andmise vajaduse, ning teisalt võimaldab see hiljem teostada järelkontrolli, kas päringu tegemine oli konkreetsel juhul tõepoolest vajalik ja/või loa andmine õigustatud.[278]

Võimalik on ka anda kohtule pädevus sõltuvalt asjaoludest ning potentsiaalse riive ulatusest määrata täiendavaid tingimusi soovitava meetme osas – nt lubatakse määrusega kogutud andmeid säilitada väga piiratud ajaperioodil või võimaldatakse andmetele juurdepääsu vaid ühel konkreetsel ametnikul või piiratud ametnike ringil.[279] Seaduses peab seejuures sätestama kohtu kaalutlusõiguse piirid, sh nt kuidas määrata meetme rakendamise ajavahemikku, juurdepääsevate isikute ringi jne.[280] Nõue, mille kohaselt peab juurdepääs andmetele olema allutatud kohtu või sõltumatu haldusasutuse eelnevale kontrollile, nõuab paratamatult uute menetluste ja pädevuste kehtestamist.[281]

[277] Hetkel kehtivas õiguses toodud nn eelkontrolli kohta vt täpsemalt P. Schasmin (viide 23), lk 63-66; P. Schasmin ja C. Ginter (viide 24), lk 48-49
[278] P. Schasmin ja C. Ginter (viide 24), lk 48
[279] L. Drewry (viide 109), lk 751
[280] P. Schasmin (viide 23), lk 59
[281] P. Schasmin ja C. Ginter (viide 24), lk 52

EK aktsepteerib, et teatud "kiireloomulistel juhtudel" võib kohtuliku eelkontrolli nõudest ka n-ö mööda minna. Sellisteks juhtudeks saavad olla olukorrad, kus andmeid on vaja koguda/kasutada koheselt ning tegutsematajätmine kujutab endas eriti suurt ohtu riiklikule julgeolekule – nt kui julgeolekuasutus on saanud info lähiajal toimuva terrorirünnaku kohta. Mõistlik oleks rakendada analoogset reeglit nagu on toodud KrMS § 126^4 lõikes 3^{282} – meedet võib rakendada kohtu kirjalikku taasesitamist võimaldavas vormis loa alusel ning kirjalik taotlus ning põhistatud luba vormistatakse 24 tunni jooksul.

f) juurdepääsuõiguste piiramine

Nagu eespool käsitletud, peaks kohtupraktika kohaselt andmete kogumine toimuma eristaval meetodil, mitte üldiselt kõikide kasutajate suhtes. Eristamine peaks toimuma teatud objektiivsete kriteeriumite alusel – nt on isik otseses seoses raske kuriteoga või on tema geograafilises asukohas kõrgendatud risk raske kuriteo toimepanemiseks.

Analoogselt peaks kohtuprakika kohaselt toimuma ka säilitatud andmetele ligipääs – ligipääsu taotlev ametiasutus toob meetme rakendamise üle otsustavale kohtule välja ligipääsuks vajalikud objektiivsed kriteeriumid ning esitama kõik asjakohased tõendid. Hetkel on kehtivas õigsuses mitmetel juhtudel jäetud määratlemata, milliste isikute kohta täpsemalt võib andmeid sideettevõtjatelt küsida.[283]

Juurdepääsuõiguse saamiseks saaks objektiivseteks kriteeriumiteks olla nt a) isiku seos raske kuriteoga (nt isik on kahtlustatav raske kuriteo toimepanemises, tõendiks on sündmuspaigalt leitud sõrmejälg, tunnistajate ütlused vmt), b) säilitatud andmed võivad olla oluliseks tõendiks või aidata muul viisil oluliselt kaasa kuriteo uurimisele, avastamisele, menetlemisele (nt asukohainfo kuriteo asetleidmise hetkel) ning c) ühelgi muul viisil ei ole võimalik tõendeid koguda ja/või kuritegu uurida, avastada menetleda (nt IP-aadress on tihti ainus jälg küberkuritegude puhul).

[282] Säte räägib jälitustoimingu läbiviimisest olukorras, kus on vahetu oht isiku elule, kehalisele puutumatusele, füüsilisele vabadusele või suure väärtusega varalisele hüvele ning loa taotlemine või vormistamine ei ole õigel ajal võimalik.
[283] P. Schasmin (viide 23), lk 57

Oluline on, et juurdepääs piirduks vaid vältimatult vajalikuga, s.t juurdepääs tagatakse vaid konkreetse isiku ja andmeliigi (nt kui on vaja teada isiku asukohta, ei ole vaja pääseda ligi tema kõne- ja IP-andmetele) ning võimalikult kitsa ajalise perioodi osas (nt kuriteole vahetult eelnev/järgnev ajavahemik). Eelistatud on n-ö üksikpäringud, igasuguste massipäringute tegemine ei taga reeglina seda, et andmeid küsitakse üksnes asjas tähtsust omavate faktide kohta ning privaatsusõiguse riive võib olla suurem kui konkreetses asjas vältimatult vajalik.[284] Mida rohkem õnnestub piiritleda ligipääsu objekti ja ulatust, seda rohkem õnnestub kaitsta ka inimeste põhiõiguseid.[285]

Kuna andmete kogumise ja kasutamise eesmärk saab olla vaid raske kuritegevuse vastane võitlus, ei saa andmetele juurdepääsuõigusi omavate asutuste nimekiri olla nii pikk, nagu kehtiv ESS võimaldab. Andmeid peaksid saama kasutada vaid sellised ametiasutused, kelle pädevuses on raskete kuritegude avastamine, uurimine ja/või menetlemine – nt prokuratuur, kohus, Politsei- ja Piirivalveamet, Kaitsepolitseiamet. Ametiasutused, kellel taoline pädevus puudub – nt kindlustusandja, Keskkonnainspektisoon, Andmekaitse Inspektisoon, tsiviilkohus – ei tohi omada võimalust taotleda andmete säilitamist ega saada säilitatud andmetele juurdepääsu.

Lisaks on oluline võimalikult suures ulatuses piirata ka andmetele asutusesiseselt juurdepääsu saavate isikute ringi. Nagu eespool öeldud, on võimalik sätestada juurdepääsuõigused isikuliselt kohtu määruses. Ühtlasi on võimalik õigusnormidega sätestada, et õiguskaitseorganid peavad kehtestama teatud tingimustele vastavad sisekorralduslikud reeglid selle kohta, millistel töötajatel, millistel juhtudel ja millises ulatuses on volitused sideandmetega toimetada.[286]

g) sõltumatu järelvalve

Lisaks kohtulikule eelkontrollile aitab inimeste õiguste kuritarvitamist kohtupraktika kohaselt ära hoida ka sõtumatu tõhus järelkontroll, s.t sõltumatu järelevalve teostamine andmete kogumise, säilitamise ja kasutamise üle. Hetkel Eestis kehtiv

[284] *Ibid*, lk 60
[285] L. Drewry (viide 109), lk 751
[286] Vt ka *ibid*

regulatsioon kohustab sideettevõtjaid säilitama logifaile andmetele ligipääsu päringute ja tehtud toimingute kohta[287] ning korra aastas esitama Tehnilise Järelevalve Ametile (TJA) andmed selle kohta, kui mitu päringut neile sideandmete saamiseks on tehtud.[288] Iseasi on see, milline roll saab olla TJA-l inimeste põhiõiguste kuritarvitamise alases järelevalves.

Oluline roll järelevalves isikuandmete kaitse valdkonnas on Andmekaitse Inspektsioonil (AKI). AKI ülesandeks on sõltumatult hinnata, kas sideandmete säilitamisel ja kasutamisel on kõiki andmekaitsereegleid järgitud või mitte. AKI poole saab pöörduda nii üksikisik (kaebuse, vaide või märgukirjaga) kui ka sideettevõtja juhul kui on toimunud isikuandmetega seotud rikkumine.[289] AKI otsused on sanktsioneeriva iseloomuga: isikuandmete kaitse seaduse 6. peatüki kohaselt on AKI-l õigus esitada ettepanekuid või soovitusi õigusrikkumise lõpetamiseks, teha täitmiseks kohustusliku ettekirjutuse, määrata sunniraha (vajadusel korduvalt), kuni ettekirjutus on täidetud, määrata väärteotrahvi raske rikkumise puhul, ettekirjutuse täitmata jätmisel või järelevalve takistamisel ja taotleda kriminaalasja algatamist.[290] Lisaks AKI-le teostab õiguskantsleri seaduse (ÕKS)[291] § 1 lg 9 kohaselt õiguskantsler järelevalvet inimeste põhiõiguste ja -vabaduste järgimise üle täidesaatva riigivõimu asutuste poolt varjatult isikuandmete ja nendega seonduva teabe kogumise, töötlemise, kasutamise ja järelevalve korraldamisel.

JAS § 36 alusel teostab julgeolekuasutuste üle järelevalvet Riigikogu julgeolekuasutuste järelevalve komisjon. Tasub silmas pidada, et tegemist on poliitilise koguga ja mitte sõltumatu asutusega ning on kaheldav, kas ja mil määral omab nimetatud komisjon ressursse ning pädevust kontrollimaks, kas konkreetsel juhul oli sideandmete säilitamine ja kasutamine vältimatult vajalik meede.[292]

---

[287] ESS § 113 lg 5
[288] ESS § 112[1]
[289] ESS § 102[1] lg 2. Nimetatud kohustus ning selle täitmise kord tuleneb e-privaatsuse direktiivi juurde käivast määrusest nr 611/2013.
[290] A. Lott. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. - Riigikohus: Tartu 2015, lk 35. Arvutivõrgus kättesaadav: http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf (09.04.2017).
[291] RT I, 06.04.2016, 23
[292] Vt ka P. Schasmin (viide 23), lk 66; U. Lõhmus. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. – Juridica 2008/VII, lk 472

h) andmesubjektide teavitamine

Lisaks sõltumatule järelevalvele peavad EIK ja EK väga oluliseks ka andmesubjektide teavitamist nende andmete säilitamisest ja kasutamisest. Sõltumatu eelkontrolli nõue iseenesest vähendab, kuid ei välista kuritarvituste riski ning kuritarvituste ärahoidmine on tõhusam, kui puudutatud isikutele antakse reaalne võimalus ise kontrollida oma andmete kasutamise õiguspärasust.[293] Juhul kui isik on teadlik enda andmete töötlemisest, on tal võimalik oma õiguste kuritarvitamise kahtluse korral pöörduda vastavate instantside (AKI, kohus, õiguskantsler vm) poole ning kasutada seadusega ettenähtud õiguskaitsevahendeid. Seda seisukohta toetab ka Riigikohus, kes on öelnud, et olukorras, kus isik ei ole oma põhiõigusi riivavast (jälitus)toimingust teadlik, on praktiliselt välistatud võimalus kasutada põhiõigust pöörduda oma õiguste kaitseks kohtu poole.[294]

Teavitamise puhul tuleb aga arvestada, et seda meedet ei saa rakendada ühetaoliselt – andmesubjekti teavitamist ei saa toimuda, kui see seaks ohtu menetluse, mille raames andmeid kogutakse ja/või kasutatakse, eesmärgi[295], s.t võib kahjustada võimalusi käimasoleva menetluse käigus kuritegu reaalselt avastada.[296] Tuleb ka arvestada, et isiku teavitamine võib ohustada riiklikku julgeolekut – julgeolekuohu tõttu isiku teavitamata jätmine ei ole EIK praktika kohaselt tingimata EIÕK-ga vastuolus.[297] Ka PS § 44 kohaselt on isikul küll õigus seaduses sätestatud korras tutvuda enda kohta riigiasutustes ja kohaliku omavalitsuse asutuses ning riigi ja kohalike omavalitsuste arhiivides hoitavate andmetega, kuid seda õigust võib piirata mh teiste inimeste õiguste ja vabaduste kaitseks ja kuriteo tõkestamiseks.[298]

Seega ei saa andmesubjekti teavitamine iseenesest olla tõhus järelevalvemeede, küll aga tuleks seda maksimaalses võimalikus ulatuses kindlasti rakendada, kuna see aitab lisameetmena tõhustada inimeste põhiõiguste kaitset õiguskaitsevahendite kasutamise võimaldamise kaudu. Eeskätt tuleks järelevalve valdkonnas siiski rõhuda AKI kui

[293] P. Schasmin ja C. Ginter (viide 24), lk 49
[294] RKPSJKo 3-4-1-42-13, p 49. Vt ka P. Schasmin (viide 23), lk 69
[295] JAS § 29. Vt ka jälitustoimingust teavitamise korda - KrMS § 126^{13}
[296] P. Schasmin ja C. Ginter (viide 24), lk 49
[297] EIKo *Klass*, p 58
[298] A. Lott (viide 290), lk 35

sõltumatu ja pädeva ametiasutuse kontrollile.

i) andmete hävitamine

Kohtupraktikas rõhutatakse ühe vajaliku tagatisena ka säilitatud andmete hävitamist peale säilitamisperioodi lõppu. See tähendab, et nii sideettevõtjad kui ka ametiasutused, kelle valduses sideandmed on, on kohustatud rakendama tehnilisi abinõusid selleks, et andmed pöördumatult hävitada peale seda, kui nende suhtes ettenähtud säilitamistähtaeg saab läbi, s.t andmete säilitamine ei ole enam välitmatult vajalik konkreetse raske kuriteo avastamise, uurimise või menetlemise jaoks.

ESS on täiesti reguleerimata jätnud kohustuse andmed peale säilitamisperioodi lõppu kustutada/hävitada. Seega peaks andmete säilitamisele seatud nõuded kindlasti sisaldama ka kohustust andmed peale säilitamisperioodi lõppu pöördumatult, s.t ilma võimaluseta neid hiljem taastada, hävitada. Asjaolust, kas andmed hävitatakse pärast ettenähtud tähtaega, sõltub suuresti see, kas nende säilitamist ja kasutamist saab pidada proportsionaalseks meetmeks.[299] Andmete hävitamine peale säilitamisperioodi lõppu välistab mh olukorra, kus andmeid kasutatakse hiljem algsest eesmärgil, nt mõne muu menetluse raames. Kuna aga sideandmete säilitamise ja kasutamise vajadust ja mõõdukust hinnatakse juhtumipõhiselt ning selleks annab loa kohus, ei ole nõuetega kooskõlas see, kui andmeid kasutatakse hiljem veel mõnel muul eesmärgil.

Kokkuvõtvalt on sideandmete säilitamise ja kasutamise proportsionaalsuse hindamisel vajalik lähtuda EIK ja EK praktikast tulenevast kontrollskeemist, mille elemendid on: a) andmete eristamine ja piiritlemine; b) seos raskete kuritegudega; c) säilitamisperioodi eristamine ja piiritlemine; d) säilitatud andmete kaitse kuritarvitamiste eest; e) kohtulik eelkontroll; f) juurdepääsuõiguste piiramine; g) sõltumatu järelvalve; h) andmesubjektide teavitamine; i) andmete hävitamine. Autor tuvastas kontrollskeemi aluseks võttes Eesti kehtivas õiguses mitmeid puudujääke. Uue regulatsiooni loomisel tuleks seadusandjal kindlasti eeltoodud kontrollskeemi elementidega arvestada ning lähtuda EIK ja EK seisukohtadest ja tõlgendustest.

[299] P. Schasmin ja C. Ginter (viide 24), lk 50

3.5. Muud juhud, millal kontrollskeemi rakendamine võiks kohalduda

Ei ole välistatud, et kontrollskeem, mille EIK ja EK on loonud hindamaks sideandmete säilitamise ja kasutamise valdkonnas rakendatavate meetmete proportsionaalsust, võiks olla asjakohane ka muudes valdkondades, kus kuritegevusevastase võitluse nimel võetakse tarvitusele inimeste põhiõiguseid riivavaid meetmeid. Ühegi kontrollskeemi elemendi puhul pole tegemist vaid lahutamatult sideandmetega seonduva nõudega. Kirjanduses on käsitletud *Digital Rights Ireland* lahendis toodud standardite mõju andmekogumisele nt lennureiside broneeringute, hotellikülastuste, ja piiriületamiste puhul,[300] eelkõige seetõttu, et rakendatavad meetmed on nendel juhtudel sideandmete säilitamise puhul kasutatavatega väga sarnased. Ka kiiruskaamerate abil kogutavate ja menetletavate andmete osas oleks paslik kasutatavad meetmed eespool toodud kontrollskeemi alusel ära hinnata.

Hetkel on Eestis päevakajaliseks teemaks siseministri soov luua majutusasutuste klientide automaatne register, et aidata jõustruktuuridel võidelda terrorismiga ning tabada tagaotsitavaid või riigis ebaseaduslikult viibivaid isikuid.[301] Vastavateemalises uudises on plaanitavaid meetmeid põgusalt ka kirjeldatud: majutusasutustes ööbima registreeritud isikute info liigub hiljemalt ööpäeva jooksul automaatsesse registrisse, mis kontrollib infot erinevate andmebaaside suhtes, nagu politsei andmekogu, sissesõidukeeldude riiklik register ning Interpoli andmebaas; kui andmebaasidest vasteid ei saada, kustutakse inimese info üldjuhul ööpäeva jooksul, kui aga ilmneb, et tegu on jõustruktuuridele huvipakkuva isikuga, kontrollib infot edasi juba vastav ametnik; majutusasutused ise peavad plaani kohaselt aga inimeste infot hoidma alles kaks aastat, et ametkonnad saaks vajadusel seda hiljem kontrollida.[302] Kirjeldatud meetmed on hirmutavalt sarnased EK poolt kehtetuks tunnistatud andmete säilitamise direktiivis ning kehtivas ESS regulatsioonis ettenähtud meetmetega, mis aga, nagu

[300] Vt F. Boehm (viide 103)
[301] Riik hakkab kontrollima majutusasutuste külastajate tausta. – Postimees, 20.02.2017. Arvutivõrgus kättesaadav: http://www.postimees.ee/4020547/riik-hakkab-kontrollima-majutusasutuste-kulastajate-tausta (24.04.2017)
[302] *Ibid*

eespool käsitletud, ei läbi EIK ja EK poolt kehtestatud kontrollskeemi ning on seega Euroopa Liidu õigusega vastuolus. See tähendab, et seadusandjal tuleks majutusasutuste külastajate andmete kogumise osas kavandatavad meetmed kindlasti täiendavalt üle vaadata ning nende proportsionaalsust hinnata EIÕK ja põhiõiguste harta ning ka EIK ja EK praktikast lähtuvalt.

KOKKUVÕTE

Käesoleva töö eesmärgiks oli välja selgitada, millistel tingimustel on Euroopa Liidu õiguse raames võimalik elektroonilise side andmeid koguda, säilitada ja kasutada kuritegevusevastases võitluses ning kas EK on oma praktikaga loonud proportsionaalsuse testi hulka kuuluvad uued kohustuslikud standardid, s.o minimaalsed nõuded, millele siseriiklik õigus peab vastama selleks, et see oleks Euroopa Liidu õiguse valguses proportsionaalne. Magistritöö hüpoteesiks oli, et sideandmete säilitamise ja kasutamise regulatsioonide hindamisel ja rakendamisel tuleb kohustuslikus korras lähtuda EK poolt sätestatud kontrollskeemist.

Magistritöö koosnes kolmest peatükist. Esimeses peatükis käsitles autor põgusalt privaatsusõiguse olemust, tõi välja selle tähtsuse demokraatlikus ühiskonnas ning analüüsis, kas ja miks on vajalik isikuandmete kaitset privaatsusõigusest eraldiseisvalt käsitleda. Kokkuvõtvalt tuvastas autor, et privaatsusõigus ning isikuandmete kaitse kui selle moodsam haru on mõlemad suure tähtsusega põhiõigused, millele on tagatud kaitse mitmete rahvusvaheliste õigusaktidega ning mille sisu ning ulatust on aidanud defineerida nii EIK kui EK. Privaatsusõiguse ning isikuandmete kaitse riive on küll lubatud, kuid seda riivet peab hindama proportsionaalsuse testi abil. Kuigi põhiõiguste harta artikliga 8 on isikuandmete kaitse iseseisva põhiõigusena kaitstud, ei ole EK oma senises praktikas seda privaatsusõigusest eraldiseisvalt sisuliselt analüüsitud. Privaatsusõigus ja isikuandmete kaitse leiavad kohtupraktikas käsitlemist ühise hübriidõigusena ning reeglina on see kohtuvaidluse esemest, s.o riivatava huvi ja riive iseloomust lähtuvalt olnud ka õigustatud. Samas võib esineda olukordi, kus isiku eraelu sfääri ei ole sekkutud, kuid sellegipoolest on esinenud isikuandmete kaitse riive ning selleks puhul saab isikule kaitset tagada just põhiõiguste harta artiklile 8 tuginedes.

Teises peatükis analüüsis autor põhjalikult EK lahendit *Digital Rights Ireland*, millega EK 2014. aastal Euroopa Liidu andmete säilitamise direktiivi kehtetuks

tunnistas. Autor käsitles lahendi olulisemaid pidepunkte ning tuletas sellest sideandmete säilitamise ja kasutamise kui privaatsusõiguse riive proportsionaalsuse hindamise standardi. *Digital Rights Ireland* lahendist jäi aga selgusetuks, kas seda standardit peaks käsitlema kui liikmesriikide siseriiklike õigusnormide proportsionaalsuse hindamise kohustuslikku kontrollskeemi. Mitmed liikmesriikid ei osanud *Digital Rights Ireland* otsuse järgselt otsustada, mida direktiivist alles jäänud riigisiseste meetmetega edasi peale hakata, lähtuti nii rangest tõlgendusest, mille kohaselt kõikide kasutajate preventatiivne sideandmete säilitamine on põhiõigustega vastuolus ega ole seetõttu lubatud, kui ka lubavast tõlgendusest, mille kohaselt ei ole sideandmete massiline säilitamine iseenesest põhiõigustega vastuolus, kui vastavas reeglistikus on olemas piisavad tagatised kasutajate põhiõiguste kaitseks.

Eestis *Digital Rights Ireland* lahend suuremat diskussiooni esile ei toonud. Õiguskantsler teostas kehtetust direktiivist üle võetud ESS normide "abstraktse" põhiseadusele vastavuse hindamise ning jõudis järeldusele, et regulatsioon, milles esinevad sarnased puudujäägid kui esinesid kehtetuks tunnistatud direktiivis, on põhiseadusega kooskõlas. Erinevalt EK-st ei käsitlenud õiguskantsler sideandmete kogumise, säilitamise ja kasutamise regulatsiooni ühe tervikuna, vaid hindas seda etappide kaupa, mis suure tõenäosusega mõjutas ka EK-st erinevale lõppjäreldusele jõudmist.

Kolmandas peatükis analüüsis autor EK lahendit *Tele2 Sverige*, millega EK kinnitas *Digital Rights Ireland* lahendis avaldatud seisukohti ning nende kohustuslikkust siseriiklike normide hindamisele. EK pidas *Tele2 Sverige* lahendis kogu sideandmete regulatsiooni tervikuna, s.t nii andmete kogumist, säilitamist kui hilisemat kasutamist, Euroopa Liidu õiguse kohaldamisalas olevaks ning keelustas sideandmete massilise preventatiivse kogumise kui ebaproportsionaalse meetme. Sellist keelustamist on küll kritiseeritud (näiteks: preventatiivse andmekogumise keelamine halvab kuritegevusevastase võitluse; keeld on vaid sümboolse mõjuga, kuna sideettevõtjad säilitavad andmeid kohustuse puudumisest hoolimata), kuid EK lähenemisega, mille kohaselt mugavus ei saa üles kaaluda inimeste põhiõigust privaatsusele ja isikuandmete kaitsele, tuleb igati nõustuda.

Autor formuleeris kolmandas peatükis töös käsitletud EIK ja EK prakika põhjal sideandmete kaitse valdkonnas privaatsusõigust riivava meetme proportsionaalsuse hindamise kontrollskeemi elemendid ning tõi nende valguses välja Eesti kehtivas õiguses esinevad puudujäägid. Kontrollskeemi elementideks on: a) andmete eristamine ja piiritlemine; b) seos raskete kuritegudega; c) säilitamisperioodi eristamine ja piiritlemine; d) säilitatud andmete kaitse kuritarvitamiste eest; e) kohtulik eelkontroll; f) juurdepääsuõiguste piiramine; g) sõltumatu järelvalve; h) andmesubjektide teavitamine; i) andmete hävitamine. Eesti kehtivas regulatsioonis esineb puudujääke iga kontrollskeemi elemendi osas. Kokkuvõtvalt leidis kinnitust magistritöö hüpotees, mille kohaselt tuleb sideandmete säilitamise ja kasutamise regulatsioonide hindamisel ja rakendamisel kohustuslikus korras lähtuda EK poolt proportsionaalsuse testi raames sätestatud kontrollskeemist.

Puudub kahtlus selles, et Eesti kehtiv sideandmete säilitamise ja kasutamise regulatsioon on Euroopa Liidu õigusega vastuolus ning seadusandja peab välja töötama uue lahenduse. Uue regulatsiooni loomisel tuleks seadusandjal kindlasti eeltoodud kontrollskeemi elementidega arvestada ning lähtuda EIK ja EK seisukohtadest ja tõlgendustest. Autor käsitles lõpetuseks põgusalt ka seda, kas EK poolt loodud kontrollskeemi oleks peale sideandmete valdkonna paslik rakendada ka muudeks juhtudeks, kus toimub andmete kogumine ja kasutamine mingitel avalikel kaalutlusel, eeskätt kuritegevusevastase võitluse eesmärgil ning leidis, et Eestis planeeritava majutusasutuste klientide andmete kogumise, säilitamise ja kasutamise regulatsiooni puhul oleks samuti vajalik viia läbi proportsionaalsuse hindamine kontrollskeemile, kuna plaanitakse kasutusele võtta sideandmete regulatsoonile üsnagi sarnaseid meetmeid.

SUMMARY

The criteria for evaluating the proportionality of limitations to the right to privacy in the Law of the European Union on the example of communications data protection

During recent years the global situation has become rather alarming due to the refugee crisis and the conflicts in Middle-East. News about terrorist attacks can be heard disturbingly often and therefore the prevention of such attacks and for fighting other serious crime is essential. Security authorities are obliged to protect the people and their interest is to use all possible and available means to ensure safety in our society. Technology is evolving rapidly and modern solutions allow easy collection and processing of data. We live in the era on Big Data, where all sorts of personal data is available in social media and the world wide web and this data can be used to make connections and conclusions about the users. Surely, the security authorities are interested in such data and are more than willing to use it for national security purposes.

However, when personal data is collected and stored, issues regarding the protection of the right to privacy will arise. The right to privacy is protected under the European Convention on Human Rights (ECHR) and the Charter of Fundamental Rights of the European Union (Charter) and is essential in the proper functioning of a democratic society. When means for collecting, storing and processing personal data are applied, they must be evaluated in the light of the aforementioned legislation.

In 2006, the EU enforced directive 2006/24/EC, which imposed compulsory electronic communications data retention for the prevention, investigation, detection, and prosecution of criminal offences in the Member States. The Directive included many provisions that were regarded as overly intervening with the right to privacy. In its 2014 decision in case *Digital Right Ireland*, the European Court of Justice (ECJ) deemed the directive null and void due to exceeding the limits of the principle of proportionality in the light of articles 7, 8 and 52(1) of the Charter. However, the ECJ did not specify, if the Member States' measures that had been established as a result

of the now void directive should also be evaluated in the light of the Charter. In its 2016 decision *Tele2 Sverige*, ECJ finally stated clearly that all domestic legislation that does not comply with the Charter, is in conflict with the law of the European Union.

This thesis took interest in the communications data retention schemes in the European Union. The aim of the thesis was to ascertain the permissible means for data retention when applying state surveillance measures in the fight against crime under the EU law, also to assess whether the ECJ has established a new standard for the evaluation of the proportionality of the Member States' domestic privacy-envading legislation. The author proposed the hypothesis, that the regulations regarding the retention and processing of communications data must be evaluated and applied pursuant to the compulsory checklist of safeguards established by the ECJ.

The thesis consisted of three chapters. In the first chapter, the essence and importance of the right to privacy was analysed and the reasons for distinguishing the "classic" right to privacy and the "modern" right of personal data protection were brought out. Both the right to privacy and right to personal data protection are deemed to be fundamental human rights in various international conventions and their essence and scope have been defined by the ECJ as well as by the European Court of Human Rights. The limitation of those rights is not prohibited, however, all such means must be in conformity with the ECHR and the Charter, i.e. do not exceed the limits of what is appropriate and necessary in order to achieve its objective. ECJ and the European Court of Human Rights both tend to handle the right to privacy and the right to personal data protection as one "hybrid right" and so far that has been justified due to the object and essence of the dispute. However, cases where personal data has been processed but there is no invasion of private life, may arise in the future – in this case article 8 of the Charter alone should provide all necessary protection for individuals.

In the second chapter, the ECJ's ruling *Digital Rights Ireland* is analysed thoroughly. The autor brought out the ECJ's most important statements and identified the essential safeguards for the proportionality evaluation standard of privacy-envading legal measures, as provided for in directive 2006/24/EC. Since many Member States

were confused what to do with the domestic measures enforced on the light of the void directive, the author briefly compares the States' reactions. Mostly the States used two different approaches: the strict interpretetation and the permissive interpretation. The approach deemed all "blanket" retention schemes, i.e measures allowing preventive masscollection of all users' data, unlawful due to infringement with the Charter, while the second approach considered that mass surveillance is not illegal *per se* when proper safeguards are in place. Estonia repesented the permissive interpretation approach: the data retention regulation derived from the void directive, mostly stated in the Electronic Communications Act, is still in force in its original state, although it has the same shortcomings as the directive itself. There has been no broad discussion about this matter, however, the Chancellor of Justice has evaluated the Electronic Communications Act in the light of the Constitution and found that there is no conflict with its provisions. This opinion is questionable, as the legislation lacks the safeguards established by the ECJ in the *Digital Rights Ireland* ruling. Most likely the Chancellor of Justice reached this dissenting opinion since she analysed the provisions regarding the collection and retention of data separately from the provisions regarding the processing of data (note: ECJ analysed the measures as a whole and did not separate different stages). If the provisions would not have been separated, all the shortcomings from differet stages would have accumulated and affected the final position. If there are shortcomings in the data processing measures, then more safeguards must be in place in the data retention measures and *vice versa*.

In the third chapter the author analysed the most recent ECJ ruling on data retention matters: *Tele2 Sverige*. In this ruling the ECJ confirmed its previous statements in *Digital Right Ireland* case, including the binding nature of the proportionality assessment standards. With *Tele2 Sverige* ECJ deemed "blanket" retention, i.e mass surveillance unlawful and regarded Member States' legislation, which allowed such measures, to be in conflict with the Charter. The prohibition of blanket retention has been criticised, firstly because it cripples crime prevention and investigantion, and secondly because it is only symbolic as telecommunications undertakings preserv the same data even if there is no such obligation. However, the autor believes that convenience can never justify the infringement of one's human rights and

fundamental freedoms and that such rights and freedoms must be respected, especially in today's modern techology based "Big Data" era.

The Author identified the necessary elements for evaluating the proportionality of privacy-envading measures, as set forth by the ECJ as well as by the Court of Human Rights. Those elements are: a) the distinction and limitation of data; b) link to serious crime; c) distinction and limitation of retention periods; d) protection of the retained data against the risk of abuse and unlawful access; e) prior review by court; f) limitation of the right to access retained data; g) supervision by an independent authority; h) informing the data subject; i) destruction of the data. Estonia's legislation has shortcomings regarding all the aforementioned elements. In conclusion, the hypothesis, that the regulations regarding the retention and processing of communications data must be evaluated and applied pursuant to the compulsory checklist of safeguards established by the ECJ, was affirmed.

There is no doubt that the data retention scheme in Estonia is in violation with the EU law and that he legislator has to adopt new measures. When adopting new measures, it is essential that the proportionality evaluation standard, as provided by the ECJ, will be considered. This standard should not, however, be bound to communications data only, but should be used in all cases regarding the collection of personal data for security purposes. Recently news about the Estonian government planning to establish measures to collect the data of all accomodation establishments' clients broke out. At first view, the planned measures seem intimidatingly similar to the communications data retention schemes that have been deemed unlawful by the ECJ and the Court of Human Rights. The legislator should assess these measures in the light of the aforementioned proportionality evaluation standard as well.

KASUTATUD ALLIKATE LOETELU

Teaduskirjandus

1. **S. Allen**. Remembering and Forgetting - Protecting Privacy Rights in the Digital Age. - European Data Protection Law Reviev, 164/2015

2. **A. Ashworth**. Human Rights, Serious Crime and Criminal Procedure. – The Hamlin Lectures. London: Sweet and Maxwell, 2002. Arvutivõrgus kättesaadav: https://socialsciences.exeter.ac.uk/media/universityofexeter/schoolofhumanitiesandsocialsciences/law/pdfs/Human_Rights_Serious_Crime_and_Criminal_Procedure.pdf (22.04.2017)

3. **V. Boehme-Neßler**. Privacy: a matter of democracy. Why Democracy Needs Privacy and Data Protection. - International Data Privacy Law, 2016/6, no 3

4. **F. Boehm ja M. D. Cole**. Data Retention after the Judgement of the Court of Justice of the European Union. - Study for the Greens/EFA Group in the European Parliament, 30.06.2014. Arvutivõrgus: http://www.janalbrecht.eu/fileadmin/material/Dokumente/Boehm_Cole_-_Data_Retention_Study_-_June_2014.pdf (09.04.2017)

5. **G. Butarelli**. The EU GDPR as a clarion call for a new global digital gold standard. - nternational Data Privacy Law, 2016/6, No 2

6. **O. Diggelmann, M. N. Cleis**. How the Right to Privacy Became a Human Right. - Human Rights Law Review 2014 (14) 3

7. **S. Douglas-Scott**. Constitutional Law on the European Union. - Pearson Education Limited, UK 2002,

8. **C. Docksey**. Four Fundamental Rights: Finding the Balance. - International Data Privacy Law, 2016/6, no 3

9. **L. Drewry**. Crimes without Culprits: Why the European Union Needs Data Retention, and How it Can Be Balanced With the Right to Privacy. - Wisconsin International Law Journal, 2016/33, no 4

10. **M. - P. Granger ja K. Irion**. The Court of Justice and the Data Retention Directive in Digital Rights Ireland: telling off the EU legislator and teaching a lesson in privacy and data protection. - European Law Review 39/2014, no 4

11. **G. Greenwald, E. MacAskill**. NSA Prism program taps in to user data of Apple, Google and others. - The Guardian, 07.06.2013. Arvutivõrgus kättesaadav: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (10.04.2017)

12. **E. Guild ja S. Carrera**. The Political and Judicial Life of Metadata: Digital Rights Ireland and the Trail of the Data Retention Directive. - CEPS Papers in Liberty and Security in Europe, no 65/May 2014. Arvutivõrgus kättesaadav: https://www.ceps.eu/system/files/EG%20and%20SC%20Data%20retention.pdf (09.04.2017)

13. **P. de Hert ja P. C. Bocos**. Case of Roman Zakharov v. Russia: The Strasbourg follow up to the Luxembourg Court's Schrems judgment. – Strasbourg Observers, 23.12.2015. Arvutivõrgus kättesaadav: https://strasbourgobservers.com/2015/12/23/case-of-roman-zakharov-v-russia-the-strasbourg-follow-up-to-the-luxembourg-courts-schrems-judgment/ (09.04.2017)

14. **C. Jones**. Background to the EU Data Retention Directive. - EU Law Analysis, 07.04.2014. Arvutivõrgus: http://eulawanalysis.blogspot.com/2014/04/background-to-eu-data-retention.html (09.04.2017)

15. **O. Lynskey**. Deconstruction Data Protection: The „Added-Value" of a Right to Data Protection in the EU Legal Order. – International & Comparative Law Quarterly 2014 (63) 3.

16. **M. Kotula**. IP addresses as personal data - the CJEU's judgment in C-582/14 Breyer. – EU Law Analysis, 04.01.2017. Arvutivõrgus kättesaadav: http://eulawanalysis.blogspot.com.ee/2017/01/ip-addresses-as-personal-data-cjeus.html (09.04.2017)

17. **A. Lott**. Põhiseadusliku korra kaitseks teostatav jälitustegevus Eestis. - Riigikohus: Tartu 2015. Arvutivõrgus kättesaadav: http://www.riigikohus.ee/vfs/1906/PKK%20j%E4litustegevuse%20anal%FC%FCs.pdf (09.04.2017)

18. **U. Lõhmus**. Elektroonilise side andmete säilitamise lõpetamata saaga. - Juridica 2015/10

19. **U. Lõhmus**. Elektroonilise side andmete säilitamise saaga sai lahenduse, Eestis siiski veel mitte. - Juridica 2016/10

20. **U. Lõhmus**. Pealtkuulamine ja Eesti põhiseaduses sätestatud õigus sõnumite saladusele. – Juridica 2008/7

21. **Ü. Madise jt** (toim). Eesti Vabariigi põhiseadus. Komm vlj. 3. vlj. Tallinn: Juura 2012

22. **R. Maruste**. Konstitutsionalism ning põhiõiguste ja -vabaduste kaitse. Tallinn: Juura 2004

23. **J. Milaj**. Invalidation of the data retention directive: extending the proportionality test. – Computer Law & Security Review 2015/31

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

25. **P. Schasmin ja C. Ginter**. Lahendite Tele2 Sverige ja Digital Rights Ireland mõju sideandmete mugavkasutusele Eestis. – Juridica 1/2017

26. **S. Schweda**. UK Surveillance Under Judicial Scrutiny: GCHQ Intelligence Sharing with NSA Contravened Human Rights, But Is Now Legal. – European Data Protection Law Review, 1/2015

27. **B. van der Sloot**. How to assess privacy violations in the age of Big Data? Analysing the three different tests developed by the ECtHR and adding for a fourth one. – Information & Communications Technology Law 2015/24

28. **D. J. Solove**. Nothing to Hide. The False Tradeoff Between Privacy and Security. Yale University Press, 2011

29. **M. Taylor**. The EU's Human Rights Obligations in Relation to its Data Protection Laws with Extraterritorial Effect. - International Data Privacy Law, 2015/5, no 4

30. **P. K. Tupay**. Õigusest eraelule kuni andmekaitse üldmääruseni ehk tundmatu õigus isikuandmete kaitsele. - Juridica 2016/4

31. **N. Vainio ja S. Miettinen**. Telecommunications data retention after *Digital Rights Ireland*: legislative and judicial reactions in the Member States. - International Journal of Law and Information Technology, 2015/23

32. **D. Warren, L. Brandeis**. The Right to Privacy. - Harvard Law Review, 1890/1891/4, 193

33. **M. White**. A Threat to Human Rights? The new e-Privacy Regulation and some thoughts on Tele2 and Watson. – EU Law Analysis, 10.01.2017. Arvutivõrgus kättesaadav: http://eulawanalysis.blogspot.com.ee/2017/01/a-threat-to-human-rights-new-e-privacy.html (09.04.2017)

34. **L. M. Woods**. Data retention and national law: the ECJ ruling in Joined Cases C-203/15 and C-698/15 Tele2 and Watson. – EU Law Analysis, 21.12.2016. Arvutivõrgus kättesaadav: http://eulawanalysis.blogspot.com.ee/2016/12/data-retention-and-national-law-ecj.html (09.04.2017)
35. **L. M. Woods**. High Court Strikes Down Data Retention Laws in Ruling on DRIPA. - European Data Protection Law Review, 3/2015

Õigusaktid

Eesti õigusaktid:

36. Eesti Vabariigi põhiseadus. - RT I, 15.05.2015, 2
37. Elektroonilise side seadus. - RT I, 23.03.2017, 5
38. Isikuandmete kaitse seadus. - RT I, 06.01.2016, 10
39. Julgeolekuasutuste seadus. - RT I, 17.12.2015, 39
40. Karistusseadustik. - RT I, 31.12.2016, 14
41. Kindlustustegevuse seadus. - RT I, 31.12.2016, 26
42. Korrakaitseseadus. - RT I, 02.12.2016, 6
43. Kriminaalmenetluse seadustik. - RT I, 31.12.2016, 46,
44. Maksukorralduse seadus. - RT I, 31.03.2017, 3
45. Politsei ja piirivalve seasdus. - RT I, 15.12.2016, 7
46. Turvaseadus. - RT I, 30.12.2015, 54
47. Väärteomenetluse seadustik. - RT I, 01.03.2017, 5
48. Õiguskantsleri seadus. - RT I, 06.04.2016, 23

Rahvusvahelised ja välisriikide õigusaktid:

49. Inimõiguste Ülddeklaratsioon. Arvutivõrgus: http://www.un.org/en/universal-declaration-human-rights/ (07.04.2017)
50. Inimõiguste ja põhivabaduste kaitse konventsioon. - RT II 2000, 11, 57
51. Kodaniku- ja poliitiliste õiguste rahvusvaheline pakt. - RT II 1994, 10, 11
52. Isikuandmete automatiseeritud töötlemisel isiku kaitse konventsioon. – RT II 2001, 1, 3

53. Rahvusvahelise organiseeritud kuritegevuse vastu võitlemise Ühinenud Rahvaste Organisatsiooni konventsioon. - RT II 2003, 1, 1
54. Euroopa Liidu toimimise leping (ELT C 326, 26.10.2012). Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=uriserv:OJ.C_.2012.326.01.0001.01.EST#C_2012326ET.01004701 (07.04.2017)
55. Euroopa Liidu põhiõiguste harta. - ELT C 326, 26.10.2012. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A12012P%2FTXT (07.04.2017)
56. Euroopa Parlamendi ja Nõukogu direktiiv 95/46/EÜ, 24. oktoober 1995, üksikisikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise kohta. - ELT L 281, 23.11.1995. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/et/ALL/?uri=CELEX:31995L0046 (07.04.2017)
57. Euroopa Parlamendi ja Nõukogu määrus (EÜ) nr 45/2001, 18. detsember 2000, üksikisikute kaitse kohta isikuandmete töötlemisel ühenduse institutsioonides ja asutustes ning selliste andmete vaba liikumise kohta. - ELT L 8, 12.1.2001. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1491558697563&uri=CELEX:32001R0045 (07.04.2017)
58. Euroopa Parlamendi ja nõukogu direktiiv 2002/58/EÜ, 12. juuli 2002, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv). - ELT L 201, 31.7.2002. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32002L0058 (07.04.2017)
59. Euroopa Parlamendi ja Nõukogu määrus (EL) 2016/679, 27. aprill 2016, füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 95/46/EÜ kehtetuks tunnistamise kohta (isikuandmete kaitse üldmäärus). - ELT L 119, 04.05.2016. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=ET (07.04.2017)

60. Euroopa Parlamendi ja nõukogu määrus (EÜ) nr 1049/2001, 30. mai 2001, üldsuse juurdepääsu kohta Euroopa Parlamendi, nõukogu ja komisjoni dokumentidele. - ELT L 145, 31.5.2001. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1491560704007&uri=CELEX:32001R1049 (07.04.2017)

61. Euroopa Nõukogu 17. jaanuari 1995 resolutsioon telekommunikatsiooniseanssidesse seadusliku sekkumise kohta. - ELT C 329, 4.11.1996. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31996G1104 (07.04.2017)

62. Euroopa Parlamendi ja Nõukogu direktiiv 97/66/EÜ, 15.12.1997, telekommunikatsioonisektoris isikuandmete töötlemise ja privaatsuse kaitse kohta. - ELT L 24, 30.1.1998. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31997L0066:EN:HTML (07.04.2017)

63. Euroopa Parlamendi 29. oktoobri 2015. aasta resolutsioon Euroopa Parlamendi 12. märtsi 2014. aasta ELi kodanike massilist elektroonilist jälgimist käsitleva resolutsiooni järelmeetmete kohta, p 51. Arvutivõrgus kättesaadav: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2015-0388+0+DOC+PDF+V0//ET (07.04.2017)

64. 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, 13.4.2006. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/legal-content/ET/TXT/?uri=CELEX%3A32006L0024 (07.04.2017)

Kohtupraktika

Euroopa Inimõiguste Kohu lahendid:

65. EIKo 5029/71, *Klass and Others v Germany*

66. EIKo 9248/81, *Leander v Sweden*

67. EIKo 20837/92, *MS v Sweden*
68. EIKo 22009/93, *Z v Finland*
69. EIKo 28341/95, *Rotaru v Romania*
70. EIKo 54934/00, *Weber and Saravia v Germany*
71. EIKo 58243/00, *Liberty v UK*
72. EIKo 62332/00, *Segerstedt-Wiberg and Others v Sweden*
73. EIKo 2872/02, *K.U. v Finland*
74. EIKo 7508/02, *LL v France*
75. EIKo 36919/02, *Armonas v Lithuania*
76. EIKo 20511/03, *I v Finland*
77. EIKo 0562/04 ja 30566/04, *S and Marper v UK*
78. EIKo 26839/05*, Kennedy v United Kingdom*
79. EIKo 47143/06 *Roman Zakharov v Russia*
80. EIKo 24029/07, *MM v UK*
81. EIKo 19522/09, *M. K. v France*
82. EIKo 37138/14, *Szabo and Vissy v Hungary*

Euroopa Kohtu lahendid:

83. EKo 15.07.1964, C-6/64, *Costa v ENEL*
84. EKo C-293/97, *The Queen v Minister of Agriculture, Fisheries and Food, ex parte Standley jt.*
85. EKo liidetud kohtuasjad C-317/04 ja C-318/04, *European Parliament v Council of the European Union and European Parliament v European Commission*
86. EKo C-301/06, *Ireland v European Parliament and European Council*
87. EKo liidetud kohtuasjad C-402/05 P ja C-415/05, *Kadi and Al Barakaat International Foundation v Council and Commission*,
88. EKo liidetud kohtuasjad C-92/09 ja C-93/09, *Volker und Markus Schecke and Hartmut Eifert v Land Hessen*
89. EKo liidetud kohtuasjad C-539/10 P ja C-550/10 P, *Al-Aqsa v Council*
90. EKo C-283/11, *Sky Österreich v Österreichischer Rundfunk*
91. EKo C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*

92. EKo liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*
93. EKo C-243/13, *European Commission v Sweden*
94. EKo C-362/14, *Maximillian Schrems v Data Protection Commisioner*
95. EKo C-582/14, *Patrick Breyer v Germany*
96. EKo liidetud kohtuasjad C-203/15 ja C-698/15, *Tele2 Sverige AB v Post- och telestyrelsen*

Riigikohtu lahendid:

97. RKHKo 19.04.2005, 3-4-1-1-05
98. RKHKo 5.10.2006, 3-3-1-33-06
99. RKHKo 7.05.2008, 3-3-1-85-07
100. RKHKo 26.06.2008, 3-4-1-5-08
101. RKPSJKo 20.03.2014, 3-4-1-42-13
102. RKKKo 23.02.2015, 3-1-1-51-14
103. RKHKo 10.06.2016, 3-3-1-84-15

Muud allikad

104. EK C-92/09 ja C-93/09, *Volker und Markus Schecke GbR v Land Hessen,* kohtujuristi ettepanek
105. EK C-131/12, *Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González,* kohtujuristi ettepanek
106. EK liidetud kohtuasjad C-293/12 ja C-594/12, *Digital Rights Ireland v Minister for Communications, Marine and Natural Resources, Seitlinger and Others*, kohtujuristi ettepanek
107. Explanations Relating to the Charter of Fundamental Rights of the European Union. – ELT C 303, 14.12.2007. Arvutivõrgus kättesaadav: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2007:303:0017:0035:en:PDF (07.04.2017)

108. Euroopa Komisjoni 27.10.2011 pressiteade*:* Commission requests Germany and Romania fully transpose EU rules. Arvutivõrgus kättesaadav: http://europa.eu/rapid/press-release_IP-11-1248_en.htm (09.04.2017)
109. Euroopa Komisjoni 18.04.2011 raport andmete säilitamise direktiivi kohta. Arvutivõrgus kättesaadav:
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2011:0225:FIN:en:PDF (09.04.2017)
110. Euroopa andmekaitseinspektori arvamus Komisjoni 18.04.2011 raporti kohta. - ELT C 279, 23.9.2011. Arvutivõrgus kättesaadav:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52011XX0923(01) (09.04.2017)
111. Eurojust's analysis of EU Member States' legal framework and current challenges on data retention, 26.10.2015. Arvutivõrgus kättesaadav: http://www.statewatch.org/news/2015/oct/eu-eurojust-analysis-ms-data-retention-13085-15.pdf (09.04.2017)
112. Ambiguous judgment of the European Court of human rights on surveillance issues. - Association Européenne pour la défense des Droits de l'Homme (AEDH). Arvutivõrgus kättesaadav:
http://www.aedh.eu/Ambiguous-judgment-of-the-European.html (09.04.2017)
113. E-Privacy. Survey requested by the European Commission, Directorate-General for Communications Networks, Content and Technology (DG CONNECT) and co-ordinated by Directorate-General for Communication. – Flash Eurobarometer 443 – TNS Political & Social, July 2016. Uuringu tulemused ja dokumendid on kättesaadavad arvutivõrgus:
http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124 (10.04.2017)
114. Õiguskantsleri 20.07.2015.a seisukoht elektroonilise side seaduse § 111^1 põhiseaduspärasuse kohta. Arvutivõrgus kättesaadav:
http://www.oiguskantsler.ee/sites/default/files/field_document2/6iguskantsleri_seisukoht_vastuolu_mittetuvastamise_kohta_elektroonilise_side_andmete_kogumine_sideettevotete_poolt.pdf (09.04.2017)

115. Õiguskantsleri 22.04.2016.a analüüs elektroonilise side seaduse § 111[1] põhiseaduspärasuse kohta. Arvutivõrgus kättesaadav: http://www.oiguskantsler.ee/sites/default/files/field_document2/elektroonilise_side_seaduse_ss_111_1_alusel_sideandmete_tootlemise_pohiseadusparasus.pdf (09.04.2017)
116. Riik hakkab kontrollima majutusasutuste külastajate tausta. – Postimees, 20.02.2017. Arvutivõrgus kättesaadav: http://www.postimees.ee/4020547/riik-hakkab-kontrollima-majutusasutuste-kulastajate-tausta
117. G. Orwell. 1984. – Tallinn: Tänapäev, 2010

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Kätlin Helena Sehver, isikukoodiga 49201260882,

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Privaatsusõiguse riive proportsionaalsuse hindamise kriteeriumid Euroopa Liidu õiguses elektroonilise side andmete kaitse valdkonna näitel", 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, 02.05.2017